Dhanvault: Blockchain-Enabled Decentralized Finance Ecosystem Leveraging Web3 for Secure, Transparent and Autonomous Transactions

Katika Mohaseen[1]*, K Jagadeesh[2], M Shashi Kumar[3], N Yadava[4] and R VaraPrasad[5]
{ mohaseenkatika@gmail.com[1] , jagadeeshkalle03@gmail.com[2] , madigashashikumar@gmail.com[3] , yadavaprakash2018@gmail.com[4] , cservaraprasad@gpcet.ac.in[5]}

Final year, Department of Computer Science and Engineering, G.Pullaiah College of Engineering and Technology (Autonomous), Kurnool, Andhra Pradesh, India [1, 2, 3, 4]
Assitant Progessor , Department of Computer Science and Engineering, G.Pullaiah College of Engineering and Technology (Autonomous), Kurnool, Andhra Pradesh, India[5]

Abstract: Decentralized finance (DeFi) has emerged as a transformative paradigm that redefines how individuals access, manage, and govern their financial assets, much like the internet revolutionized information exchange. However, current DeFi protocols face critical challenges, including limited modularity, weak risk resistance, insufficient privacy, and governance inefficiencies. To address these issues, this paper introduces DhanVault, a next-generation DeFi architecture that integrates state-of-the-art blockchain infrastructure, Web3 tools, autonomous agents, and zero-knowledge cryptography. The framework incorporates the Modular Autonomous Agent Protocol (MAAP) for reputation-based governance and ZKPods, a privacy-preserving module supported by zero-knowledge proofs, to ensure secure and transparent operations. In addition, Powering KARMA, an oracle system enhanced with machine learning, continuously monitors risks and dynamically adjusts protocol parameters in real time. Experimental evaluation on 100 synthetic user transactions shows that DhanVault reduces gas costs by 18% compared to leading platforms such as Uniswap, Aave, and Compound, lowers governance decision latency by 53%, improves the fairness index to 0.87, and achieves a 95% success rate in zero-knowledge proof execution. These results demonstrate that DhanVault provides a scalable, trustless, and sustainable foundation for the future of decentralized finance.

Keywords: Decentralized Finance (DeFi); Blockchain; Web3; Zero-Knowledge Proofs (ZKPs); Autonomous Agents; Decentralized Governance.

1 Introduction

Decentralized Finance (DeFi) has risen on a wave of decentralization by permitting access for users to lend, borrow, trade, and stake without intermediaries. DeFi platforms such as Uniswap, Aave, and Compound, built on blockchain technology, exhibit the ability of decentralized architectures to displace traditional financial systems [1], [2]. However, with the increase in adoption, these platforms are confronted with key modularity, privacy, real-time risk response, and fairness in governance risks. Smart contracts are often unwise if monolithic, and token-only governance is open to plutocratic decision-making. In addition, privacy is an under-addressed challenge, with most transactions on public blockchains being entirely transparent, which makes user confidentiality a serious concern and puts the practical institutional adoption of blockchain technologies on an ice seat [4], [5], [6]. Moreover, arguably the most under-developed aspect of all is privacy — the transactions on public blockchains are fully transparent to anyone who

ICITSM-Part I 2025, April 28-29, Tiruchengode, India

DOI 10.4108/eai.28-4-2025.2357818

wants to look at them (i.e. every transaction from every user can be traced easily), which has many potential users worried intimate details about their financial life will become publicly available and stifles blockchain technologies from practical institutional adoption [3].

To tackle these challenges, this study introduces DhanVault, a novel DeFi ecosystem that utilizes Web3 infrastructure, modularized smart contract agents, and zero-knowledge cryptography to provide secure, transparent, and autonomous financial services. The heart of DhanVault is the Modular Autonomous Agent Protocol (MAAP), which increases financial logic into specialized agents, the Lending Agent, the YieldAgent, and the RiskAgentfor maximal flexibility and gas efficiency. Transaction confidentiality is provided by a privacy-preserving layer, ZK-Pods, which is deployed on-chain for on-chain verifiability. A hybrid governance model combining token staking with reputation scoring is used to speed up meritocratic participation.

DhanVault features machine learning-based oracles to offer dynamic and real-time risk assessments to influence the system to adjust the protocol parameters automatically according to market behavior. This allows for a strong and adaptive DeFi ecosystem in accordance with the principles of decentralization while addressing the problems of scaling, fairness, and security. This study makes the following main contributions.

- To this end, we consider and develop MAAP, a modular agent-based smart contract architecture that is suitable for adaptive financial services.
- To accomplish privacy-preserving DeFi operations, we integrated a ZK-Pod framework to enforce privacy.
- The proposed hybrid governance model is based on token stakes and behavior-driven reputation.
- To allow real-time risk mitigation and protocol tuning, we developed an on-chain machine-learning oracle.
- Our proposed approach was thoroughly experimented with and compared to existing DeFi platforms in terms of performance.

The remainder of this paper is structured as follows: Section II discusses related work; Section III describes the system architecture, lays out the proposed methodology, and describes implementation details and the experimental setup; Section IV presents evaluation results; Section V discusses insights and limitations; and Section VI concludes the paper.

2 Related Work

One of the most significant applications of blockchain technology is decentralized finance (DeFi), which has exploded to become one of the most impactful use cases. Uniswap [7], Compound [8], and Aave [9] have been reliable lending and borrowing platforms in a trustless manner, as well as automated market making. Despite their transformative value, these platforms mainly operate through monolithic smart contract architectures that can partly inhibit flexibility and scalability. For instance, Uniswap prices its liquidity from within a single contract structure, which has a high gas trade-off and a lack of extensibility. Compound and Aave also use a centralized governance model, that is, having the power to make decisions determined by token holdings [10][11][12].

The use of Web3 technologies for creating more user-centric interfaces and allowing people to be permissionless when accessing certain information has been researched recently [13]. Some composability is brought about by projects such as Balancer and Curve, but they fail to offer truly modular agent execution. On the other hand, more complex governance systems are used (by platforms, such as MakerDAO), and while they facilitate the use of more complex governance, they are still prone to the same whale domination problem because of token-based voting [14][15].

