Simão Amaro - Code Audits Lead

Simão is a highly accomplished individual with a Master's degree in Aerospace Engineering from the prestigious Instituto Superior Técnico who brings a unique skill set to the blockchain industry. Aerospace engineering graduates, like Simão, possess strong analytical thinking, problem-solving, and attention-to-detail skills, enabling him to approach projects with a meticulous and systematic approach.

Programming Languages

- Solidity, Javascript, and Python

Simão's Journey at Three Sigma

Simão's passion for software development, security, coding tools, infrastructure, and blockchain led him to join Three Sigma. His expertise in conducting code audits and uncovering critical vulnerabilities quickly earned him a leadership role in the code auditing team, where he continuously enhances software security and reliability.

Awards

- 1st place AIBC hackathon gameFi track - Simão showcased his remarkable skills by winning the AIBC hackathon, where he single-handedly developed AZ Worlds, a LayerZero-based game. This cross-chain game employs a finance/skill play-to-earn model where players engage in fierce competition for power and receive rewards.
- 3rd place in the Taiko Infrastructure Prize - Simão's drive for innovation led him to the ETHPrague 2023 hackathon, where he presented SwiftGate, a batch-based bridging protocol. His work drastically reduces the required signatures for asset bridging, improving efficiency and scalability while minimizing cost.
- 2nd place Web3Berlin sponsored by XDC - Simão built DexBook, a decentralized on chain order book with off chain order matching. The orders are efficiently implemented in 2 linked lists, receiving off chain hints for settlements.

Code Audits

- **Maple Finance (4x)** - Lending Markets Redefined.
- **Vertex -** Lightning-fast orderbook DEX with powerful trading features & cross-margining for max efficiency
- **Singularity -** Similar to Tornado Cash but with KYC
- **Ostium -** Onchain Perps for Real World Assets
- **NFT Perp** - Perpetual futures DEX for NFTs
- **Clip Finance** - Infrastructure layer for cross-chain yield products
- **Glacier** - Liquid Staking in Avalanche.
- **Fuji Finance** - Cross-chain Lending Protocol
- **leNFT -** NFT trading and borrowing & DEX
- **Yeti Finance** - Borrowing and Lending
- **Keyring** - Zero-knowledge compliance oracle

- **OrdiSwap** - Dynamic AMM infrastructure to BRC-20
- **MetaZero** - RWA Omnichain tokenization
- **OpenLeverage** - Social space with money games.
- **Trestle** - Celestia/Ethereum bridge with staking incentives.

Competitive Audits

#16 Sherlock - LSW

#8 Code4rena last 90 days

#29 Cantina

Best results

- **Exactly Protocol** - Lending - 1st place.
- **PoolTogether V5** - Lending with rng rewards - 1st place.
- **Optimism Safe Extensions** - Safe modules and guard for Optimism - 2nd place.
- **INIT Capital** - Lend, Borrow, and Access Yield Strategies with Liquidity Hook - 2nd place.
- **Arbitrum Fault Proofs** - Fault proofs for the Arbitrum blockchain - 3rd place.
- **Tellor** - Lending - 3rd place.
- **Zivoe** - RWA Lending - 3rd place.
- **TapiocaDAO** - Omnichain stablecoin, borrowing, and lending - 6th place.
- **Perennial V2** - Perennial is built from first principles as a powerful DeFi primitive that scales to meet the needs of traders, LPs, and developers - 7th place.
- **Renzo** - EigenLayer integration - 7th place.
- **Chainlink Staking V2** - Staking smart contracts for Chainlink - 8th place.
- **Titles** - NFTs - 8th place.

Other audits

- **Tokemak** - Borrowing/lending with automated yield allocation.
- **Blast** - Yield bearing L2.
- **GoGoPool -** liquid stacking protocol on Avalanche.
- **Ethos Reserve -** liquidity fork that supports multiple assets.
- **Wenwin -** lottery system that gets winning tickets from Chainlink.
- **Frankencoin -** decentralized Swiss Franc stablecoin backed by other on-chain assets.
- **ENS -** decentralized naming service for Ethereum.
- **AJNA -** peer-to-peer lending/borrowing protocol.
- **Venus -** decentralized money market.
- **Base -** L2 built using the optimism stack**.**
- **ZkSync -** ZK-EVM Layer 2.
- **Ajna Protocol** - lending, borrowing, and trading without governance or oracle.
- **Venus Protocol Isolated Pools** - lending and borrowing protocol on the BNB Chain.
- **veRWA** - voting-escrow incentivization model for Canto RWA (Real World Assets) similar to veCRV with its liquidity gauge.

Engineering Projects

- **Arc Bridge** - Our solidity batch verifier is tailored specifically for Merkle Patricia Tree proofs. This tool enables the verification of multiple leaves simultaneously using a single proof instead of verifying each leaf separately. It significantly reduces computational overhead and accelerates verification, while also minimizing storage requirements for proofs.
- **Defimons NFT Sales contract** - Designed and developed the new Whitelist sale type that integrates a Merkle Tree structure to allocate NFT quantities to eligible participants, ensuring a fair and transparent distribution process.
- **Mezzanote fully on-chain NFTs** - Successfully integrated SSTORE2 into their infrastructure to optimize storage and enhance the efficiency of on-chain data management, while implementing on-chain data compression techniques to reduce storage costs and improve overall performance.
- **Slither automatic detectors** - To further strengthen the security of the code developed and audited at Three Sigma, we have developed custom detectors tailored to our specific requirements. These detectors seamlessly integrate with Slither, allowing us to conduct comprehensive code analysis and efficiently identify and address potential vulnerabilities.
- **Automated Audit Report Generator** - To simplify and standardize the auditing process, we have developed an automated audit report generator that eliminates the need for manual compilation and formatting of audit findings. This tool fetches GitHub issues from a repository with a predefined structure and seamlessly parses them into a comprehensive report.