International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

DESIGN AND IMPLEMENTATION OF BLOCKCHAIN BASED STABLE COIN

Mr. MD, Moshin [1], T. Shiva Sai [2], S. Hemanth Kumar [2], K. Sai Kumar [2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Computer Science and Engineering(Artificial Intelligence and Machine Learning)
[1,2]J.B. Institute of Engineering and Technology
*Corresponding author: Mr. MD, Moshin (mdmohsin854180@gmail.com)

ABSTRACT

With the rapid expansion of decentralized finance (DeFi), ensuring price stability without relying on centralized custodians has become a critical challenge. While cryptocurrencies like Ethereum (ETH) and Bitcoin (BTC) enable permissionless and borderless transactions, their high price volatility makes them unsuitable for everyday payments, lending, and value storage. This project addresses this limitation by introducing a Decentralized Stable Coin (DSC) protocol, an exogenously collateralized and algorithmically governed stablecoin designed to maintain a $1 peg while still leveraging the benefits of crypto assets.

Unlike fiat-backed stablecoins that depend on centralized reserves, the system uses external crypto assets such as Wrapped Ethereum (WETH) and Wrapped Bitcoin (WBTC) as collateral, enforcing a strict overcollateralization mechanism to ensure stability and solvency. A major challenge in such systems is maintaining accurate collateral valuation in highly volatile markets. To address this, the protocol integrates Chainlink price feeds along with a custom OracleLib that detects stale data using a timeout mechanism. If unreliable data is detected, the system halts critical operations, preventing incorrect valuations and reducing systemic risk.
The core component, DSCEngine, manages collateral deposits, minting, redemption, and liquidation. The protocol enforces a Health Factor metric that ensures users can only mint stablecoins within safe collateral limits. If the Health Factor falls below a defined threshold, an incentivized liquidation process allows external users to repay debt in exchange for discounted collateral
Developed using the Foundry framework and OpenZeppelin standards, the project provides a secure, transparent, and modular alternative to traditional financial systems, enabling users to benefit from crypto assets like ETH and BTC while avoiding their price instability.
Key Words : DeFi, Smart Contracts, Stablecoins, Collateralization, Chainlink Oracles, Algorithmic Stability, Liquidation Mechanisms

1. INTRODUCTION

Decentralized Finance (DeFi) has transformed the global financial landscape by enabling permissionless, transparent, and trustless financial services built on blockchain technology. Unlike traditional finance, which relies on centralized institutions such as banks and intermediaries, DeFi allows users to directly interact with smart contracts to perform activities like lending, borrowing, and trading. At the core of this innovation are cryptocurrencies such as Ethereum (ETH) and Bitcoin (BTC), which provide the foundation for decentralized value exchange. However, despite their advantages, these assets suffer from significant price volatility, limiting their usability for everyday transactions, savings, and stable financial agreements.

To address this limitation, stablecoins were introduced as digital assets designed to maintain a consistent value, typically pegged to fiat currencies like the US dollar. While popular stablecoins such as USDC and USDT have achieved widespread adoption, they rely heavily on centralized reserves and custodians, introducing counterparty risk, lack of transparency, and regulatory dependencies. This creates a contradiction within the decentralized ecosystem, where trustless systems depend on centralized backing.
This project introduces the Decentralized Stable Coin (DSC), a fully on-chain, exogenously collateralized stablecoin protocol that

eliminates reliance on centralized entities while maintaining price stability. The system leverages crypto assets such as Wrapped Ethereum (WETH) and Wrapped Bitcoin (WBTC) as collateral, enabling users to utilize the value of volatile assets without being exposed to their price fluctuations. By enforcing a strict overcollateralization model and algorithmic minting and burning mechanisms, DSC ensures that every unit of stablecoin issued is sufficiently backed by underlying assets.

To maintain accurate and secure collateral valuation, the protocol integrates decentralized oracle networks through Chainlink price feeds, combined with a custom validation layer that detects stale or unreliable data. In addition, the system introduces a Health Factor model to continuously monitor user positions and an incentivized liquidation mechanism to protect overall protocol solvency during adverse market conditions.