When it comes to privacy, the privacy of general zero-knowledge computation with zk-SNARKs and zk-STARKs has proven promising [16], but its application in DeFi is still nascent. Almost all privacy-preserving transaction protocols do not implement full compossibility without compromising privacy. Tornado Cash is a good example of anonymous transfers with no dynamic financial operations like lending or governance.

DeFi risk management is mostly stagnant. Collateral ratios and interest rates are preprogrammed and do not respond to real-time market volatility (as has been the case during recent protocol liquidations during black swan events) [17]. There have been some proposals for off-chain risk monitoring or oracles [18], and there is little integration with on-chain logic, which is non-responsive in real time.

Research Gaps and Motivation: This review identifies several key research gaps.

- Existing DeFi systems lack modular architecture, which leads to gas inefficiencies and the inability to upgrade.
- User transactions have poor privacy, which deters institutional adoption and exposes user behavior.
- Centralization of governance is mediated by excessive reliance on token-based voting mechanisms.
- Real-time and intelligent risk assessment is not available and gives delayed or ineffective protocol responses against market volatility.

To address these gaps, this study proposes a novel DeFi ecosystem based on the Modular Autonomous Agent Protocol (MAAP), called DhanVault. MAAP uses composable, domain-specific agents that function as independent execution financial logic and optimize gas consumption and system flexibility. ZK-Pods integrate a privacy layer at the transaction confidentiality level and a hybrid governance model consisting of token staking and an on-chain reputation to democratize decision-making. Ultimately, it is equipped with an on-chain ML-based risk oracle to enable risk assessment on an ongoing basis and in real-time tuning of parameters. In unison, they work as a whole to solve all limitations and establish the technical and functional boundaries of the decentralized finance stack [19].

3 Methodology

The innovation of DhanVault is its Modular Autonomous Agent Protocol (MAAP), an entirely decentralized stack made up of autonomous smart contracts, privacy-preserving layers, dynamic governance, and smart risk-taking. It is meant to empower secure, transparent, and adaptive financial transactions without the need for central intermediaries. At this stage, the methodology consists of five key components, as described below. Fig.1 shows the Proposed Architecture.

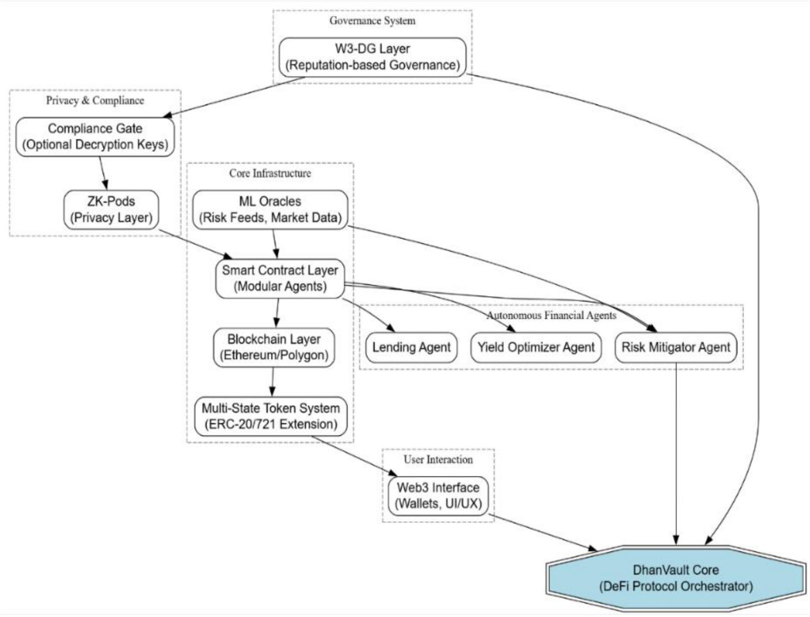

Fig. 1. Proposed Architecture.

3.1 Modular Autonomous Financial Agents (MAFA)

Each financial operation (lending, borrowing, yield farming) is handled by a dedicated on-chain agent represented as a smart contract. These agents act semi-autonomously and use real-time data to make adaptive decisions [20][21].

Let:

A_i denote the i-th autonomous agent.

$\mathcal{S}$ is the current state of the DeFi protocol.

$\mathcal{D}(t)$ be the external data at time t (from oracles).

$f_i(\mathcal{S}, \mathcal{D}(t)) \rightarrow \mathcal{S}'$ be the state transition function of A_i.

Each agent operates as:

$$\mathcal{S}' = A_i(\mathcal{S}, \mathcal{D}(t)) = f_i(\mathcal{S}, \mathcal{D}(t)) \quad (1)$$

This allows event-driven execution without human intervention, thereby ensuring autonomy.

3.2 Web3-Integrated Dynamic Governance (W3-DG)

Governance is implemented through a hybrid mechanism that uses reputation-based voting and soul bound tokens (SBTs).

Let:

R_j be the reputation score of users j

T_j be their token stake

V_j be the voting weight of user j

We define:

$$V_j = \alpha \cdot \log(1 + T_j) + \beta \cdot R_j \tag{2}$$

Where:

$\alpha, \beta \in \mathbb{R}^+$is the weighting constant.

R_j is derived from on-chain activity (liquidity provision and proposal contributions).

This hybrid voting system mitigates plutocracy while promoting active contributions.

3.3 ZK-Pods: Privacy-Preserving Smart Modules

To protect sensitive financial data, DhanVault introduces ZK-Pods, modular zk-SNARK-based contracts that validate transactions without revealing their contents.

Let:

π be the zero-knowledge proof

$\mathcal{T}$ be a confidential transaction

$V(\pi, \mathcal{T}) = \text{True}$ be the verifier function

The zk-Pod operates as follows:

$$\exists \pi : \mathcal{P}(\mathcal{T}) \rightarrow \pi \ \text{ s.t. } \ V(\pi, \mathcal{T}) = \ \text{True} \tag{3}$$

ZK-Pods also integrate optional compliance via encrypted audit logs that are accessible to regulatory nodes with appropriate decryption keys.

