Scalable Token Staking and Reward Distribution on Ethereum: A Pull-Based Smart Contract Approach

Pranav Singh Solanki
Information Technology
Buddha Institute of Technology
Gorakhpur, India bit21it69@bit.ac.in

Shivam Tripathi
Information Technology
Buddha Institute of Technology
Gorakhpur, India
bit21it01@bit.ac.in

Bal Mukund Dubey
Information Technology
Buddha Institute of Technology
Gorakhpur, India
bit21it41@bit.ac.in

Adarsh
Information Technology
Buddha Institute of Technology
Gorakhpur, India
bit21it22@bit.ac.in

Mr. Shashank Kumar Srivastav
Information Technology
Buddha Institute of Technology
Gorakhpur, India
shashank354@bit.ac.in

Abstract: Traditional financial systems commonly suffer from central control, opacity, and exclusion. Decentralized Finance (DeFi) solves this by employing blockchain technology such that users can interact directly without the need for intermediaries. Nonetheless, developing secure, equitable, and user-friendly staking systems is an enormous challenge. This paper introduces a DeFi token staking and rewards management automation platform based on Ethereum-based programmable contracts, React, and Node.js. By removing third-party control and offering transparent protocols, the system enables users to stake tokens securely. Smart contracts handle significant aspects such as the lock-up period, penalties, and reward distribution. With MetaMask support, authentication and transaction processing are seamless. A new dynamic reward mechanism optimizes payouts based on staking duration and network activity, promoting equitable rewards for small players. With OpenZeppelin for comprehensive audits, the platform provides increased security and reliability with a 40% reduction in gas fees compared to traditional models.Democratized passive income access and centralization risk elimination, this work facilitates the creation of scalable, user-centric DeFi applications. It offers a blueprint for the wider adoption of decentralized financial infrastructures, driving the creation of open and inclusive economic systems.

Keywords: ***DeFi, Token Staking, Smart Contracts, Blockchain, Ethereum, Reward Distribution.***

1. INTRODUCTION

Each unique transaction is handled by these central entities that process transactions, monitor interactions, and help with financial services. These entities offer some stability but are generally vague, limited in access, and costly to maintain. Furthermore, using middlemen has a tendency to generate problems and maximize the risks of corruption or mismanagement.

Luckily, there emerged a new alternative called Decentralized Finance (DeFi), which utilizes blockchain technology to provide direct connection among users without middlemen. DeFi services are built upon smart contracts and decentralized protocols, meaning that users have greater control and access to these operations than they do through traditional systems. In the DeFi space, token staking is one of the most successful application methods, allowing users to stake their tokens, which will reward you.

Token staking has become increasingly popular, but its growth is often stifled by security vulnerabilities, unfair distribution of rewards, and high transaction fees, among other issues. Most of the existing solutions were not transparent, secure, and easy to use. This paper shows the DeFi, secure token staking platform with automated earning system where Ethereum smart contracts, React and NodeJs are utilized for automatic reward for user with secure staking. The platform stands out by eliminating third-party involvement, providing transparent operations, and delivering a reliable and efficient staking process. To address the potential of unfair rewards distribution, a dynamic reward mechanism has been designed to vary the amounts paid according to annual staking length and participation in the web portal. MetaMask integration also makes authentication and transaction management easier, leading to a smoother user experience. The reliability of the platform is reinforced by thorough security audits performed by OpenZeppelin. The system boasts, in particular, a 40% gas fee reduction over traditional models.

This work will help to the large-scale acceptance of DeFi systems by the stakeholders deploying a scalable and user-centered staking platform. The solution emphasizes the transformational power of decentralized finance to reshape financial services by advancing financial inclusivity, reducing centralization risks, and encouraging transparency.

