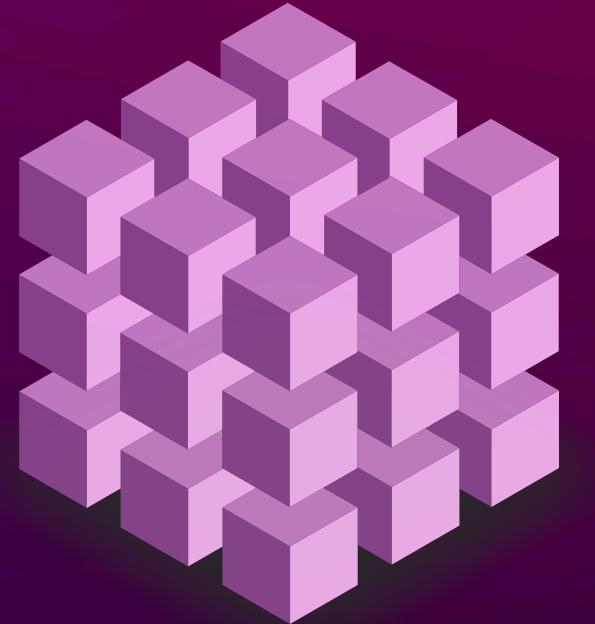


Progetto DeFi: Attacco tramite Manipolazione degli Oracle

Nitesh Kumawat

Corso: BLOCKCHAIN AND CRYPTOCURRENCIES



Introduzione: DeFi e il Ruolo degli Oracoli

- 1 La DeFi ha rivoluzionato i servizi finanziari, rendendoli aperti, trasparenti e accessibili.
- 2 Tuttavia, la sua rapida evoluzione ha esposto nuove superfici di attacco, come la manipolazione degli oracoli di prezzo.
- 3 Gli oracoli sono servizi di terze parti che forniscono dati esterni (es. tassi di cambio) alle blockchain.
- 4 La loro integrità è fondamentale per il corretto funzionamento dei protocolli DeFi.

Obiettivo del Progetto

Dimostrare

Evidenziare la vulnerabilità dei protocolli DeFi che si affidano a oracoli di prezzo on-chain non robusti.



Analizzare

Comprendere le meccaniche di un attacco di manipolazione del prezzo orchestrato tramite flash loan.



Scenari

Esplorare due distinti scenari di attacco per una comprensione approfondita



Metodologia: Due Scenari di Attacco



Analisi 1

Simulazione di un attacco in un ambiente didattico con protocolli semplificati (SimpleLender.sol e SimpleAMM.sol).



Obiettivo Analisi 1

Illustrare come la bassa liquidità possa essere sfruttata per alterare il prezzo e contrarre prestiti sottocollateralizzati.



Analisi 2

Simulazione di un attacco in un contesto più realistico, sfruttando un flash loan da Aave per manipolare il prezzo spot di una pool Uniswap V2.



Obiettivo Fase 2

dimostrare la fattibilità pratica con strumenti e protocolli standard del settore

Analisi 1: Ambiente Controllato e Didattico

1

SimpleAMM.sol: AMM semplificato, agisce come oracolo di prezzo vulnerabile a causa della dipendenza diretta dalle riserve di liquidità

2

SimpleLender.sol: Protocollo di prestito di base, utilizza SimpleAMM come unica fonte di prezzo.

3

Attacker.sol: Contratto che orchestra l'attacco in una singola transazione atomica (simulando un flash loan)

Architettura del Protocollo (Semplificata):



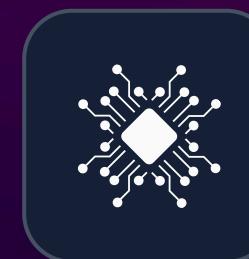
Acquisizione capitale (ETH) tramite simulazione flash loan.



Manipolazione del prezzo: swap significativo di ETH per USDC in SimpleAMM, gonfiando artificialmente il prezzo di USDC.



Deposito dell'USDC manipolato come garanzia in SimpleLender.



Richiesta di prestito ETH sovradimensionato basato sul prezzo manipolato.



Ripagamento del "flash loan" iniziale e realizzazione del profitto.