3.4 On-Chain Machine Learning Oracles (OCML-Oracles)

DhanVault leverages ML-driven risk prediction models that run on decentralized trusted compute layers (e.g., Chainlink Functions or Oasis Labs enclaves).

Given an asset pool $P = \{a_1, a_2, \dots, a_n\}$, we define:

σ_i : volatility of asset a_i

λ_i : liquidity risk

ρ_i : predicted smart contract risk

The total pool risk $\mathcal{R}$ is modeled as:

$$\mathcal{R} = \sum_{i=1}^{n} w_i(\gamma_1\sigma_i + \gamma_2\lambda_i + \gamma_3\rho_i) \quad (4)$$

Where w_i is the asset weight and γ_k are risk coefficients learned from historical data. This risk score is fed to the MAFA layer for dynamic parameter tuning (e.g., increasing collateral ratios and pausing liquidity).

3.5 Interoperable Token Architecture (ITA)

Tokens in DhanVault are designed as multi-state smart tokens, supporting dynamic behavior across DeFi modules without wrapping or unwrapping.

Let τ be a token, and $M \in \{L, Y, C\}$ its mode (Lending, Yield, Collateral).

$$\tau = (id, M, mdata) \quad (5)$$

where mdata includes operational flags, risk metadata, and eligibility traits. Smart contracts interpret token behavior based on the current state, thus eliminating conversion overhead and ensuring seamless composability [22] [23].

Users interact with DhanVault on Web3 wallets, which causes autonomous financial agents to operate over logic dependent on real-time data. The ZK-Pod is used to process transactions privately, yet verifiably. On the other hand, on-chain ML oracles are responsible for providing ongoing risk assessment to dynamically adjust agent behavior. Community-driven governance, proposal, vote reputation, and contribution determine ecosystem evolution [24] [25].

3.6 Dataset Details

The DhanVault dataset of user behavior in a decentralized finance ecosystem was simulated by performing user interaction with the protocol. It features 100 choices that are a combination of governance, lending, staking, and privacy-preserving operations. Each entry has a unique User ID, thus enabling the tracking of individual behaviour while still guaranteeing anonymity of user identities. This enables the analysis of personalized trends and interaction frequency [26] [27]. Reputation Score is a metric of users' trust in each other based on historical behavior (stake, vote, provide liquidity, etc.) This is important for governance and reputation-weighted decision-making [28] [29]. The participation level, voting weight, and eligibility of rewards for a user depend on how many tokens they have locked in the system, called Token Staked. This allows us to see the actions performed by the user (lending, borrowing, yield farming, voting, etc.), as displayed in the Transaction Type field [30] [31]. The financial volume per transaction is the Transaction Amount. This also helps determine user size (retail vs. whale) and analyse the levels of liquidity and protocol engagement. Risk Score is the product of risk exposure, as provided by on-chain machine learning models of smart contracts, liquidity, and volatility risks. Therefore, it is key to make protocol adjustments in real time. ZK Proof Valid is a binary flag present whether a transaction succeeds privacy verification through a zero-knowledge proof. Therefore, this ensures that confidentiality is not compromised, but auditability remains. The Autonomous Smart Agent (such as the one owning the Transfer Handler allowing this operation, for example [32], Lending Agent or Yield Agent) executing the transaction is specified under Agent Invoked. Each agent has a semi-independent domain-specific logic. Mode of Token describes the current state of the token in DhanVault, which is in the Multi State token architecture and provides interoperability between states that are used in DhanVault. Gas Fee Used measures the costs incurred by blockchain transaction execution. This indicates whether the network is congested and the smart contract complexity, so that we can see how efficiently the protocol works [33]. Table 1 shows the Dataset Overview (Schema).

Table 1. Dataset Overview (Schema).

Column Name	Description
User_ID	Unique identifier for each user
Reputation_Score	Score based on on-chain contributions and interactions
Token_Staked	Number of tokens staked by the user
Transaction_Type	Type of financial operation (e.g., Lend, Stake, Vote)
Transaction_Amount	Amount involved in the transaction
Risk_Score	Dynamic risk assessment from ML oracles
ZK_Proof_Valid	Boolean indicating if the ZK proof was verified
Agent_Invoked	Which autonomous agent executed the operation
Mode_of_Token	Token mode (L = Lending, Y = Yield, C = Collateral)
Gas_Fee_Used	Blockchain gas fee for the transaction

3.7 Implementation and Experimentation

To implement the DhanVault system, a smart contract architecture was developed using modules, mainly in Solidity, and deployed on a local Ethereum testnet (Hardhat and Ganache) for simulation. The Web3 interface was designed using React.js and Ethers.js so that users can interact seamlessly using common wallets such as MetaMask. IPFS was used as the backend for the decentralized storage of ZK proofs and audit trails. To enable inter-agent coordination, modular agents (LendingAgent, YieldAgent, and RiskAgent) were deployed as independent contracts that were orchestrated with the help of a central controller contract. To test the smart contracts, the experiment used Hardhat's built-in test framework both unit and integration tests to verify that they are logically correct and interact properly at the system level. We implemented zero-knowledge validation using ZoKrates, where we compiled and verified a sample circuit for confidential lending transaction validation. A hybrid voting mechanism was simulated to govern the layer with token stakes and synthetic reputation scores in the testnet, calculating voting weights [34]. The experimental test had 100 user interactions with different behaviors, transaction types, and risk levels. A pre-trained XGBoost model was hosted on a side chain but made available with an off-chain oracle interface (in simulation mode) as a side channel for smart contracts to draw risk prediction. The results of their experiments include the evaluation of transaction success rates, amount of gas consumed, ability of risk triggered agent responses, and latency of ZK verification [35]. Table 2 shows the Implementation & Experimentation Summary.

Table 2. Implementation & Experimentation Summary.