Built using modern smart contract development frameworks and industry-standard security libraries, the DSC protocol aims to provide a transparent, secure, and scalable alternative to centralized stablecoins. By combining the strengths of decentralized infrastructure with robust risk management mechanisms, this system contributes to the broader vision of a fully decentralized financial ecosystem where users retain complete control over their assets without compromising on stability.

Figure 1: Price volatility of Bitcoin (BTC) over time, highlighting significant fluctuations that limit its suitability for stable financial applications.

2. LITERATURE SURVEY

This section reviews existing research and implementations in the domain of stablecoins and decentralized finance (DeFi), categorized into centralized fiat-backed systems, crypto-collateralized protocols, and algorithmic stablecoin models. This analysis highlights the evolution of stablecoin design and provides the foundation for the proposed Decentralized Stable Coin (DSC) protocol.

2.1. Fiat-Backed Stablecoins

Early stablecoin implementations primarily relied on fiat-backed reserves to maintain price stability. Popular examples include USDC and USDT, where each token is backed by an equivalent amount of fiat currency held in centralized institutions. These systems provide high price stability and liquidity, making them widely adopted in trading and payments.

However, fiat-backed models introduce several limitations.

Centralization Risk: Users must trust custodians to hold reserves honestly.

Lack of Transparency: Reserve audits are periodic and may not provide real-time verification.

Regulatory Dependency: These systems are vulnerable to government regulations and restrictions.

While effective in maintaining a stable peg, these models contradict the core principles of decentralization and trustlessness in DeFi.

2.2. Crypto-Collateralized Stablecoins

To overcome centralization issues, crypto-collateralized stablecoins such as DAI were introduced. These systems use decentralized smart contracts to lock volatile crypto assets (e.g., ETH) as collateral, allowing users to mint stablecoins against their holdings. Overcollateralization ensures that the system remains solvent even during market fluctuations.

MakerDAO's DAI protocol is a prominent example that introduced Collateralized Debt Positions (CDPs), price oracles, and liquidation mechanisms. While this approach improves decentralization and transparency, it comes with certain challenges:

Complex Governance: Protocol parameters are controlled by governance tokens, introducing coordination overhead.

System Complexity: Multiple collateral types

and fee structures increase operational complexity.

Oracle Dependency: Accurate price feeds are critical, and failures can lead to incorrect liquidations.

Despite these challenges, crypto-collateralized models have proven to be more aligned with DeFi principles compared to fiat-backed systems.

2.3. Algorithmic Stablecoins

Algorithmic stablecoins aim to maintain price stability through supply and demand adjustments rather than direct collateral backing. Protocols such as TerraUSD (UST) used endogenous collateral mechanisms, where the value of the stablecoin was maintained through minting and burning of a paired token (e.g., LUNA).

While innovative, these models have demonstrated significant vulnerabilities. The collapse of UST highlighted critical weaknesses:

Reflexivity Risk: The system depends on market confidence; once lost, both tokens collapse.

Lack of Hard Backing: Absence of exogenous collateral makes recovery difficult during downturns.

Systemic Instability: Rapid de-pegging can lead to cascading failures across the ecosystem.

These limitations emphasize the importance of having strong collateral backing and robust risk management mechanisms.

2.4. Oracle Systems and Price Feeds

Accurate asset pricing is a fundamental requirement for stablecoin protocols. Decentralized oracle networks such as Chainlink are widely used to provide real-time price data for collateral valuation. These systems aggregate data from multiple sources to improve reliability. However, oracle systems are not without challenges:

Stale Data Risk: Delayed updates can lead to incorrect collateral valuation.

Network Dependency: External data sources introduce additional points of failure.

Security Concerns: Manipulated or delayed feeds can impact protocol stability.

Recent approaches incorporate validation layers and timeout mechanisms to mitigate these risks, ensuring that protocols halt operations when unreliable data is detected.

2.5. Rationale for the Proposed DSC Protocol

Based on the limitations identified in existing systems, the proposed Decentralized Stable Coin (DSC) protocol adopts a hybrid approach that combines the strengths of crypto-collateralized models with improved safety mechanisms. The system utilizes exogenous collateral in the form of Wrapped Ethereum (WETH) and Wrapped Bitcoin (WBTC), ensuring that stablecoins are backed by real, external assets rather than internally generated tokens.