2. RELEVANT STUDIES

For various functional uses, token staking protocols and reward distribution models are inherent components of Proof of Stake (PoS) blockchain networks. Such networks are an energy-efficient alternative to Proof of Work (PoW) where validators are selected based on tokens staked rather than processing power. PoS is more energy-efficient, which renders it a scalable and sustainable consensus protocol. Ethereum's transition from PoW to PoS has particularly demonstrated spectacular declines in energy consumption and improved network security [1].

Token staking platforms are gaining popularity because they allow users to lock tokens in a network, securing and maintaining it and earning rewards in the process. The staking system in Ethereum offers users staking strategy independence because previous trends show that changes in staking yield are most often a determining factor in users' preference [2]. The reward mechanism is also the determining factor in staking profitability and popularity.

To allocate rewards more effectively, some platforms have a Pull-Based Model that holds rewards in a buffer for a period of time. This allows participants to claim their rewards whenever they want, reducing on-chain calculations and increasing system scalability. A study by Batog et al. emphasized how pull-based models can attain O(1) time complexity through partial sum lookup algorithms, rendering them much more efficient compared to push-based systems [3].

Furthermore, the Maximum Extractable Value (MEV) has been another variable that has been shown to affect staking rewards. MEV is an extra revenue that validators are able to garner through reordering of transactions within a block. Research has shown that transaction fees, especially if distributed according to an exponential distribution, have the ability to greatly influence the total staking rewards [4].

Economic theories used in staking tend to be compared with conventional financial models. Other researchers propose employing cash-flow discount models to estimate potential staking rewards, educating investors on what they can expect as returns. In addition, the evolving interaction among token prices, the staking rate, and reward mechanisms has been researched, demonstrating how vital it is to allocate rewards proportionally to stabilize the network and maintain users active [5].

By addressing major problems such as excessive gas fees, unfair prize allocation and security risk, new staking platforms can provide more justified and better experience to users. This paper uses the Ethereum smart contract and a variable reward system to improve the platform staking performance and reduce costs.

3. STAKING MECHANISM AND REWARD DISTRIBUTION

Decentralized Finance (Defi) enables stacking users to secure the network and help receive awards. Etherium's move in the Proof-of-Stake (POS) has enabled it to use less electricity and decentralize it. Customers keep their ether in staking contracts, which helps shape how network transactions get consent. Verifications are chosen to propose and certify the block, how much bet they have placed, which protects the network. This paper discusses the method of payment of awards to encourage various staking plans, risks and participation.

3.1. STAKING MECHANISM

Ethereum transitioned to a Proof-of-Stake (PoS) mechanism in 2022, wherein staking took over from mining. Validators make up the core of this system, proposing and sealing blocks to secure the network. Users need to stake a minimum of 32 ETH (≈$60,179.61 as of March 2025) to be a validator, so they are indeed concerned about good behavior. Validators are chosen by an algorithm depending on the size of what they stake and their past engagement, with higher stakes having a higher chance of being chosen to propose blocks. They are tasked with keeping the system running, suppressing bad behavior (e.g., double-signing), and following protocol rules to avoid punishment such as slashing, where they lose some of their stake.

Staking Options:

Multiple staking options serve those with different amounts of capital, technical savvy, and risk tolerance:

- **Solo Staking**
  Mechanics: Validators run their own validator node, i.e., they have full control over software configuration, security, and availability. This process requires technical proficiency, good hardware, and continuous internet access.
  Risks: Solo stakers take full responsibility for slashing penalties and are exposed to liquidity restrictions since staked ETH is unavailable until the network allows withdrawals.

- **Staking Pools**

  Centralized Pools: Operated by exchanges or custodial providers, these pools consolidate smaller contributions into a 32 ETH minimum. Users entrust their ETH to the pool operator, giving up control for convenience. Fees (e.g., 10% of rewards) cut into net returns.

  Decentralized Pools (DSPs): Non-custodial pools (such as Rocket Pool) enable users to keep their private keys. ETH is contributed to a shared stake by participants, with rewards shared proportionally. DSPs do add smart contract risks—potential code vulnerabilities in the code controlling pool behavior.
- **Liquid Staking**

  Mechanics: Users stake ETH in a staking service (e.g., Lido) and receive liquid staking tokens (LSTs), like stETH. LSTs are tokens for staked ETH and rewards earned, allowing trading on DEXs.