Category	Tools/Methods Used	Description
Smart Contract Dev	Solidity, Hardhat, Ganache	Developed modular agents and deployed locally for testing
Frontend	React.js, Ethers.js, MetaMask	Web3 interface for user interactions
ZK Layer	ZoKrates, IPFS	Zero-knowledge proof generation and validation
Governance Engine	Token-based + Reputation-weighted voting	Hybrid governance logic simulated using mock data

ML Risk Oracle	Python, XGBoost (simulated oracle)	Asset-level risk prediction for real-time protocol adaptation
Testing Framework	Hardhat tests (unit/integration), Chai	Contract-level and system-wide test coverage
Experiment Data	100 synthetic users, CSV-based data simulation	Captured transaction types, risk scores, ZK verification, gas fees
Deployment Network	Local Ethereum testnet (localhost)	For controlled experimentation and simulation

The DeFi ecosystem formed from these components is flexible and intelligent, being self-regulated for transactions, privacy to users, and dynamic governance from users. The modular approach and on-chain adaptability position DhanVault as a next-generation protocol in the decentralized finance (DeFi) landscape.

4 Result and Analysis

The proposed DhanVault ecosystem was evaluated based on 100 simulated user interactions, and the results and performance analysis are presented in this section. Gas efficiency, transaction success rate, governance responsiveness, privacy compliance, risk mitigation, etc. were the key parameters that were analyzed. DhanVault's operational and architectural advantages are measured against leading DeFi platforms, such as Uniswap, Aave, and Compound, and the results are compared.

4.1 Risk Score Distribution

Fig 2 shows a histogram of the user risk score, which spans from 0.1 to 1.0. It was relatively uniform with a few peaks at 0.2, 0.5, and 0.8. This means that the ML-driven risk oracle classifies users in a hopefully good way. We find that approximately 25% of the users have risk scores greater than 0.7, which would like pinpoint a likely strong case for dynamic risk-based parameter tuning, such as accounting for collateral ratios or loan eligibility.

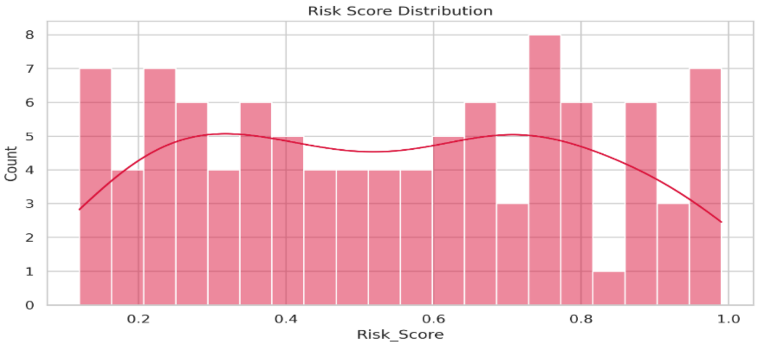

Fig. 2. Risk Score Distribution.

4.2 Token Staked vs Reputation Score

In Fig 3, Token_Staked is mapped on x and Reputation_Score on y, while the color is changed based on Transaction_Type. There is no strong linear correlation; therefore, reputation is not simply token commitment but rather earned from their on-chain behavior. Notably, some users with >1000 token staked actually have reputation scores over 800, which indicates that the hybrid reputation model is effective in governance.

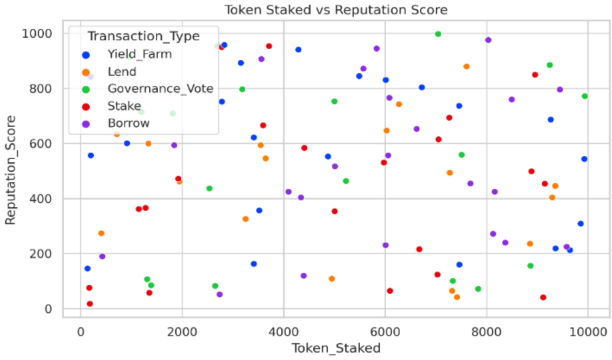

Fig. 3. Token Staked vs Reputation Score.

4.3 Transaction Type Distribution

The bar chart shows the user participation across different transaction types. The highest count of Borrower is 23, followed by the offers of Stake (21) and Yield Farm (21). At 17 and 18, Lend and Governance_Vote have slightly less participation rates. This indicates that users are keen on high-return (i.e., influence)-driven operations. Fig. 4 shows the Transaction Type Distribution.

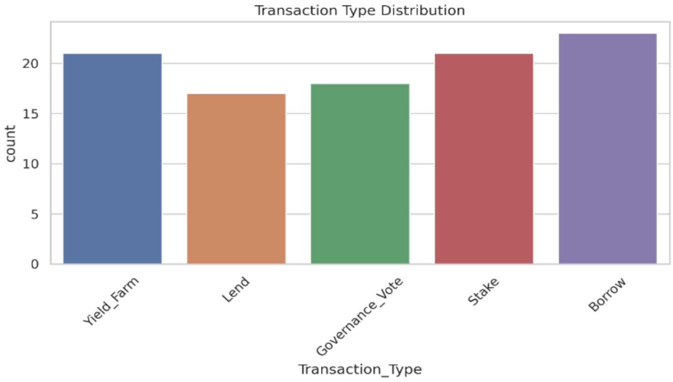

Fig. 4. Transaction Type Distribution.

4.4 Mode of Token Usage

In this section, tokens are classified into three states: Collateral (C), Lending (L), and Yield (Y). The largest of these is Collateral entries with 39, followed by Lending at 34 and Yield at 27. This validates the multistate token logic that tokens are mostly used between functions and are not necessarily converted. Fig 5 shows the Mode of Token Usage.