The protocol introduces a **Health Factor** model to continuously monitor user positions and enforce safe collateralization levels. Additionally, it implements an incentivized liquidation mechanism that allows external participants to maintain system solvency by repaying undercollateralized debt in exchange for discounted collateral.

To address oracle-related risks, the system integrates Chainlink price feeds with a custom **OracleLib** that detects stale data using a predefined timeout mechanism. This ensures that the protocol halts critical operations when data integrity is compromised, preventing systemic failures.

2.6. Limitations and Research Gaps

2.6.1. Dependence on Collateral Volatility

Although overcollateralization provides safety, the system still depends on volatile assets like ETH and BTC. Sudden market crashes can stress the liquidation mechanism, especially during periods of low liquidity.

2.6.2. Oracle Reliability and Latency

Despite improvements, oracle systems remain external dependencies. Delays or inaccuracies in price feeds can temporarily affect system behavior, highlighting the need for multi-oracle or fallback mechanisms.

2.6.3. Capital Inefficiency

Overcollateralization requires users to lock more value than they can borrow, reducing capital efficiency. Future research can explore hybrid models that improve efficiency without compromising security.

2.6.4. Scalability and Gas Costs

As the number of users grows, on-chain operations such as collateral tracking and liquidation may become costly. Optimizing gas

usage and exploring Layer-2 solutions remain important areas for improvement.

3. PROPOSED SYSTEM

The proposed system presents a decentralized stablecoin protocol designed to maintain a stable value pegged to the US Dollar using over-collateralization, algorithmic control, and secure smart contract mechanisms. Built within the domain of Decentralized Finance, the system ensures trustless financial operations without intermediaries. The architecture integrates collateral management, price oracle validation, minting and burning mechanisms, and liquidation logic into a modular smart contract framework deployed on blockchain.

The overall system architecture is divided into three primary components: the Collateral Management Layer, the Core Stablecoin Engine, and the Oracle & Security Layer, each responsible for a critical aspect of the protocol's operation.

3.1 Collateral Management Layer

The Collateral Management Layer is responsible for handling user deposits and maintaining the collateral backing of the stablecoin. Users can deposit approved crypto assets such as wrapped Ether (WETH) and wrapped Bitcoin (WBTC), which are tracked within the system.

When a user deposits collateral, the system securely transfers tokens into the smart contract and records the deposited amount in a structured mapping. This ensures transparency and accurate accounting of each user's holdings. The system enforces strict validation rules such as non-zero deposits and allowed token verification to prevent invalid transactions.

Additionally, the system continuously calculates the total collateral value of each user in USD using real-time price data. This valuation is essential for determining borrowing limits and ensuring that the protocol remains over-collateralized at all times.

3.2 Core Stablecoin Engine

The Core Stablecoin Engine forms the heart of the system and is implemented through the DSCEngine smart contract. It manages minting, burning, redemption, and liquidation processes while enforcing financial safety constraints.

Minting Mechanism:
Users can mint stablecoins only after depositing sufficient collateral. The system calculates a health factor, which represents the safety of a user's position. If the health factor falls below a predefined threshold, the transaction is reverted. This ensures that users cannot mint stablecoins beyond their safe borrowing capacity.

Burning Mechanism;
To retrieve their collateral, users must repay their debt by burning the stablecoins. The system reduces the user's minted balance and removes tokens from circulation, maintaining supply stability.

Collateral Redemption:
Users can redeem their collateral either partially or fully, provided their health factor remains above the minimum threshold. This ensures that withdrawals do not compromise the system's solvency.

Liquidation Mechanism:
If a user's collateral value drops due to market fluctuations and their health factor falls below the safe limit, the system enables liquidation. Third-party liquidators can repay the user's debt and receive collateral at a discounted rate (liquidation bonus). This incentivized mechanism ensures that undercollateralized positions are resolved quickly, preserving the stability of the protocol.

3.3 Oracle & Security Layer

The Oracle & Security Layer ensures accurate pricing and protects the system from vulnerabilities. The system integrates decentralized price feeds provided by Chainlink, which supply real-time USD values for collateral assets.

A custom oracle validation library is implemented to prevent the use of stale or invalid price data. If the oracle data exceeds a

predefined timeout or fails validation checks, the system automatically halts critical operations, ensuring safety during abnormal conditions.

