International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

AI Based Decentralized Custodial Wallet for Gas Optimised Transaction

Ms. Susmitha M N[1], *Mr. Rohit Kumar Singh* [2], *Mr. Utkarsh* [3], *Mr. Joel Machado* [4], *Ms. Ria Megan Picardo*[5]

[1]Assistant Professor, Dept. of CSE, MVJ College of Engineering, Karnataka, India
[2-5]Students, Dept. of AI&ML, MVJ College of Engineering, Karnataka, India

DOI: https://doi.org/10.55248/gengpi.5.0524.1115

ABSTRACT:

This paper presents an innovative solution to the challenges faced by traditional custodial wallets in managing gas fees in blockchain transactions. We introduce a custodial wallet integrated with Artificial Intelligence (AI), specifically designed to optimize gas usage. The wallet leverages a machine learning algorithm, DeepAR, to dynamically analyze market conditions, transaction history, and gas fee trends. This model adapts to real-time changes, enabling users to optimize their transactions by predicting favorable gas fee windows. The research involves the design and development of the custodial wallet, the implementation of AI components for gas fee prediction, and a comparative performance assessment against conventional custodial wallets. The result is a user-friendly wallet that enhances transaction efficiency and contributes to a more sustainable and cost-effective blockchain experience. This research has the potential to significantly impact the blockchain industry by providing a more efficient and economical transaction method.

Keywords: Custodial wallet, Machine learning , Deep AR , Gas fee, Ethereum

Introduction:

In the current digital era, the proliferation of cryptocurrencies has revolutionized the financial landscape. As these digital assets gain traction, the associated transaction costs, particularly the ‘gas’ fees in Ethereum blockchain, have become a critical consideration for users. Gas fees are compensations provided to miners for incorporating data entries into the blockchain. However, these fees can fluctuate significantly during peak times, causing transactions with lower maximum gas limits to experience longer wait times before being added to the blockchain. This variability in gas prices underscores the importance of efficient gas fee management and prediction. Traditional custodial wallets, which are used to store and manage digital assets, often struggle with this challenge. The inefficiencies in managing gas fees can lead to increased transaction costs and longer processing times, hindering the user experience. To address this issue, this research introduces an innovative solution: an AI-integrated custodial wallet designed to optimize gas usage in blockchain transactions.

This wallet leverages the power of artificial intelligence, specifically a machine learning algorithm known as DeepAR, to dynamically analyze market conditions, transaction history, and gas fee trends. By adapting to real-time changes, the wallet provides users with predictive insights into favorable gas fee windows. This empowers users to strategically time their transactions, optimizing gas efficiency and enhancing the overall transaction experience.The research encompasses the design and development of this AI-integrated custodial wallet, the implementation of the DeepAR algorithm for gas fee prediction, and a comparative performance assessment against traditional custodial wallets. The ultimate goal is to create a user-friendly wallet that not only improves transaction efficiency but also contributes to a more sustainable and cost-effective blockchain experience. This research holds significant potential to transform the blockchain industry by offering a more efficient and economical method for conducting transactions.

Literature Survey:

“Blockchain Transaction Fee Forecasting : A Comparison of Machine Learning Models” [1] is a paper that compares different modeling approaches, including LSTM, attention mechanism, CNN-LSTM(hybrid models). The hybrid model outperforms other models, particularly at earlier lookaheads. Attention models have comparable performance to the hybrid model at longer lookaheads. The relevant factors that influence gas price in the Ethereum network include block utilization, transaction urgency, ETH value, miner count, and unconfirmed transaction count. Gas price has been found to have a negative correlation with miner count and unconfirmed transaction count. Gas price is also negatively associated with ETH value, indicating that network users are concerned with the cost of network usage in terms of real currency value. The limitations of this study are primarily related to available computing resources since combining CNN with LSTM becomes a very complex model and requires more computational resources and this models require a additional hardware in order to test the data and the accuracy is less compared to the newly time series models.

"Network Activity and Ethereum Gas Prices" [2] is a paper that shows a relationship between network activity and ethereum gas price using quantile linear regression . The results show that the number of intraday transactions within the Ethereum blockchain is the most consistent variable in explaining gas fees. As the number of transactions increases, it puts more demand on the Ethereum network, leading to potential congestion. As a result the gas fee increases and only finds how the network activity can affect the gas price but nor exactly predict the gas fee.

"Ethereum Gas Price Prediction Using Facebook Prophet Model" [3] is a paper in which the prediction of gas prices was conducted in using the Facebook prophet model in python programming language with the aim to narrow the gap between the current unexpected gas fee price and the ability of predicting the future gas fee, based on past gas prices and current dataset gathered daily for eight years between 2015 and 2022 and prophet model considers the time series to be stationary and does not capture interactions between multiple seasonal patterns. Training the model with a large number of observations may require more resources, and the process might become time consuming.