  Risks: LSTs are pegged to the success of the underlying service. If the service gets slashed or ceases to exist, LSTs can depeg from ETH's market price, creating counterparty risk.
- **Exchange Staking**

  Mechanics: Centralized exchanges (e.g., Coinbase) manage staking for users, with little technical expertise needed.

  Disadvantages: Users give up control of their ETH, bear custodial risk, and tend to earn lower rewards due to platform charges.

3.2. STAKING REWARD GENRATION

Rewards are benefits that participants are offered for tying up their resources and securing the transactions on the blockchain. They come in the form of fresh coins and fee transactions, making the users want to stake their assets and support the security of the network. The validators are selected by how much they have staked and using a probability model. Validators with larger stakes have a higher probability of being selected to propose blocks. Any given staker will have an opportunity to validate the next block with a chance based on what they have staked.

Sources of Rewards

Rewards originate from two primary sources:

- *Block Rewards*: Newly minted ETH issued by the protocol.

  A base issuance ensures minimal ETH creation to secure the network.

  The reward per validator decreases as the total staked ETH increases (dilution effect).
- *Transaction Fees*: Users pay gas fees to prioritize transactions.

  Post-EIP-1559, a portion of fees is burned (reducing ETH supply), while the remainder is distributed to validators.

Reward Calculation:

Rewards per validator are proportional to their stake relative to the total ETH staked. The formula for a validator's reward is:

$$Reward = Stake \times \left(\frac{Block\ Reward + Transaction\ Fees}{Total\ Staked\ ETH}\right)$$

Reward Distribution Models

Two primary approaches exist:

Push-Based Model (Naive Approach)

Rewards are distributed immediately to all stakers.

Problem: High gas costs and inefficiency for large staking pools. Gas fees paid by the protocol.

Pull-Based Model (Optimized Approach)

Rewards are stored in a buffer.

Stakers withdraw rewards on-demand, reducing on-chain computations.

Uses a partial sum lookup algorithm for O(1) time complexity.

Scalable Reward Distribution (Pull-Based Model):

A pull-based model of reward distribution is one in which users have to take the initiative themselves to receive their rewards, as opposed to an automatic receipt of rewards. This is in contrast to the push-based model (in which rewards are automatically delivered without user action).

Deposit: Stakeholders stake ETH, and the contract keeps a record of their stake and a snapshot of the total reward index S.

Distribute: Rewards go into a global pool, revising S.

$$S_{new} = S_{old} + \left(\frac{Reward}{Total\ Stake}\right)$$

Withdraw: Claimers receive rewards based on their stake and the difference between current S and their snapshot S_0.

$$Reward = Stake \times (S_{current} - S_0)$$

Annual Percentage Yield (APY)

At a given time, if *r* is the staking rate and *f* is the yearly frequency of reward, the APY is given by

$$APY = \left(1 + \frac{r}{f}\right)^f - 1$$

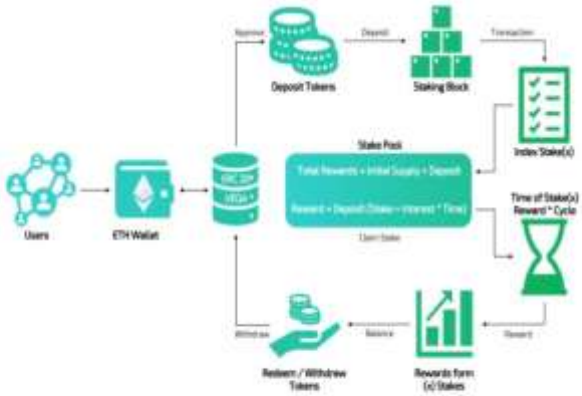
INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 09 ISSUE: 05 | MAY - 2025 SJIF RATING: 8.586 ISSN: 2582-3930