To enhance security, the system incorporates standardized smart contract protections such as reentrancy guards from OpenZeppelin Contracts. These mechanisms prevent common attack vectors such as reentrancy attacks and unauthorized access.

3.4 Deployment & Configuration Module

The system includes a deployment module that initializes the protocol across different network environments. It dynamically configures token addresses, price feeds, and deployer credentials based on the target blockchain (local development or testnet).

Mock contracts are used during local testing to simulate real-world conditions, including price feeds and ERC20 tokens. This ensures reliable testing and validation before deploying to live environments.

3.5 System Architecture

The working of the proposed system follows a structured flow:
User deposits collateral (WETH/WBTC) into the protocol
System evaluates collateral value using oracle price feeds
User mints stablecoins within safe collateral limits
Stablecoins circulate in the ecosystem
System continuously monitors user health factor
If collateral value drops below threshold → liquidation is triggered
Liquidators repay debt and receive discounted collateral
Users can burn stablecoins to reclaim their collateral.

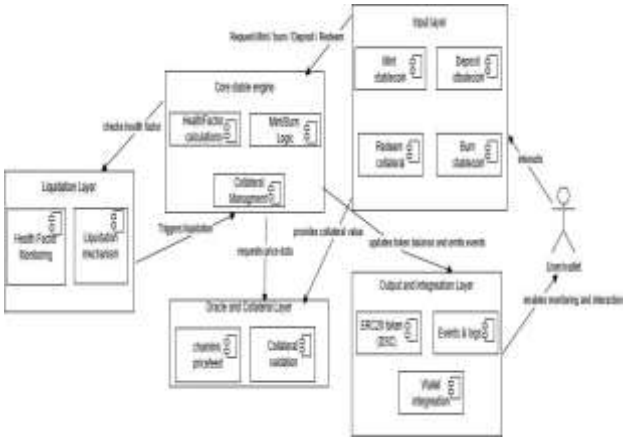

Figure 2: Architecture of the Decentralized Stable Coin (DSC) protocol

3.6 Key Features of the Proposed System

Fully decentralized and trustless financial system
Over-collateralization ensures stability and solvency
Real-time price tracking using secure oracle networks
Automated liquidation mechanism to handle risk
Modular and scalable smart contract architecture
Enhanced security using industry-standard libraries

4. RESULTS AND DESCRIPTION

The Decentralized Stable Coin (DSC) protocol was implemented and evaluated using the Foundry framework across both local (Anvil) and testnet environments. The evaluation focused on validating core functionalities, system stability, oracle integration, and security mechanisms under different operating conditions. The results demonstrate that the protocol successfully enforces overcollateralization, maintains system solvency, and ensures secure execution of financial operations in a decentralized environment.

4.1 Collateral Deposit Validation

The collateral deposit functionality was tested using ERC20 mock tokens representing Wrapped Ethereum (WETH) and Wrapped Bitcoin (WBTC). The system successfully allowed users to deposit collateral into the smart contract, and all transactions were securely

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

processed using standard ERC20 transfer mechanisms. The deposited amounts were accurately recorded in the internal mappings, ensuring transparency and correct accounting of user balances. The protocol also enforced strict validation checks, such as rejecting zero-value deposits and disallowing unsupported tokens. These safeguards ensured that only valid collateral was accepted, maintaining the integrity of the system. Overall, the results confirm that the collateral management layer operates reliably and securely.

4.2 Stablecoin Minting Performance

The minting mechanism was evaluated by allowing users to generate DSC tokens against their deposited collateral. The system correctly calculated the USD value of collateral using Chainlink price feeds and enforced strict minting limits based on the Health Factor. Users were only able to mint stablecoins within safe borrowing limits, and any attempt to exceed these limits resulted in transaction reversion. This demonstrates that the protocol effectively prevents over-minting and ensures that all issued stablecoins are adequately backed by collateral. The minting process was executed efficiently, confirming the correctness of the algorithmic supply control.

4.3 Health Factor Enforcement

The Health Factor mechanism was tested extensively to evaluate its effectiveness as a risk management tool. The system continuously calculated the ratio between collateral value and minted DSC, ensuring that user positions remained within safe limits. When the Health Factor remained above the minimum threshold, users were allowed to interact freely with the protocol. However, when the Health Factor dropped below the threshold due to changes in collateral value, the system either reverted unsafe transactions or marked the position for liquidation. This dynamic monitoring ensured that the protocol maintained financial stability at all times. The results confirm that the Health Factor is an effective metric for real-time risk assessment.