The paper **"A Machine Learning Approach for Gas Price Prediction in Ethereum Blockchain" [4]** predictes gas fee using Prophet and deep learning algorithms such as Long-Short Term Memory (LSTM) and Gated Recurrent Unit (GRU). An evaluation of the obtained results show that the LSTM and GRU proposed models outperform . In this case, LSTM and GRU provide a low mean squared error (MSE) of 0.008. Additionally, the challanges of this paper is that LSTM and GRU cannot forecast for long term dependencies. Both the models can be computationally intensive, especially when dealing with large and complex time series datasets.

"Comparative Graph Analysis on Ethereum: 'The Merge' and Gas Price Prediction" [5] is a paper used to predict how the transaction has been affected after "The Merge" event and used various graph based models for gas fee prediction using predictive and descriptive analysis such aNode2Vec and GATv2. Additionally, the challanges of the paper is that the graph based models wont perform well on sequential data. The graph representation does not appropriately capture the underlying relationships in the time series, the model might struggle to make accurate.

The paper **"A Better Approach for Recommending the Ethereum Gas Price" [6]** applies deep learning algorithm called GRU for gas fee prediction which is sampled of around five days of data from 20 November, 2019 (block 8,965,759) to November 24, 2019 (block 8,995,344) and evaluate the different price recommendation strategies. Moreover, the challanges of the paper is the architecture of a GRU is fixed once it is designed, and it might not adapt well to various types of time series data. GRUs may have limitations in capturing highly complex patterns or relationships in time series data.

"A Practical and Economical Bayesian Approach to Gas Price Prediction" [7] is the paper used to compare the traditional gas oracle with the Gaussain process models . The GP model maintains reasonable accuracy in estimating gas prices when transaction volumes fluctuate greatly. Existing oracles like GS-Express and Geth tend to overestimate or underestimate prices under such conditions. Secondly, the GP model possesses time efficiencies in both model training and prediction. It takes less time to train and predict compared to other oracles. Additionally, the challanges is that if the data is not pre processed properly then prediction of the model might be incorrect. It is not effective in predicting the time series data. When transactions is fee is zero it can introduce noise and affect the performance of the model.

The paper **"Examining Usability Issues in Blockchain-Based Cryptocurrency Wallets" [8]** discusses blockchain wallets in user's perspective. It highlights the bad user experience design of the wallets, briefing about the complex nature of holding number of keys(public, private), password and the point that we cannot recover our account back, if we don't have the private key and cannot make multiple accounts. The limitation of the paper is that the difficulty in holding and managing a mneomonic phase and in availability if off-chain data.

The paper **"A new key protocol design for cryptocurrency wallet" [9]** talks about the security of cryptocurrency assets depends on owners safeguarding cryptographic keys. Loss or theft of keys has resulted in fund losses. Keys can be safe, lost, leaked or stolen, with certain probabilities for each state. The analysis informs users on optimal wallet design given key fault probabilities. However, the challanges faced that the paper is having too many keys to handle one account it is just an overhead on the user to maintain the keys and also hinders smooth user experience.

"Auto payments via Account Abstraction" [10] is the paper focuses on enabling users to make automatic payments from their non-custodial crypto wallets without sharing their private keys. The user creates an allowed list of merchants and transactions that the smart contract can process autonomously. Moreover, the challanges faced are that, it won't be possible for an external smart contract or off chain application to hold funds or lock them in interest of both sender and receiver.

"Decentralised custodial wallet using Multi-Factor key Derivation Function." [11] is a paper that focuses on the design of a decentralized cryptocurrency wallet that derives keys from multiple authentication factors like passwords, OTPs, hardware tokens, and out-of-band authentication. This allows users to "log in" to their wallet like a centralized service while gaining the security of multi-factor authentication and decentralization. It also highlights the method of account recovery. Moreover, this paper discusses on building a custodial wallet it focuses on decentralising the process by disclosing the private key for multiple logins to other wallets, making the lock funds or control function difficult to implement. The focus is to keep it centralised while making the transaction possible only when user signs.

Proposed Methodology:

The proposed system introduces an innovative approach of employing a variety of machine learning methods, we utilize the DeepAR Algorithm, a specialized feature of Amazon SageMaker. This algorithm is purpose-built for time series forecasting and probabilistic forecasting, making it an ideal tool for our task of predicting blockchain transaction fees. The DeepAR Algorithm offers several advantages that make it a superior choice for our project. Firstly, it is less complex, which simplifies the forecasting process by automatically learning temporal patterns. Secondly, it requires fewer computational resources, which is a significant advantage in terms of efficiency. Lastly, DeepAR has demonstrated superior performance over traditional models in terms of accuracy and speed.