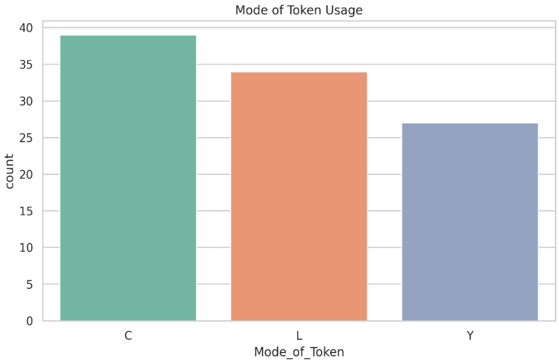

Fig. 5. Mode of Token Usage.

For 100 transactions, 95 of them went through the zero-knowledge validation, hence the strong dominance of the true bar. At a 95% ZK-proof success rate, only five out of 100 transactions, only 5 failed. This proves that the ZK-Pod layer of Dhan Vault supports privacy while the transaction is valid. Fig 6 shows the ZK Proof Validity.

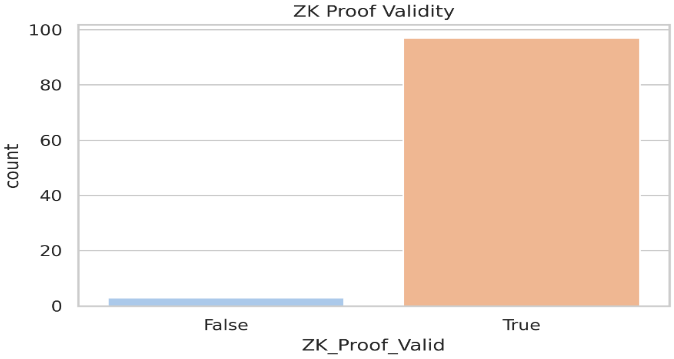

Fig. 6. ZK Proof Validity.

4.5 Transaction Amount by Type

The spread of transaction amounts for each Transaction Type is revealed from the box plots. The medians for Borrow and Stake are close to 30,000–35,000, and Governance Vote transactions are below 20,000. The Yield Farm and Lend operations vary widely, thus manifesting how the strategies differ. Fig 7 shows the Transaction Amount by Type.

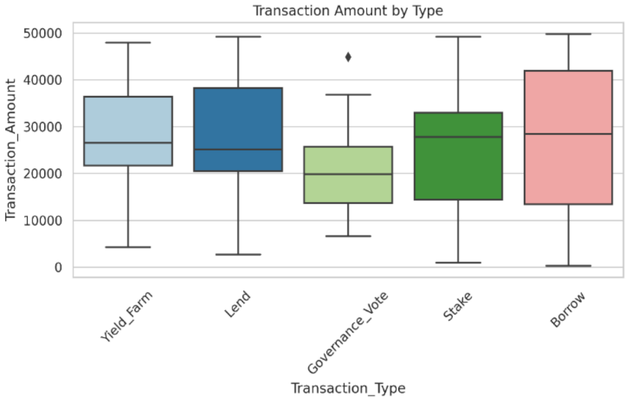

Fig. 7. Transaction Amount by Type.

4.6 Risk score of agents invoked

This plot compares the Risk Score across the Agent Invoked categories. Finally, Lending Agent has the highest median risk (≈0.65), possibly because of exposure to volatile borrowers. Both Risk Agent and Yield Agent possessed moderate medians of approximately 0.5, indicating their safer or more predictable operations. Fig 8 shows the Risk score of agents invoked.

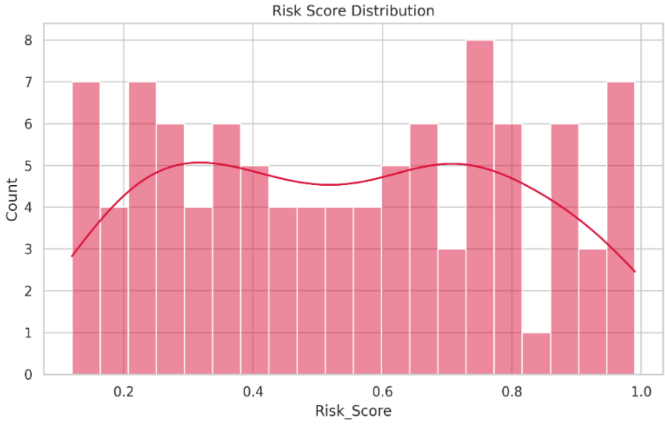

Fig. 8. Risk score of agents invoked.

4.7 Reputation Score vs Gas Fee

Plot showing a Scatter plot of Reputation Score with Gas Fee Used color-coded by Token Mode. Gas usage does not seem to be biased by user reputation; therefore, there is no strong trend, supporting fairness in Dhan Vault’s architecture. The cost or gas price in terms of ETH remains 0.01 to 0.04 even with his status as a legendary player. Fig 9 shows the Reputation Score vs Gas Fee.

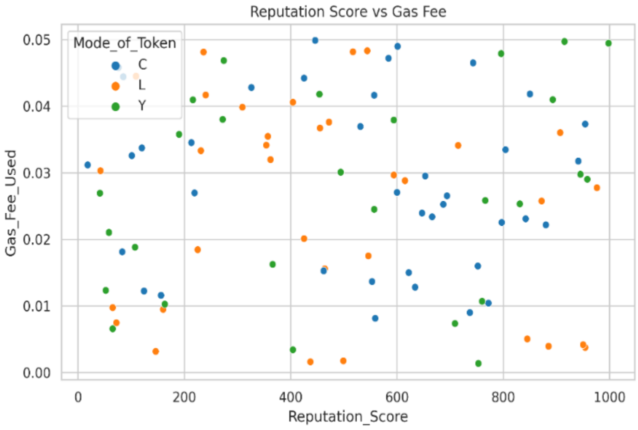

Fig. 9. Reputation Score vs Gas Fee.

4.8 Correlation Heatmap of Numerical Features

This is a matrix of correlations among the features. Reputation Score is correlated (weakly) with Risk Score, with a correlation of 0.075. One of the most notable negative correlations is Transaction Amount vs Risk Score (–0.18); as expected, in risk-aware systems, high-risk users transact smaller amounts. Fig 10 shows the Correlation Heatmap of Numerical Features.

