TEX — True Exchange (Decentralized Crypto Currency Exchange for Indian Markets)

Surendra Tripathi1*, Tarun Kotagiri2, P Sanjeeva3, Saurabh Aggarwal4

1Assistant Professor, Department of CSE, KG Reddy College of Engineering & Technology, Hyderabad, Telangana, India
2Student, Department of CSE, KG Reddy College of Engineering & Technology, Hyderabad, Telangana, India
3Associate Professor, Department of Computer Science and Engineering(AIML), GRIET, Bachupally, Hyderabad, Telangana.
4Uttaranchal Institute of Technology, Uttaranchal University, Dehradun, 248007

ABSTRACT: Cryptocurrencies have been gaining popularity in India, but the lack of reliable and safe platforms for trading has been a significant concern. This research paper proposes a decentralized exchange (DEX) platform that enables Indian users to trade cryptocurrencies for Indian Rupees (INR). The system uses the Chainlink decentralized oracle network to convert INR to the equivalent ETH, the base currency for trading on the DEX platform. The proposed platform aims to provide secure and transparent trading to users, ensuring that transactions are executed instantly and at a fair market price. The paper outlines the technical details of the proposed DEX platform, including the integration with Chainlink oracles for price feeds and the development of smart contracts for trading. The platform utilizes the Ethereum blockchain and is built using Solidity, a programming language for smart contracts. Finally, the paper concludes with an evaluation of the proposed DEX platform, highlighting its potential benefits for Indian users and its potential impact on the broader cryptocurrency ecosystem in India. This research paper's findings can guide the development of more secure and reliable DEX platforms in India and beyond.

Keywords — blockchain, cryptocurrency, decentralized exchange, chainlink oracle network, Ethereum, smart contracts, gas optimization

1 INTRODUCTION

Cryptocurrencies have emerged as a popular digital asset form that allows for decentralized and secure transactions without intermediaries such as banks or financial institutions. However, the lack of reliable and safe trading platforms has been a significant concern for users in India, hindering the adoption of cryptocurrencies. Recently, the Indian government has taken a step forward to regulate cryptocurrencies, which can be seen as a sign of increasing crypto adoption in India. To address the issue of reliable and safe trading platforms, this research paper proposes a decentralized exchange (DEX) platform that enables Indian users to trade cryptocurrencies in terms of Indian Rupees (INR). The proposed platform aims to provide secure and transparent trading to users, ensuring that transactions are executed instantly and at a fair market price. The platform utilizes the Ethereum blockchain and is built using Solidity, a programming language for smart contracts. The integration of Chainlink oracles provides reliable and accurate price feeds to the platform, which can convert INR to the equivalent ETH, the base currency for trading on the DEX platform.

*Corresponding Author: sur.svits@gmail.com

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).
2 RELATED WORK

Cryptocurrency trading in India is currently dominated by centralized exchanges that operate as intermediaries between buyers and sellers. These exchanges offer limited support for trading with INR and often need help with payment processing and regulatory compliance.

Centralized exchanges also face security risks such as hacking and theft, as they hold large amounts of users’ funds in centralized wallets. Users have little control over their funds, and the lack of transparency in the trading process can lead to price manipulation and unfair trading practices.[4]

Moreover, the Indian government has been cautious about using cryptocurrencies, and the Reserve Bank of India (RBI) has not given permission to banks and other financial institutions to deal with cryptocurrencies [5]. This has created a regulatory vacuum in the market, with users and traders needing clarification on the legality of trading cryptocurrencies[6].

3 METHODOLOGY

The proposed system is a decentralized exchange (DEX) platform that runs on the Ethereum network and utilizes smart contracts to enable secure and transparent trading of cryptocurrencies. The system architecture is based on Web 3.0 and blockchain technology, which ensures that all transactions are stored in a verifiable and tamper-proof manner without requiring trust.

The platform enables two parties to exchange ERC-20 tokens on the blockchain network using Web 3. The platform is designed to be open, transparent, and secure, with users always in control of their funds. To ensure reliable and accurate price feeds for trading, the platform uses Chainlink decentralized oracle network, which screens through multiple data feeds and aggregates to facilitate the INR to ETH conversion in a decentralized manner, which is the base currency for trading on the DEX platform. The integration of Chainlink oracles ensures that users receive fair market prices and enables seamless trading with INR and other tokens. Group Decision Making is generally described as a best alternative selection process of selection from a given set of feasible options based on the opinions of a group of people or the participating entities frequently referred to as experts [3].

Overall, the proposed DEX platform is a secure, transparent, and decentralized trading platform that utilizes smart contracts and blockchain technology to enable secure and reliable trading of cryptocurrencies. The platform's ability to trade in INR can increase the adoption of cryptocurrencies in India.

The smart contract-based trading system enables instant and transparent trading, with users having complete control over their funds. The proposed platform is tested in a model scenario, successfully exchanging Ethereum on the blockchain test networks (Sepolia, goerli). The study included testing the smart contract on a hardhat network where the security coverage is tested. To optimize the performance of the proposed DEX platform, several gas optimization techniques were implemented and tested on the hardhat network using chai and mocha frameworks.
3.1 SMART CONTRACT

The Transactions contract is written in Solidity with latest version and licensed under MIT standard. It imports the Hardhat Ethereum development environment and contains the following state variables, events, and functions:

**State variables:**

- transactionsCount: an unsigned integer to keep track of the total number of transactions.

**Events:**

- Transfer: an event emitted every time a new transaction is added to the blockchain. It contains the sender's address, receiver's address, transaction amount, message, timestamp, and keyword.

**Storage:**

- Transactions: an array of TransferStruct objects that holds all the transactions added to the blockchain.