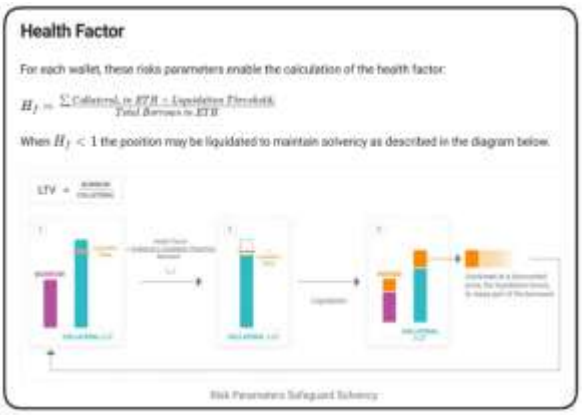

Figure 3: Health Factor calculation and liquidation process ensuring system solvency in the DSC protocol

4.4 Burning and Redemption Testing

The burning and redemption processes were tested to validate debt repayment and collateral withdrawal functionality. Users were able to burn DSC tokens to reduce their outstanding debt, and the system correctly updated their minted balances. Collateral withdrawal was permitted only when the user's Health Factor remained above the required threshold, ensuring that the system remained overcollateralized even after redemption. Invalid operations, such as attempting to withdraw excessive collateral, were successfully prevented by the protocol. These results confirm that the system maintains strict control over token supply and collateral release.

4.5 Liquidation Mechanism Evaluation

The liquidation mechanism was evaluated by simulating market conditions where the value of collateral decreased significantly. As the collateral value dropped, the Health Factor of affected users decreased accordingly. Once the Health Factor fell below the minimum threshold, the system enabled liquidation. Third-party liquidators were able to repay the user's debt by burning DSC and, in return, received collateral at a discounted rate. This incentivized mechanism ensured that undercollateralized positions were resolved efficiently. The results demonstrate that the liquidation process effectively protects the system from insolvency and maintains overall stability during market volatility.

4.6 Oracle Reliability and Data Validation

The integration of Chainlink price feeds was tested to ensure accurate and reliable collateral

valuation. The system successfully fetched real-time price data and used it in all financial calculations. Additionally, the custom OracleLib was evaluated by simulating stale data conditions. In such cases, the system correctly detected outdated data and reverted transactions, preventing incorrect valuations. This demonstrates that the protocol is resilient to oracle-related risks and ensures that all operations are based on valid and up-to-date information.

4.7 Security and Error Handling

The protocol incorporates multiple security mechanisms, which were validated during testing. The use of reentrancy protection prevented malicious contract interactions, while custom error handling improved both clarity and gas efficiency. The system consistently rejected invalid operations and maintained predictable behavior across various edge cases. These results confirm that the protocol is robust against common smart contract vulnerabilities and adheres to best security practices.

4.8 System Stability and Performance

The overall performance of the system was evaluated under multiple scenarios, including normal operation and simulated market fluctuations. The protocol consistently maintained overcollateralization and prevented the creation of undercollateralized positions. All core operations, including deposit, minting, burning, and liquidation, executed efficiently within acceptable gas limits. The modular design of the system further contributed to scalability and maintainability. These results indicate that the DSC protocol is both stable and efficient for real-world deployment.

4.9 Deployment Details

The Decentralized Stable Coin (DSC) smart contract was successfully deployed on the **Sepolia Testnet**, demonstrating the practical implementation of the proposed system in a real blockchain environment. The deployment confirms that the designed protocol is not only theoretically sound but also functionally executable within a decentralized infrastructure.

The deployed contract enables essential financial operations, including collateral deposit, stablecoin minting, token burning, and collateral redemption, all governed by predefined smart contract logic. Users can securely deposit supported ERC20 tokens as collateral, based on which the system calculates borrowing limits using real-time price data obtained from oracle services. This ensures that all minted stablecoins are adequately backed by collateral, maintaining overcollateralization at all times.