A key component of our project is the development of a custodial wallet. This wallet plays a crucial role in the time-locking of assets, a feature that enhances the security and control of cryptocurrency transactions. When a sender and receiver agree on a time frame for a cryptocurrency transfer, our model, powered by the DeepAR Algorithm, suggests the optimal time and date for the transaction. This suggestion is based on a variety of factors, including historical transaction fee data, network congestion, and market conditions. Once the time and date are agreed upon, the sender's assets are locked using off-chain methods. This ensures the security of the assets during the waiting period. When the agreed time arrives, the assets are automatically transferred to the recipient. This combination of time series forecasting and secure asset management could provide a powerful tool for users of your system, optimizing their transactions while ensuring the security of their assets. It's a forward-thinking application of machine learning and blockchain technology.

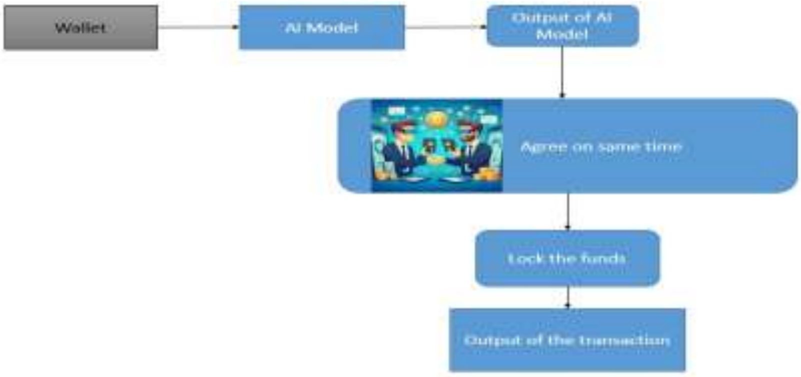

Fig 1 System workflow

Conclusion:

In conclusion, the research undertaken in this study illuminates the intricate and fluctuating nature of gas price forecasting within the Ethereum network. The findings underscore the paramount importance of meticulous data collection and rigorous pre-processing to ensure the accuracy of predictive models. A notable challenge identified is the integration of the DeepAR model into blockchain systems, which requires careful consideration and innovative solutions. Furthermore, the research highlights the significant impact of various network parameters on gas fees, emphasizing the need for a comprehensive understanding of these factors to optimize transaction costs effectively. This study contributes valuable insights into the realm of blockchain transaction efficiency, paving the way for more sustainable and economical cryptocurrency interactions.

REFERENCES:

HARDWARE REQUIREMENTS

- computer with the latest requirements
- Scanner/camera
- Hard Disk : 120 GB
- Monitor : 12” LED
- Input devices : Keyboard, Mouse
- RAM : 8GB

SOFTWARE REQUIREMENTS

- Operating System : Windows 10, 64-bits Operating System
- Coding Language : Python
- Software Tool : Google Colab
- API : Keras,Scikit-learn

Research Papers:

1. Shigeyuki Hamori,"Network Activity and Ethereum Gas Prices" , https://doi.org/10.3390/jrfm16100431

2. Babatomiwa Omonayajo, Auwalu Saleh Mubarak, Fadi AlTurjman, Zubaida Said Ameen, "Ethereum Gas Price Prediction Using Facebook Prophet Model", 2022 International Conference on Artificial Intelligence in Everything (AIE), https://doi.org/10.1109/AIE57029.2022.00093

3. Rawya Mars, Amal Abid, Saoussen Cheikhrouhou, Slim Kallel, "A Machine Learning Approach for Gas Price Prediction in Ethereum Blockchain", 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC), https://doi.org/10.1109/COMPSAC51774.2021.00033

4. Sam M. Werner , Paul J. Pritz, Daniel Peraez, "A Better Approach for Recommending the Ethereum Gas Price" , In proceedings of The 2nd International Conference on Mathematical Research for Blockchain Economy (MARBLE 2020), https://doi.org/10.48550/arXiv.2003.03479

5. ChihYun, Chuang and TingFang Lee, "A Practical and Economical Bayesian Approach to Gas Price Prediction" , The International Conference on Deep Learning, Big Data and Blockchain (Deep-BDB 2021). Deep-BDB 2021, https://doi.org/10.48550/arXiv.2305.00337

6. Md Moniruzzamin, Farida chowdary, Md Sadek Ferdous, "Examining Usability Issues in Blockchain-Based Cryptocurrency Wallets" , http://dx.doi.org/10.1007/978-3-030-52856-0_50

7. Soonwhwa sung , "A new key protocol design for cryptocurrency wallet" , https://doi.org/10.1016/j.icte.2021.08.002 Keywords:Cryptocurrency, walletKey, protocolBlockchain

8. Andrew beams, Ranjit Kumarsean, Mohammed mohsenminaei bidgoli, Mahdi Zamani, Srinivasan Raghuraman,"Autopayments via Account Abstraction" , https://www.tdcommons.org/cgi/viewcontent.cgi?article=6403&context=dpubs_series

9. Vivek Nair, Dawn Song, "Decentralised custodial wallet using Multi-Factor key Derivation Function" , https://arxiv.org/pdf/2306.08168

10. Conall Butler, Martin Crane, "Blockchain Transaction Fee Forecasting : A Comparison of Machine Learning Models" , https://doi.org/10.3390/math11092212