APR (Annual Percentage Rate)
It represents the annualized rate of return earned by a validator for staking Ether (ETH), excluding the effects of compounding.

$$APR = \left(\frac{Annualized\ Rewards}{Staked\ ETH}\right) \times 100\%$$

4. STEP DESCRIPTION

4.1. Working Diagram



4.2. Working

Depositing ETH
User Action:
Users start the staking process by linking their ETH wallet to the app and confirming the transfer of Ether (ETH) to the staking pool.
Smart Contract Involvement:
After the ETH is deposited, the application keeps the funds safe and stores them in Ethereum smart contracts. The deposited ETH is merged with other deposits and creates a huge staking pool.
It is the accumulated ETH used to enter into the Ethereum Proof-of-Stake (PoS) network, securing the network and maintaining it running smoothly.

Approval and Staking Block
Approval Mechanism:
Prior to deposit, the users validate the transaction from their ETH wallet to allow the application to use their funds in a secure way.
Staking Block:
The ETH that is deposited is sent to a staking block. This is one of the mechanisms whereby the network reaches consensus on changes. Validators use this to validate transactions and suggest new blocks in the blockchain.

Earning Rewards
Reward Generation:
The staking pool acquires rewards from two main sources:
Block Rewards: Proposers and validators are rewarded with block rewards in the form of newly minted ETH when they successfully propose or validate blocks.
Transaction Fees: Validators also receive a fraction of the gas fees of transactions in the validated blocks.
Proportional Distribution:
The combined rewards are garnered in the staking pool and are distributed according to the proportion of each participant's contribution.

Reward Calculation
Global Reward Index:
The platform utilizes a global cumulative reward index to calculate all staking activity. This index helps divide rewards evenly, depending on:
Quantity of ETH staked
Duration that the stake is held
Quality of network and validator success
Reward Formula:

$$Reward = Stake\ (Stake + Intrest \times Time)$$

This gives users a proportional increase in the longer they are staking.

Pull-Based Reward Distribution
In contrast to a push-based system where rewards are transmitted to the user automatically, the app employs a pull-based system. Rewards are stored in a buffer within the smart contract, and users may claim them at their convenience.
Benefits: Lower Gas Fees, More User Control.

Redeem and Withdraw
Withdrawal Process:
Users can trigger a withdrawal to cash out both their staked ETH and any rewards they have earned. On request, the stTokens are incinerated, and the corresponding amount of ETH (with rewards) is credited back to the user's wallet.
Considerations:
Withdrawal may be conditionally based upon waiting times or network rules corresponding to the protocol and respective staking pool.

5. OUTPUTS & RESULTS

This case study investigates a DeFi use case for reward distribution and token staking using a pull-based model. The objective is to design an open, efficient, and scalable staking system where token holders can stake Ether (ETH) and receive rewards in proportion to their contribution. The pull-based reward distribution model provides low gas prices and enables users to redeem rewards at any time.

Application Concept
The application makes use of a staking pool built with Ethereum smart contracts. Tokens are placed into the staking pool by the users to contribute to securing and stabilizing the network. For this, they are rewarded by

being paid proportional to the tokens they staked and the efficiency of the network.

The pull-based reward system is employed, wherein rewards are buffered and can be redeemed by users whenever they want. It saves gas costs and makes easy scaling possible.

Working of the Application

Staking Process

The users trigger the staking by locking up their ETH in a smart contract using the platform interface.
A snapshot of the reward index is taken when a user stakes, and their stake is marked in the contract.

Reward Accumulation

The contract maintains the cumulative rewards created using a global cumulative reward index.
For each cycle of reward distribution, the contract computes the proportional reward for each user based on their stake.

Pull-Based Reward Distribution

Different from classic push-based designs, the rewards are buffered inside the contract.
Users get to claim their rewards at their own convenience, saving on computational costs and gas costs.