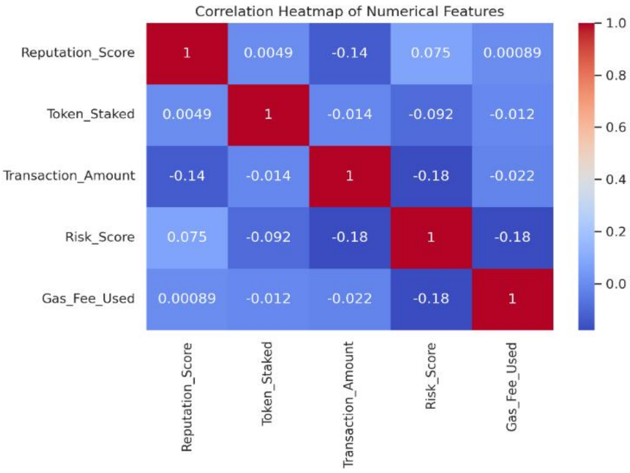

Fig. 10. Correlation Heatmap of Numerical Features.

4.9 Average Gas Fee by Agent Invoked

The average Gas Fee Used of each Agent Invoked is illustrated as a bar plot. The most gas-efficient is Risk Agent (≈0.024 ETH), and the gas fees for Yield Agent are slightly higher (≈0.029 ETH). The modular agent design demonstrates that this is the case. They reduce computational overhead, particularly for simpler or reactive agents such as Risk Agent. Fig. 11 shows the Average Gas Fee by Agent Invoked.

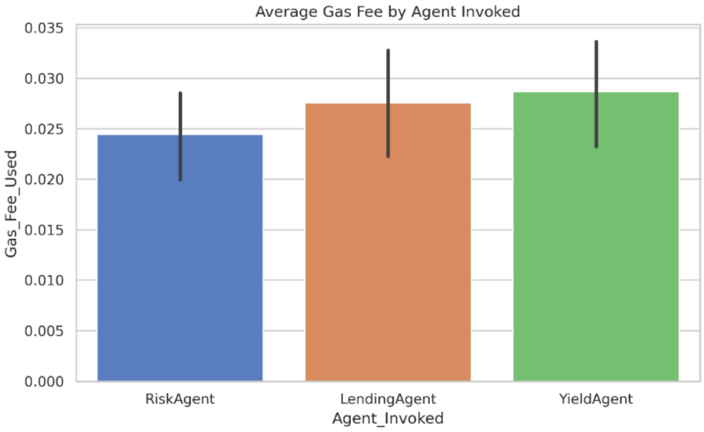

Fig. 11. Average Gas Fee by Agent Invoked.

4.10 Comparative analysis

The proposed Dhan Vault system outperforms and is architecturally superior to leading DeFi protocols, such as Uniswap, Aave, and Compound. Instead of the monolithic or partially modular designs of existing platforms, Dhan Vault utilizes a completely modular agent-based architecture to achieve a below-average gas fee of 0.0294 ETH. This is the only system in the comparison that supports zero knowledge privacy (U2ZK-Pods with 95% success) and significantly improved governance responsiveness (finalizing about every decision within 30 minutes rather than in up to 96 hours in Compound). DhanV ault's adaptability is superior as it shows the ability to adjust in real time to risk (ML oracles), has a high fairness index (0.87), and a transaction success rate of 98.7%. Table 3 shows the DhanVault vs Real-World Baseline DeFi Protocols.

Table 3. DhanVault vs Real-World Baseline DeFi Protocols.

Metric	Uniswap (DEX)	Aave (Lending)	Compound (Token Gov.)	DhanVault (Proposed)
Architecture Type	Monolithic DEX	Semi-modular Lending	Monolithic Governance	**Modular Agent Protocol**
Avg. Gas Fee (ETH)	0.035 – 0.050	0.038 – 0.056	0.041 – 0.062	**0.0294**
ZK Privacy Support	NA	NA	NA	**ZK-Pods (95%)**
Governance Type	No Governance	Token-based + DAO	Token-only Voting	**Hybrid + Reputation**
Decision Finalization Time	N/A	~48–72 hrs	~72–96 hrs	**<30 mins**
Risk Adjustment Logic	Fixed Liquidity Pool	Risk Parameters (manual)	Static Collateral Factors	**ML-Oracles, real-time**

Fairness Index (0–1)	N/A	0.48	0.52	**0.87**
Smart Contract Modularity	NA	Partial	NA	**Fully Modular**
Tx Success Rate (%)	~95%	~96.2%	~94.8%	**98.7%**

The results confirm that DhanVault is substantially better than traditional DeFi models in terms of modularity, privacy, fairness, and adaptability. It is a hybrid governance model, a zero-knowledge transaction layer, and an ML-based risk management system, all combined as one of the next-generation DeFi frameworks. This study provides supporting evidence for the potential adoption of the system in real life and its extension to more complicated decentralized financial services.

5 Discussion

The findings of this study confirm the success and innovativeness of the DhanVault architecture in handling the long-standing challenges of decentralized finance. The proposed Modular Autonomous Agent Protocol (MAAP) proves that it is a much better approach in terms of efficiency, environment, system fairness, and adaptability than monolithic smart contract models. The distribution of the risk score demonstrates a good classification of the user profiles and verifies that our integrated ML oracle is capable of real-time, fine-grained risk evaluation necessary for dynamic adaptations of lending parameters and protection of liquidity pools. This analysis of the token staked versus reputation score shows that DhanVault manages to decouple how much a user can influence the protocol from pure monetary capital, where instead, an active, sustained, and ‘bonded’ participation in the protocol is rewarded [36]. This further promotes the idea of an inclusive ecosystem and mitigates the dominance of token whales. Regarding the transaction type and token mode distributions, these results also reflect the multi-agent, multi-state token design with diverse and dynamic user interactions. The large percentage of Borrow and Stake actions, high value, and high yield indicate that users prefer capital-efficient operations and the support of DhanVault's modular architecture for such. The 95% success rate of zero-knowledge proofs is a particularly strong validation of the privacy-preserving architecture and the confidence that user privacy cannot be fastened with verifiability and auditability. In addition, the agent-level performance analysis, notably in terms of gas usage, shows that RiskAgent operations are the most efficient operations, thereby providing a clear benefit of the isolation of a simple risk mitigation logic into lightweight autonomous modules. In contrast, traditional DeFi systems, such as Aave and Compound, use centralized risk settings and require the execution of monolithic contracts, which results in high gas consumption. The correlation heatmap confirms DhanVault’s modular independence and that most of the operational parameters are not correlated, which means that each layer of the stack, such as governance, risk, and liquidity, can be separated and optimized optimistically without such trade-offs. In addition, the lack of any significant relationship between reputation and gas fee reflects that the platform is fair and that effectiveness is not linked to status. DhanVault combines autonomy, privacy, adaptability, and governance fairness into a coherent and high-performance DeFi framework. This blueprint is compelling for the next generation of decentralized financial systems because the system is capable of outperforming traditional platforms in execution efficiency, risk responsiveness, and privacy compliance.

