0.1 Conclusion

The research and development of the Multi-chain Stablecoin Protocol have resulted in a significant architectural advancement within the Decentralized Finance landscape. When compared to existing solutions, the proposed system demonstrates distinct advantages over both single-chain lending protocols and traditional cross-chain bridges. Unlike protocols such as MakerDAO, which are confined to the liquidity of a single network, this system successfully unlocks the value of assets across heterogeneous chains without forcing users to migrate their capital physically. Furthermore, in contrast to the prevalent "Lock-and-Mint" bridge models that introduce systemic risk through the creation of wrapped assets, the "State Orchestration" architecture developed in this thesis maintains the security of native collateral. By synchronizing the financial state rather than the asset itself, the protocol minimizes the attack surface and eliminates the dependency on fragile wrapped token pegs.

Throughout the implementation of this thesis, several critical objectives have been achieved. The most notable contribution is the successful validation of the Hub-and-Spoke architecture, proving that the high-performance Solana blockchain can effectively serve as a global settlement layer for slower, liquidity-rich EVM networks. The project also introduced a novel cryptographic innovation with the Universal Wallet, leveraging Solana's native Secp256k1 program to allow Ethereum users to control their cross-chain positions trustlessly. This eliminates the significant user experience friction typically associated with managing multiple wallet standards. From a reliability standpoint, the integration of the Mutex locking mechanism on EVM controllers and the Saga pattern for error handling has proven robust, ensuring data consistency and zero fund loss even under simulated network partition scenarios.

However, the current iteration of the system is not without limitations. The most prominent constraint is the centralization of the Guardian infrastructure. While the middleware functions correctly as a proof-of-concept, it currently operates as a single server, representing a single point of failure and a trusted setup that contradicts the core ethos of decentralization. Reflecting on the process, the most valuable lesson learned was the paradigm shift required to design for "Eventual Consistency" rather than "Atomic Transactions." Developing for asynchronous distributed ledgers required a defensive programming approach, accepting that state synchronization is probabilistic and time-dependent, necessitating rigorous fail-safe mechanisms like the implemented revert logic.

0.2 Future Work

To transition this academic prototype into a production-ready protocol, the immediate focus of future work must address the hardening of the system's security and reliability. The primary task is the decentralization of the Guardian Network. The current single-node middleware must be evolved into a consensus-based network of validators. This involves implementing a threshold signature scheme or a multi-party computation (MPC) framework, requiring a supermajority of independent nodes to attest to an event before a state transition is executed on the Solana Hub. Additionally, prior to any mainnet deployment, the smart contracts across both the EVM and SVM layers require comprehensive security audits by third-party firms to identify and rectify potential reentrancy vectors or arithmetic vulnerabilities that may have escaped the testing phase.

Looking towards the long-term evolution of the protocol, the research opens several avenues for advanced technological integration. A key area for exploration is the replacement of the optimistic Guardian network with Zero-Knowledge (ZK) Proofs. By implementing ZK-Light Clients directly on the Solana smart contracts, the system could mathematically verify the state roots of the Ethereum blockchain, achieving a truly trustless interoperability model that does not rely on human or server-based relayers. Furthermore, the protocol creates a foundation for a decentralized governance model. Future development should include the implementation of a DAO structure, allowing stakeholders to vote on critical risk parameters such as Loan-To-Value ratios and the onboarding of new collateral types, including Real-World Assets, thereby transforming the protocol into a community-owned public infrastructure.