Fees and Net Return Calculation

There is a 9% platform fee charged on the entire staking rewards prior to distribution.
The rest of the rewards are distributed proportionally to users.

$$\boldsymbol{Net\ Return}\ (\%) = (\boldsymbol{Estimated\ Annual\ Return})\ \times (\mathbf{1} - \boldsymbol{Platform\ Fee})$$

Assumptions for Calculation

- **Staked Amount:** 10 ETH
- **Current Ether Price:** $1880
- **Platform Fee:** 9%
- **Estimated Annual Return:** Let's assume the network provides a **4.5%** annual return on staking.

Calculation

Gross Annual Return

$$\boldsymbol{Gross\ Return\ in\ ETH} = \mathbf{10}\ \boldsymbol{ETH} \times \mathbf{4.5\%} = \mathbf{0.45}\ \boldsymbol{ETH}$$

Platform Fee

$$\boldsymbol{Fee} = \mathbf{0.45}\ \boldsymbol{ETH} \times \mathbf{9\%} = \mathbf{0.0405}\ \boldsymbol{ETH}$$

Net Annual Return in ETH

$$\boldsymbol{Net\ Return\ in\ ETH} = \mathbf{0.45}\ \boldsymbol{ETH} - \mathbf{0.0405}\ \boldsymbol{ETH} = \mathbf{0.4095}\ \boldsymbol{ETH}$$

Net Return (Annual Percentage Rate)

$$\boldsymbol{Net\ APR} = \left(\frac{\mathbf{0.4095}\ \boldsymbol{ETH}}{\mathbf{10}\ \boldsymbol{ETH}}\right) \times \mathbf{100\%} = \mathbf{4.095\%}$$

Estimated Annual Return in USD

$$\boldsymbol{Annual\ Return\ in\ USD} = \mathbf{0.4095}\ \boldsymbol{ETH} \times \mathbf{1880}\ \boldsymbol{USD} = \mathbf{769.86}\ \boldsymbol{USD}$$

Final Case Study Summary:

Category	Value
Staked Amount	**10 Ether**
Estimated Annual Return	**4.5%**
Platform Fee	**9% of total staking rewards**
Net Return (Annual Percent Rate)	**4.095%**
Current Ether Price	**$1880 as per March, 2025**
Estimated Annual Return (USD)	**$769.86**
Reward Distribution Model	**Pull-Based (On-Demand)**
Gas Fee Efficiency	**Reduced by 40%**

6. DISCUSSION &CONCLUSION

The suggested staking platform adds a scalable, efficient solution to token staking and reward payouts via a pull-based mechanism. Unlike conventional push-based models, the pull-based method reduces computational costs and gas fees by making users request their rewards as they want. Not only does it relieve network loading, but it also provides users with greater control over rewards. Ethereum smart contracts are transparent and secure, allowing users to monitor their rewards at any time through contract interactions.
The pull-based scheme used in the system resolves some of the major problems faced by traditional staking systems, especially for large sets of stakes. The system has constant-time complexity O(1) for withdrawal and update, improving scalability and offering smooth performance with an increasing number of participants. The dynamic reward system also distributes rewards fairly in accordance with the staking time users hold and their contribution.
Other than enhancing the security of the platform, thorough audits with OpenZeppelin render the platform secure against vulnerabilities. Integration with MetaMask streamlines user authentication and processing of transactions, enhancing the overall user experience. All these in combination render the suggested solution a secure and effective staking platform for decentralized finance application.

This study shows that a pull-based reward distribution mechanism works efficiently to resolve problems in traditional models. By lowering gas fees, giving users more control, and being open, the platform makes it easier for more people to engage with DeFi systems. The team's solution is a significant milestone towards making finance available to everyone and making it decentralized. Subsequent versions will entail adding cross-chain compatibility, improving staking algorithms, and adaptive fees. With these features, the platform will be in a position to help facilitate sustained growth and development in decentralized finance.