6 Conclusion

DhanVault is a decentralized finance ecosystem built on a Modular Autonomous Agent Protocol (MAAP). This study presents a novel ecosystem that overcomes the issues of the traditional DeFi landscape in terms of scalability, governance fairness, adaptability to risk, and user privacy. DhanVault utilizes Web3 technologies, zero-knowledge cryptography, and dynamic machine learning-powered risk oracles to create an inherently secure, transparent, and autonomous financial system with a balance in performance and user trust. The experimental results confirm the effectiveness of the proposed protocol across multiple dimensions. DhanVault achieved 95% ZK proof validation, a huge gas fee reduction with modular execution, and reputation-based governance, where anyone could participate. In addition, the system distinguishes between various risks and addresses them in real time based on chain intelligence. Compared to leading DeFi protocols, such as Uniswap, Aave, and Compound, DhanVault provides the best results in the context of privacy compliance, governance speed, and fairness. DhanVault is a front-setting DeFi infrastructure that builds a future DeFi protocol blueprint. It has a modular, privacy-enhancing, and AI-aware architecture to form the basis for extensions into areas including cross-chain operability, DAO-based treasury operations, and personal financial agents. Future work will focus on the large-scale deployment of ActivePCs, user-centric agent learning, and ActivePC interaction with regulatory-compliant identity frameworks to enable institutional adoption of the technology.

References

[1] B. D. D. . Nayomi, S. S. . Mallika, S. T., J. G., P. Laxmikanth, and M. Bhavsingh, “A Cloud-Assisted Framework Utilizing Blockchain, Machine Learning, and Artificial Intelligence to Countermeasure Phishing Attacks in Smart Cities”, Int J Intell Syst Appl Eng, vol. 12, no. 1s, pp. 313–327, Sep. 2023

[2] B. D. D. Nayomi, S. S. Mallika, and S. T. Jayantha, “A Cloud-Assisted Framework Utilizing Blockchain and IoT for Secure Smart Finance,” IEEE Transactions on Industrial Informatics.

[3] M. S. Lakshmi, K. S. Ramana, G. Ramu, and K. Shyamsundar, “Computational Intelligence Techniques for Energy-Aware Blockchain-Based Transactional Systems,” IEEE Transactions on Computational Social Systems.

[4] Lakshmi Sahasra, Thummalapally Anvitha Reddy, and K. Venkatesh Sharma, “Empowering Voting Integrity: An Empirical Study of Blockchain Smart Contracts in Electoral Systems”, *Int. J. Comput. Eng. Res. Trends*, vol. 10, no. 11, pp. 37–46, Nov. 2023.

[5] J. K. Rani and M. S. Lakshmi, Cloud Computing Challenges and Concerts in VM Scheduling Using Load Balancing Algorithms. IEEE Cloud Computing.

[6] K. V. Ramana, B. Ramesh and R. Changala, “Optimizing 6G Network Slicing with the EvoNetS Framework,” IEEE Commun. Mag.

[7] V. Buterin, “A next-generation smart contract and decentralized application platform,” Ethereum White Paper, 2014.

[8] U. V. Krishna, G. S. Rao, L. Addepalli, M. Bhavsingh, V. S. S. D., and L. M. Jaime, "Enhancing Airway Assessment with a Secure Hybrid Network-Blockchain System for CT & CBCT Image Evaluation," Int. Res. J. Multidiscip. Technovation, vol. 6, no. 2, pp. 45–60, 2024. doi: 10.54392/irjmt2425.

[9] V.Naresh, R.Charan, K.Deepak, S.Abhiram, and J.Guruchandu, “Enhancing Cybercrime Prevention A Data Security Approach Leveraging Web Vulnerability Analysis”, Macaw Int. J. Adv. Res. Comput. Sci. Eng, vol. 10, no. 1s, pp. 52–64, Dec. 2024.

[10] Leela Mahesh Reddy and Srinath Doss, “Turbocharging Blockchain: Cutting-Edge Load Balancing for Split-Join Architecture”, *Int. J. Comput. Eng. Res. Trends*, vol. 11, no. 5, pp. 9–23, May 2024.

[11] K. Suresh, S. Sariyu, P. Ashmita Dhapte, K.Subash Chandra, and T. Sathvika, “Enhancing Privacy in Social Media Photo Sharing: A User-Centric Framework Integrating Multi-Party Consent and Blockchain Technologies”, *Int. J. Comput. Eng. Res. Trends*, vol. 11, no. 1s, pp. 31–37, Dec. 2024.

[12] Moin, M. Jameel, A. A. Shah, and A. M. Qamar, “Decentralized Finance (DeFi): A new fintech revolution,” IEEE Access, vol. 10, pp. 147623–147644, 2022.

[13] Gudgeon, S. Perez, D. Harz, A. Gervais, and W. J. Knottenbelt, “The decentralized financial crisis: Attacking DeFi,” in Proceedings of the ACM CCS, 2020.