**Functions:**

- getConversionRate(): a function that interacts with Chainlink to get the INR conversion rate in ETH.
- addToBlockchain(): a function that adds a new transaction to the blockchain by creating a new TransferStruct object and appending it to the transactions array. This function uses the receiver's address, transaction amount, message, and keyword as input parameters.
- getAllTransactions(): a function that returns an array of all the transactions added to the blockchain.

All functions are set to public visibility. The Chainlink price feed used is TUSD/ETH, and the Chainlink contract address is 0x3886BA987236181D98F2401c507Fb8BeA7871dF2.

3.2 Transaction details

**Fig. 2.** Transaction details of a trade in INR
To enable users to trade in terms of INR, we are utilizing the Chainlink oracle network, specifically the Chainlink Aggregator V3, to convert INR values to ETH. The Chainlink Oracle network is a decentralized system that provides reliable and accurate data for smart contracts. The Chainlink Aggregator V3 is a specific Oracle contract that provides the current market price of a cryptocurrency in terms of another cryptocurrency or fiat currency.

Initiating a transaction in our system involves providing the INR value as input. The Chainlink oracle network is then queried to obtain the current INR conversion rate to ETH. Once the conversion rate is obtained, the INR value is converted to its equivalent ETH value using the conversion rate. The resulting ETH value is then sent to the intended recipient of the transaction.

By utilizing the Chainlink Oracle network, our system can provide a reliable and accurate conversion rate for INR to ETH. This enables Indian users to trade cryptocurrencies in terms of native Indian currency.

3.3 PERFORMANCE OPTIMIZATION

Several gas optimization techniques were implemented in the smart contracts to optimize the proposed DEX platform's performance.

Firstly, immutable and constant variables were used instead of mutable variables wherever possible. This is because mutable variables require more gas to execute as they need to be updated in storage. In contrast, immutable and constant variables are stored in the contract's bytecode and do not require any storage updates.

Secondly, errors were used instead of required statements in some cases. Require statements consume a significant amount of gas, and user errors instead can help reduce the gas cost. For example, if a user tries to perform an invalid action, an error can be returned instead of using a required statement to ensure that the condition is met.

Furthermore, efficient data structures, such as mapping and arrays, were prioritized over more complex data structures, which can be expensive to execute.

Other optimization techniques include minimizing the number of external calls and using off-chain solutions where possible. Additionally, gas prices were monitored to ensure that the gas fees charged to users were reasonable and did not discourage trading activity.

![Smart contract gas report](image)

Fig. 3. Smart contract gas report

3.4 SECURITY TESTING

The smart contract was tested using the MochaJavaScript testing framework and the Chai assertion library. The specific function tested is to add transactions to the blockchain with different sets of parameters and then check if a function to retrieve the transactions correctly retrieved all three transactions and their associated details. A function to get transaction count is tested to retrieve the current transaction count stored in the blockchain successfully. The function to get transactions returns an array of objects containing details of each transaction, including the receiver, amount, message, and keyword.

The test results show that the function in the intelligent contract successfully retrieved all three transactions that were added using another function, and their associated details were correct. The test also confirmed that an intelligent contract function successfully added transactions to the blockchain with the specified parameters.
3.5 FULL COVERAGE TEST

Solidity is a programming language to develop smart contracts on the Ethereum blockchain. Testing intelligent contracts is crucial to ensure they work as intended and are free from bugs and vulnerabilities[22]. Code coverage tools are used to measure the effectiveness of tests by determining the percentage of code covered by the tests.

3.6 Test Description

The smart contract manages financial transactions and includes functions for adding and retrieving transactions. This research paper explores using a code coverage tool, specifically Solidity Coverage, to measure the effectiveness of tests on a smart contract deployed on the Ethereum blockchain. The tests were written using the Mocha JavaScript testing framework and the Chai assertion library. The Solidity Coverage tool was used to generate a code coverage report, which shows the percentage of code covered by the tests [23].

4 Results

The Solidity Coverage tool generated a code coverage report for the smart contract. The report showed that the tests covered 80% of the smart contract functions and statements. This means that all functions and statements in the smart contract were tested at least once, indicating that the tests effectively verified the smart contract's functionality. The code coverage reports also shows that the tests provided coverage for all branches and paths through the smart contract functions, indicating that the tests were comprehensive.

5 CONCLUSION

In conclusion, the proposed decentralized cryptocurrency exchange platform offers a solution to the need for more reliable and safe trading platforms for cryptocurrency users in India. The platform enables users to trade cryptocurrencies in terms of Indian Rupees (INR) and provides a secure, transparent, and fair market for trading. Chainlink's decentralized aggregator price feed ensures that users receive reliable and accurate price feeds for trading. The platform also allows for the trading and swapping custom ERC20 tokens, further enhancing its functionality and utility for users.
The proposed DEX platform has the potential to significantly impact the Indian cryptocurrency market by providing users with a reliable and safe platform for trading. Moreover, its potential benefits, such as the ability to trade in INR and swap custom tokens, make it a valuable addition to the broader cryptocurrency ecosystem. Overall, this research paper comprehensively analyses the proposed DEX platform, highlighting its technical details, security measures, and performance optimization techniques.

The platform's reception by the Indian economy could be significant, as it provides a reliable and safe platform for trading, which has been a significant concern in India's cryptocurrency market. The platform's potential impact on the broader cryptocurrency ecosystem in India must be considered, as it provides a valuable addition to the current infrastructure. The findings of this research can be used to guide the development of more secure and reliable DEX platforms in India and beyond, contributing to the growth and development of the cryptocurrency ecosystem.

REFERENCES