Attacco Realistico su Fork della Mainnet Ethereum

1

LendingProtocol.sol è un contratto vulnerabile che permette di depositare USDC e prendere in prestito WETH, usando un prezzo spot manipolabile da Uniswap V2

2

Attack.sol: contratto attaccante che interagisce con Aave V3 (flash loan) e Uniswap V2 Router (per manipolare il prezzo spot)

Architettura del Protocollo (Reale):



Flash loan di 1000 WETH da Aave



Manipolazione del prezzo su Uniswap: vendi 1000 WETH per USDC → il prezzo WETH scende



Deposito degli USDC (ottenuti dallo swap) come collaterale nel protocollo Lending

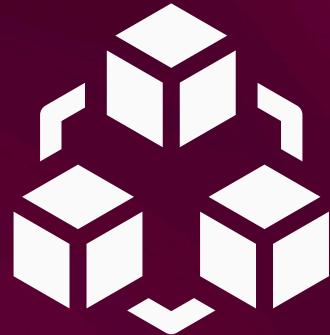


Richiesta di prestito di WETH, sfruttando il prezzo manipolato (ti danno più WETH del dovuto)



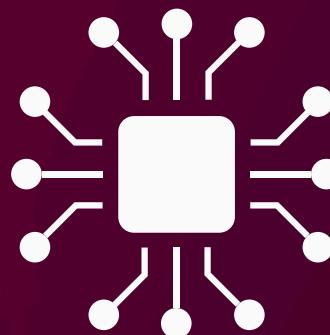
Rimborso del flash loan (1000 WETH + fee) con parte dei WETH ricevuti

La Vulnerabilità Chiave: Oracoli Spot



Prezzi Instantanei Vulnerabili

I protocolli si affidano a prezzi "spot" diretti dalle pool AMM.



Amplificazione con Flash Loan

Gli attacchi usano flash loan per manipolare i prezzi e sfruttare la discrepanza in una singola transazione atomica



Mancanza di Resilienza

Assenza di TWAP o oracoli aggregati espone a perdite finanziarie

Soluzioni: Verso Oracoli Robusti

TWAP

Adottare Time-Weighted Average Prices per resistere a manipolazioni istantanee.



Oracoli Aggregati

Integrare con soluzioni come Chainlink, che usano fonti multiple.

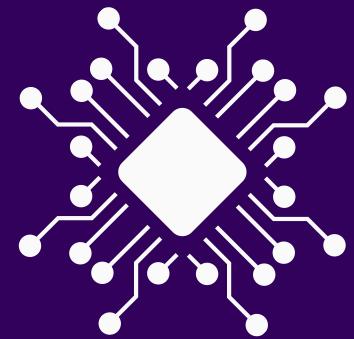


Maggiore Liquidità

Aumentare la liquidità delle pool rende la manipolazione economicamente impraticabile.

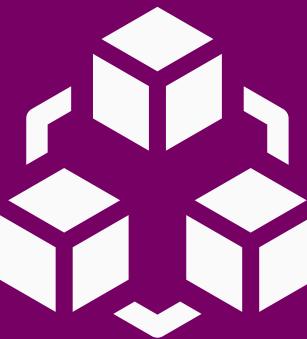


Conclusioni Finali



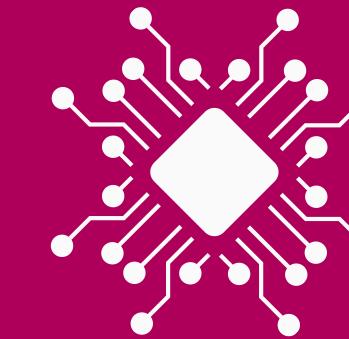
Vulnerabilità degli Oracoli Spot

Gli attacchi dimostrano la fragilità dei protocolli che usano oracoli di prezzo istantanei.



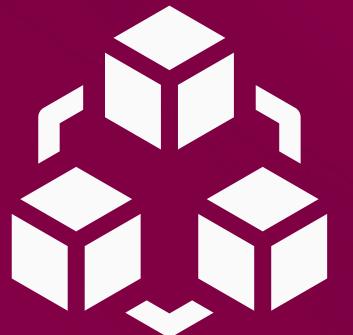
Impatto Critico sulla DeFi

La sicurezza dei fondi dipende direttamente da oracoli robusti e resistenti alla manipolazione



Necessità di Evoluzione

Adottare soluzioni avanzate è cruciale per la stabilità e fiducia nell'ecosistema DeFi.



GRAZIE

MILLE