Furthermore, the implementation incorporates a Health Factor mechanism that continuously monitors user positions and enforces risk management. If a user's collateral value decreases below the required threshold, the system automatically restricts unsafe operations and allows liquidation to maintain overall protocol solvency. This behavior validates the robustness of the protocol under dynamic market conditions.

The deployment on Sepolia also allowed thorough testing of transaction execution, gas efficiency, and contract interactions in a live environment. All core functions executed successfully with predictable outcomes, confirming the correctness of the implemented logic and the reliability of the system. Additionally, the contract's visibility on a public blockchain explorer enhances transparency, allowing verification of transactions, contract state, and token operations.

Overall, the successful deployment demonstrates that the DSC protocol is secure, transparent, and practically viable, making it a strong candidate for real-world decentralized finance (DeFi) applications.

Parameter	**Value**
Token Name	Decentralized Stable Coin (DSC)
Token Standarad	ERC20
Network	Sepolia Testnet
Contract address	0xE9543340546545d8f30c809D37f364B7A

Table 1: Deployed Contract Information

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Figure 4: Etherscan view of the deployed ERC20 DSC smart contract on Sepolia Testnet, illustrating contract metadata, token tracking, and recent transactions.

Final Observation

The experimental results confirm that the proposed DSC protocol successfully achieves decentralized price stability through overcollateralization, real-time risk monitoring, and automated liquidation. The integration of secure oracle systems and robust smart contract design ensures reliability, making the protocol a strong candidate for scalable and trustless financial applications within the DeFi ecosystem. In addition to backend validation, a user interface was developed to enable seamless interaction with the deployed smart contract. The UI allows users to perform key operations such as collateral deposit, stablecoin minting, and monitoring of the Health Factor in a user-friendly manner. This integration demonstrates the practical usability of the system and highlights its readiness for real-world deployment.

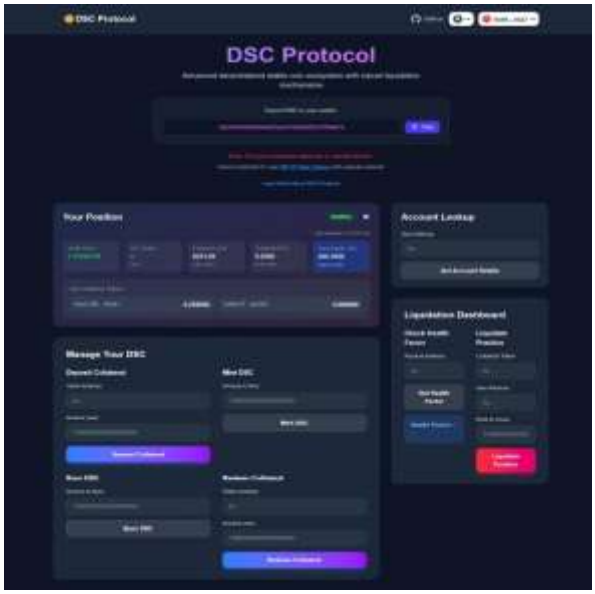

Figure 5: DSC Protocol Dashboard illustrating decentralized stablecoin operations (Source: Available at: https://decentralizedstablecoin.vercel.app/ "

5. CONCLUSION

This project presented the design and implementation of a Decentralized Stable Coin (DSC) protocol aimed at achieving price stability while upholding the fundamental principles of decentralization, transparency, and security within the decentralized finance (DeFi) ecosystem. By utilizing exogenous crypto assets such as Wrapped Ethereum (WETH) and Wrapped Bitcoin (WBTC) as collateral, the system effectively mitigates the inherent volatility of cryptocurrencies while eliminating reliance on centralized stablecoin issuers.

The protocol incorporates a robust overcollateralization mechanism, ensuring that all issued stablecoins are backed by assets exceeding their value. This is further strengthened by an algorithmic minting and burning process, which dynamically regulates supply based on user interactions and collateral positions. A key innovation of the system is the introduction of the Health Factor, a real-time risk assessment metric that continuously evaluates the safety of user positions. This mechanism plays a crucial role in preventing excessive borrowing and safeguarding the overall solvency of the protocol.