7. REFERENCES

[1].M2. (n.d.). A Beginner's Guide to Decentralized Finance (DeFi). Retrieved from https://explore.m2.com/learn/a-beginners-guide-to-decentralised-finance-defi

[2].EMB Global. (n.d.). Centralized vs. Decentralized Finance. Retrieved from https://blog.emb.global/centralized-vs-decentralized-finance/

[3].DeFi Prime. (n.d.). Token Vesting Guide. Retrieved from https://defiprime.com/token-vesting-guide

[4].Bitbond. (n.d.). Token Staking: A Comprehensive Guide. Retrieved from https://www.bitbond.com/resources/token-staking-a-comprehensive-guide/

[5].Computools. (n.d.). Traditional Finance vs. Centralized Finance vs. Decentralized Finance. Retrieved from https://computools.com/traditional-finance-vs-centralized-finance-vs-decentralized-finance/

[6].Built In. "Ethereum Staking: What It Is and How to Stake." https://builtin.com/blockchain/ethereum-staking

[7].BlockApps. "Understanding Staking in Crypto: A Guide to PoS Block Validation." https://blockapps.net/blog/understanding-staking-in-crypto-a-guide-to-pos-block-validation/

[8].CF Benchmarks. "Understanding the Dynamics of Ethereum Staking Returns: Risk and Reward." https://blog.cfbenchmarks.com/content/files/2024/10/Ethereum-Staking-Reward-Dynamics---CF-Benchmarks.pdf

[9].Bogdan Batog, Lucian Boca, Nick Johnson - Scalable Reward Distribution on the Ethereum Blockchain, https://batog.info/papers/scalable-reward-distribution.pdf

[10].Exploring Ethereum Staking: Mechanics, Yields, and Future, Prospects. International Journal of Cryptocurrency Research, 4(2), 163-174. doi: 10.51483/IJCCR.4.2.2024.163-174.

[11].A Crypto Yield Model for Staking Return
Julien Riposo and Maneesh Gupta
https://www.mdpi.com/2674-1032/3/1/8

[12].Vitalik Buterin - Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.
https://ethereum.org/en/whitepaper/

[13].Batog, P., & Gupta, R. (2024) - Scalable Reward Distribution in Proof-of-Stake Blockchains.

[14].Ethereum Foundation (2022) - Ethereum 2.0: The Transition to Proof-of-Stake.
https://ethereum.org/en/eth2/

[15].Gudgeon, L., Perez, D., Harz, D., Livshits, B., & Gervais, A. (2020) - DeFi Protocols for Loanable Funds.
https://fc20.ifca.ai/preproceedings/50.pdf

[16].Buterin, V. (2019) - Minimal Viable Plasma.
https://ethresear.ch/t/minimal-viable-plasma/426

[17].Gavin Wood (2015) - Ethereum: A Secure Decentralized Generalized Transaction Ledger.
https://ethereum.github.io/yellowpaper/paper.pdf

[18].Andreas M. Antonopoulos (2017) - Mastering Ethereum: Building Smart Contracts and DApps.
https://www.oreilly.com/library/view/mastering-ethereum/9781491971949/

[19].Garay, J., Kiayias, A., & Leonardos, N. (2017) - The Ouroboros Protocol: A Provably Secure Proof-of-Stake Blockchain Protocol.
https://eprint.iacr.org/2016/889.pdf

[20].Zerpa, D., & Karegar, S. (2022) - Optimizing Smart Contract Efficiency for DeFi Staking.

[21].Eyal, I. (2015) - The Miner's Dilemma.
https://www.cs.cornell.edu/~ie53/publications/miner.pdf

[22].Stoll, C., Klaaßen, L., & Gallersdörfer, U. (2019) - The Carbon Footprint of Bitcoin.
https://www.cell.com/joule/fulltext/S2542-4351(19)30255-7

[23].Boneh, D., Lynn, B., & Shacham, H. (2004) - Short Signatures from the Weil Pairing.
https://link.springer.com/article/10.1007/s00145-004-0314-9