FRANK CASTLE

RUST/SOLANA AUDITOR

CONTACT INFO

https://x.com/0xcastle_chain

https://t.me/castle_chain

castlechain99@gmail.com

https://github.com/Frankcastleauditor

ABOUT FRANK CASTLE

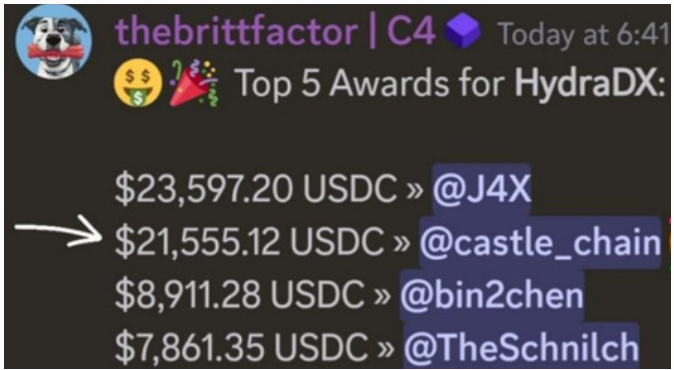
Frank Castle is a seasoned smart contract security researcher with a focused expertise in auditing Rust-based contracts and decentralized infrastructure across leading blockchain ecosystems, including **Solana** , **Polkadot** , and **Cosmos** (CosmWasm). Frank's experience includes work with industry-renowned audit firms such as **Pashov Audit Group** and **Shieldify Audit** Company, in addition to competitive auditing platforms like **Code4rena** and **Cantina**.

Frank Castle has successfully conducted over 6 **Solana** private audits with **Pashov Audit Group**, more than 3 **Solana** audits with **Shieldify**, and completed over **15 private audits**, establishing a track record of rigor and excellence in smart contract security. His comprehensive experience and hands-on knowledge with **Rust-based** ecosystems underscore his commitment to advancing blockchain security and best practices.

PUBLIC ACHIEVEMENTS

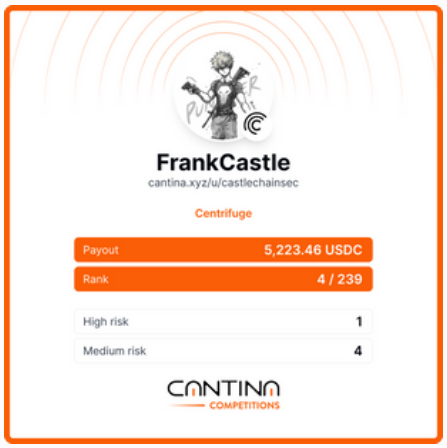
1. **HydraDX Omnipool Audit, Code4rena:** Demonstrated excellence by securing 2nd place in the largest Rust audit in Code4rena history, which was also the platform's first-ever Polkadot contest. Frank identified a **critical high-severity** finding and multiple medium-severity issues, achieving a solo high for the competition. This achievement was rewarded with $21,555.12 USDC.

Contest link : https://code4rena.com/reports/2024-02-hydradx



2. **Centrifuge Audit, Cantina :** Achieved 4th place in the highly competitive Centrifuge audit, surpassing over 240 participants. Frank's findings included one **high-severity issue** and **four medium-severity** issues, securing a reward of 5,220 USDC.

Contest Link : :https://cantina.xyz/competitions/a0a58a8b-247e-4203-b3cb-476ded9d5515



PRIVATE ACHIEVEMENTS

- I have completed over 6 **Solana** private audits with Pashov Audit Group for large protocols like **LayerZero** and **Hydration** "L1 implementation" ,and **Pump.fun** within a span of two months, uncovering approximately 5 critical, 15 high, 30 medium, and over 50 low-severity issues. Due to my consistent performance and exceptional results, I am regularly assigned **Solana** and Rust audits by the Audit Group, reflecting their confidence in my expertise and meticulous approach.

- I have completed three private **Solana** audits with **Shieldify Security,** where I identified multiple critical issues and vulnerabilities. This work reflects my commitment to uncovering and addressing high-risk vulnerabilities in complex smart contract environments.

