Course IV:

DeFi Risks and Opportunities

2. Governance, DNS, Oracle Risk, DEX and Custodial Risks

(iii) Oracle Attack

Risks: Oracle risk

What is oracle risk?

- Oracles are one of the last unsolved problems in DeFi and are required by most DeFi protocols in order to function correctly.
- Fundamentally, oracles aim to answer the simple question: How can off-chain data be securely reported on chain?
- Without oracles, blockchains are completely self-encapsulated and have no knowledge of the outside world other than the transactions added to the native blockchain.

Risks: Oracle risk

What is oracle risk?

- Many DeFi protocols require access to secure, tamper-resistant asset prices to ensure that routine actions, such as liquidations and prediction market resolutions, function correctly.
- Protocol reliance on these data feeds introduces *oracle risk*.
- If an oracle's *Cost of Corruption* is ever less than an attacker's potential *Profit from Corruption*, the oracle is extremely vulnerable to attack.

Risks: Oracle risk

Types: Shelling-point oracle

- This oracle relies on the owners of a fixed-supply token to vote on the outcome of an event or report the price of an asset.
- Examples of this type of oracle include Augur and UMA.
- While Schelling-point oracles preserve the decentralization components of protocols that rely on them, they suffer from slow times to resolution.

Risks: Oracle risk

Types: API oracle

- These oracles are centralized entities that respond asynchronously to requests for data or prices.
- Examples include Provable, Oraclize, and Chainlink. All systems relying on API-based oracles, must trust the data provider to respond accurately to all queries.

Risks: Oracle risk

Types: Application-specific oracle service

- This type of oracle is used by Maker and Compound.
- Its design differs based on the requirements of the protocol it was developed for.
- For example, Compound relies on a single data provider that the Compound team controls to provide all on-chain price data to the Compound oracle.

Risks: Oracle risk

Highest risk

- Oracles, as they exist today, represent the highest risk to DeFi protocols that rely on them.
- All on-chain oracles are vulnerable to front-running, and millions of dollars have been lost due to arbitrageurs.
- Additionally, oracle services, including Chainlink and Maker, have suffered crippling outages with catastrophic downstream effects.
- Until oracles are blockchain native, hardened, and proven resilient, they represent the largest systemic threat to DeFi today.