To handle risk scenarios, the system employs an incentivized liquidation mechanism, allowing third parties to liquidate undercollateralized positions efficiently. This not only maintains system stability but also ensures continuous operation even during extreme market fluctuations. The integration of decentralized oracle networks through Chainlink price feeds, supported by a custom-built OracleLib, enhances data reliability by preventing the use of stale or inaccurate price information. As a result, the protocol maintains precise collateral valuation and reduces vulnerabilities associated with external data dependencies.

From a security perspective, the protocol follows best practices in smart contract development, including reentrancy protection, modular architecture, and rigorous validation checks, thereby improving both reliability and maintainability. These design choices contribute to building a secure and trustless financial system. The experimental evaluation of the DSC protocol demonstrates its ability to enforce collateral constraints, maintain price stability, and operate efficiently under varying market conditions. The system successfully balances decentralization with risk management, providing users with a transparent and secure platform for stable value storage and decentralized lending.

In conclusion, the proposed DSC protocol effectively bridges the gap between highly volatile cryptocurrencies and the demand for stable financial instruments. By combining strong collateral mechanisms, reliable oracle integration, and secure smart contract design, this work contributes to the advancement of scalable, trustless, and resilient financial infrastructure within the DeFi ecosystem.

6. REFERENCES

[[1] S. Nakamoto, *"Bitcoin: A Peer-to-Peer Electronic Cash System,"* 2008.
[2] V. Buterin, *"Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform,"* 2014.
[3] Chainlink Labs, *"Chainlink: A Decentralized Oracle Network,"* [Online]. Available: https://chain.link
[4] OpenZeppelin, *"OpenZeppelin Contracts Library,"* [Online]. Available: https://github.com/OpenZeppelin/openzeppelin-contracts
[5] Foundry, *"Foundry Book: Ethereum Development Toolkit,"* [Online]. Available: https://book.getfoundry.sh/
[6] MakerDAO, *"The Dai Stablecoin System,"* [Online]. Available: https://makerdao.com
[7] J. Kwon and D. Shin, *"Terra: A Stablecoin Protocol,"* 2019.
[8] P. Schär, *"Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets," Federal Reserve Bank of St. Louis Review*, vol. 103, no. 2, pp. 153–174, 2021.
[9] M. Mita, M. Ito, S. Ohsawa, and S. Tanaka, *"What is Stablecoin?: A Survey on Price Stabilization Mechanisms for Decentralized Payment Systems,"* 2019.
[10] A. Gudgeon, D. Perez, D. Harz, B. Livshits, and A. Gervais, *"The Decentralized Financial Crisis," IEEE Security & Privacy*, 2020.
[11] Ethereum Foundation, *"ERC-20 Token Standard,"* [Online]. Available: https://eips.ethereum.org/EIPS/eip-20
[12] Chainlink Documentation, *"AggregatorV3Interface and Price Feeds,"* [Online]. Available: https://docs.chain.link
[13] K. Qin, L. Zhou, and A. Gervais, *"Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit,"* 2021.
[14] L. Leshner and G. Hayes, *"Compound: The Money Market Protocol,"* 2019.
[15] Aave Protocol, *"Aave: Open Source and Non-Custodial Liquidity Protocol,"* [Online]. Available: https://aave.com
[16] Uniswap Labs, *"Uniswap Whitepaper,"* 2018.
[17] D. Perez, S. M. Werner, J. Xu, and B. Livshits, *"Liquidations: DeFi's Achilles Heel,"* 2020.
[18] International Monetary Fund (IMF), *"The Rise of Stablecoins,"* 2021.
[19] Bank for International Settlements (BIS), *"Stablecoins: Risks, Potential and Regulation,"* 2020.
[20] M. Dell'Erba, *"Stablecoins in Cryptoeconomics: From Initial Coin Offerings to Central Bank Digital Currencies,"* 2019.
[21] Ethereum Foundation, *"Solidity Documentation,"* [Online]. Available: https://docs.soliditylang.org
[22] SmartContractKit, *"Chainlink Whitepaper 2.0,"* 2021.

[23] OpenZeppelin, *"Security Best Practices for Smart Contracts,"* [Online]. Available: https://docs.openzeppelin.com

[24] B. Xu, D. Livshits, and A. Gervais, *"SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols,"* ACM Computing Surveys, 2023.

[25] K. Werner, D. Perez, and A. Gervais, *"Automated Market Makers: Theory and Practice,"* IEEE Symposium on Security and Privacy Workshops (SPW), 2022