- I have successfully completed over ten private **Solana** audits, along with two audits for **Polkadot** and one for **CosmWasm**. This diverse experience across multiple blockchain ecosystems underscores my adaptability and depth in smart contract security research.

All my **+10 private audits** can be found in this GitHub repository, along with their reports and the number of findings identified.
Github repo : https://github.com/Frankcastleauditor/public-audits/blob/main/README.md

SKILLS

- Problem Solving and Analysis
- Rust-Based Blockchain experience
- Smart Contract Auditing and Security
- Blockchain Infrastructure and Protocol Knowledge
- Testing Techniques
- Competitive Security

EXPERIENCES

HydraDX Omnipool Audit

Role: Smart Contract Auditor

Audited HydraDX's Omnipool, a next-gen single-pool AMM on Polkadot, focused on maximizing liquidity efficiency.

Key Components Audited:
Omnipool: Assessed the security of a unified liquidity pool for all assets.
Stableswap: Evaluated low-slippage AMM mechanics designed for stablecoins.
Oracle: Reviewed EMA-based pricing for accuracy and resistance to manipulation.
Circuit Breaker: Analyzed liquidity flow controls to prevent excessive asset movements.

Key Vulnerabilities Identified:
Liquidity Drainage: Discovered a flaw allowing liquidity exhaustion in stableswap by setting `asset_in` to `asset_out`.
Total Liquidity Removal: Uncovered that removing all liquidity could disable future liquidity additions and share minting.
User Fund Loss on Price Manipulation: Found potential losses for users unable to withdraw fairly after swap disablement due to manipulated prices.

Skills Gained:
- Advanced AMM and Oracle security
- Circuit Breaker mechanisms for flash loan defense

Centrifuge Audit

Role: Smart Contract Auditor

Audited **Centrifuge,** a Substrate-based protocol enabling on-chain financing of real-world assets for transparent, decentralized borrower-lender transactions.

Key Components Audited:
- **Asset Tokenization**: Assessed security of real-world asset tokenization, ensuring accurate on-chain representation and robust risk management.
- **Liquidity Pools**: Reviewed cross-chain liquidity aggregation for L1 and L2 integrations, providing stable yield generation for investors.
- **Collateral Management:** Evaluated mechanisms for collateralized lending and yield generation, focusing on secure asset-backed borrowing.

Skills Gained:
- Advanced tokenization and collateral management
- Cross-chain liquidity security

LayerZero OFT V2 Audit

Role: Solana Auditor

Audited **LayerZero** OFT V2 for **Solana**, focusing on secure **cross-chain messaging** and token interoperability within LayerZero's omnichain ecosystem. The audit involved a detailed review of LayerZero's message handling and token transfer functionalities, covering essential components to ensure security and consistency across chain interactions.

Key Components Audited:
- **init_oft**: Examined initialization logic for creating Omnichain Fungible Token (OFT) instances, focusing on preventing manipulation during token setup and configuration.
- **lz_receive and lz_receive_types**: Assessed LayerZero's message receiving functions, ensuring data integrity and type safety for incoming cross-chain messages.
- **quote_oft and quote_send**: Reviewed pricing and quote calculations for token transfers, checking for consistent rate handling to prevent discrepancies in cross-chain transactions.
- **send and set_oft_config**: Verified the security of token sending operations and configuration updates for OFTs, preventing unauthorized changes in token parameters.

Key Vulnerabilities Identified:
1. **Mint Decimal Manipulation:** Found that attackers could manipulate `ld2sd_rate`, inflating token amounts received when transferring from Ethereum to Solana by exploiting discrepancies in rate settings.
2. **Inconsistent Message Composition**: Identified variations in `compose_msg` functions that could lead to errors in message handling, risking unexpected behavior in certain scenarios.

Skills Gained:
- Advanced cross-chain rate management and token accounting
- Consistent message composition for secure omnichain messaging

PROFILES

- Code4rena profile : https://code4rena.com/@castle_chain
- Sherlock Public profile : https://audits.sherlock.xyz/watson/castle_chain
- Cantina profile : https://cantina.xyz/u/castlechainsec
- Github profile : https://github.com/Frankcastleauditor
- X profile : https://x.com/0xcastle_chain