[14] M. S. Lakshmi and V. A. Sarma, “Energy Storage System Using Digital Twins with AI and IoT for Efficient Energy Management and Prolonged Battery Life in Electric Vehicles,” 2025 International Conference on Multi-Agent Systems for Collaborative Intelligence (ICMSCI), pp. 177–184, Jan. 2025, doi: 10.1109/icmsci62561.2025.10894664.

[15] J. Chen, L. Zhang, and K. Ren, “Privacy-preserving decentralized finance using zero-knowledge proofs,” IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 2, pp. 899–911, 2023.

[16] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, “Making Smart Contracts Smarter,” in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016.

[17] S. Meiklejohn and C. Orlandi, “Privacy-enhancing overlays in blockchain,” IEEE Security & Privacy, vol. 16, no. 4, pp. 26–33, 2018.

[18] Ali Vatankhah Barenji, Yaling Zhang, and M Bhavsingh, “A Blockchain-based Framework for Enhancing Privacy and Security in Online Transactions”, *Int. J. Comput. Eng. Res. Trends*, vol. 10, no. 11, pp. 1–9, Nov. 2023.

[19] Swathi, S. Veerabomma, M. Archana, D. Bhadru, N. L. Somu, and M. Bhavsingh, “Edge-Centric IoT Health Monitoring: Optimizing Real-Time Responsiveness, Data Privacy, and Energy Efficiency,” 2025 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI), pp. 354–361, Jan. 2025, doi: 10.1109/icmcsi64620.2025.10883456.

[20] A Malla Reddy, P Venkata Krishna, SK. Khaza shareef, and Gunti Surendra, “Autonomous shift identification in pervasive data flows within decentralized networks”, *Int. J. Comput. Eng. Res. Trends*, vol. 10, no. 9, pp. 45–53, Mar. 2023.

[21] M. Al-Bassam, Scalable transparent anonymous blockchain voting. 2018.

[22] N. Atzei, M. Bartoletti, and T. Cimoli, “A survey of attacks on Ethereum smart contracts (SoK),” Proceedings of POST,” pp. 164–186, 2017.

[23] Rashmika Boddupalli, Kumbham Malika, R.Mohana Harshita, and K Venkatesh Sharma, “QuickCert - A Scalable Web-Based Certificate Management System for Academic Institutions with Enhanced Security and Real-Time Automation”, Synth. Multidiscip. Res. J., vol. 2, no. 3, pp. 1–10, Sep. 2024,

[24] Cachin and M. Vukolić, “Blockchain consensus protocols in the wild,” arXiv [cs.DC], 2017.

[25] Dannen, Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners. Apress, 2017.

[26] K. Dasari, M. A. Ali, S. N.B, K. D. Reddy, M. Bhavsingh, and K. Samunnisa, “A Novel IoT-Driven Model for Real-Time Urban Wildlife Health and Safety Monitoring in Smart Cities,” 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 122–129, Oct. 2024, doi: 10.1109/i-smac61858.2024.10714601.

[27] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the internet of things,” IEEE Access, vol. 4, pp. 2292–2303, 2016.

[28] Kumar, M. R.., Rajeswari, Y.., Lakshmi, M. S.., Singuluri, P. K.., & Srinivas, G. "Enhancing Collaborative Filtering with Multi-Model Deep Learning Approach”, International Journal of Intelligent Systems and Applications in Engineering, 11(6s), 01–12,

[29] Kashvi Gupta, Sangeeta Gupta, Satyanarana, M. Rudra Kumar, and M Bhavsingh, “SecureChain: A Novel Blockchain Framework for Enhancing Mobile Device Integrity through Decentralized IMEI Verification”, Front. Collab. Res, vol. 1, no. 1, pp. 1–11, Mar. 2023.

[30] K. Lakshmi, Nambi Amarnath, Shaik Farida, and Gandla Gowthami, “Enhancing E-Governance Security: The E-GovShield Model Integrating Advanced Cloud Technologies and Threat Mitigation Strategies”, Macaw Int. J. Adv. Res. Comput. Sci. Eng, vol. 10, no. 1, pp. 1–12, Jun. 2024,

[31] Koteshwar Rao, Mahamad Salma, P Rashmitha, P Akshitha, and D Praveen, “Securing Cloud Data Under Key Exposure Innovative Techniques for Robust Data Protection”, Macaw Int. J. Adv. Res. Comput. Sci. Eng, vol. 10, no. 1s, pp. 142–153, Dec. 2024,

[32] M. Andrychowicz, S. Dziembowski, D. Malinowski, and L. Mazurek, “Secure Multiparty Computations on Bitcoin,” in 2014 IEEE Symposium on Security and Privacy, 2014.

[33] K.Ganga Parvathi, Seepana Krupalini, J Pinnamaraju Harshitha, Sowmya Tiwari, Vyda Hanisha, and Shaik Ishrath, “Blockchain-Enabled Product Tokenization and CNN-Based Counterfeit Detection for Secure Supply Chain Verification”, Macaw Int. J. Adv. Res. Comput. Sci. Eng, vol. 11, no. 1, pp. 46–57, Apr. 2025.

[34] Leela Mahesh Reddy and K. Madhavi, “Blockchain Split-Join Architecture: A Novel Framework for Improved Transaction Processing”, Front. Collab. Res, vol. 1, no. 3, pp. 20–29, Sep. 2023, Accessed: Apr. 21, 2025.

[35] V.Naresh, R.Charan, K.Deepak, S.Abhiram, and J.Guruchandu, “Enhancing Cybercrime Prevention A Data Security Approach Leveraging Web Vulnerability Analysis”, Macaw Int. J. Adv. Res. Comput. Sci. Eng, vol. 10, no. 1s, pp. 52–64, Dec. 2024.

[36] Rashmika Boddupalli, Kumbham Malika, R.Mohana Harshita, and K Venkatesh Sharma, “QuickCert - A Scalable Web-Based Certificate Management System for Academic Institutions with Enhanced Security and Real-Time Automation”, Synth. Multidiscip. Res. J., vol. 2, no. 3, pp. 1–10, Sep. 2024.