Game theoretic security vulnerabilities in Chainlink

TU Delft

CSE3000 Research Project
Security Analysis of Decentralized Finance (DeFi) Systems

By Hans Dekker (4692357, j.l.dekker@student.tudelft.nl)
Supervisor: Oğuzhan Ersoy
Responsible professor: Zekeriya Erkin

1. Background

DeFi protocols need real world information
Oracles provide this information
How do we know data is valid?

Chainlink

Chainlink: Decentralized Oracle Network
Network of oracle nodes
Answers aggregated, correct answers rewarded
Two tiers:

- Tier 1 nodes provide data,
- Tier 2 nodes resolve disputes

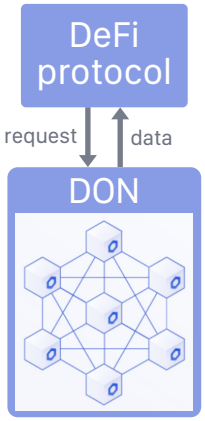

Figure 1: Decentralized Oracle Network

2. Problem: lack of transparent incentives

Security relies on future revenue of Tier 2: not transparent to users
Users can not verify game theoretic security

Table 1: Expected profit of N2 given Tier 2 consensus and variable definitions

N2	Tier 2 consensus: Honest	Tier 2 consensus: Dishonest
Honest	F	$F + \Delta F$
Dishonest	0	$M + B + S$

F	Expected future revenue
ΔF	Change in expected future revenue. Assumed to be greater than 0 on grounds of dishonest majority losing credibility and larger total revenue going to honest nodes
M	Expected profit gained by exploiting corrupted data
B	Expected profit gained by bribes
S	Expected profit gained through short selling

3. Research Question

How can we mitigate the game theoretic security vulnerabilities
In Chainlink's Decentralized Oracle Networks?

4. Methodology

Literature & documentation study
Comparing payoff matrices

5. Mitigation: explicit financial incentive

Require Tier 2 nodes to lock LINK tokens: st
Honest stakeholders fork the system after an attack

In the forked network,
dishonest nodes lose their tokens
Tokens in old network become worthless
Results in cost of st for dishonest nodes

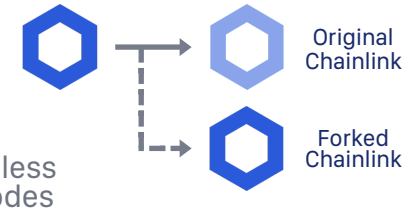

Figure 2: Forking mechanism

6. Results

Users can estimate whether $\mathrm{st} \geq$ profit from dishonest behaviour
Even though the expected value of future revenue is unclear
Users can verify that profit gained by dishonest behaviour ≈ 0

Table 2: Expected profit of N2 given Tier 2 consensus and mitigation

N2	Tier 2 consensus: Honest	Tier 2 consensus: Dishonest
Honest	F	$F + \Delta F$
Dishonest	0	$M + B - st$