Security Evaluation of GoQuorum-based Smart Contracts

A Case Study of Malfunctioning Access Control and Private State Divergence

By Cheyenne Slager
b.c.slager@student.tudelft.nl

Under supervision of Prof. Dr. Kaitai Liang

1. Research Question

"What are security vulnerabilities of GoQuorum-based smart contracts and how can they be mitigated?"

2. Problem Statement

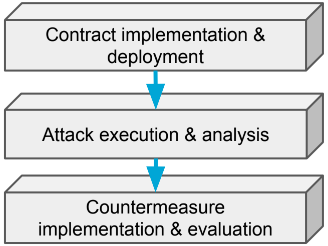
GoQuorum is an enterprise blockchain platform that supports smart contracts and enables private transactions.

Smart contracts enable automated payment while eliminating the need for third-party involvement.

Vulnerabilities with regard to the privacy and security aspects of smart contracts still exist

At risk are great financial losses.

3. Methodology


Contract implementation & deployment

Attack execution & analysis

Countermeasure implementation & evaluation

7. Conclusion

State consistency and **transaction privacy** can both be maintained without third party involvement by using **ZKP**'s. However, no quick fix is readily available. Further research is recommended.

Malfunctioning access control due incorrect use of ***tx.origin*** can be detected with analysis tools; MythX is recommended. Using *msg.sender* fixes the vulnerability.

4. Vulnerabilities

Private state divergence

Since private transactions are not available to all network participants, private states can diverge. If Mallory privately sends tokens to Bob, Alice does not know, allowing Mallory transfer the same tokens to Alice

Malfunctioning access control

Using *tx.origin* is a faulty way of validating the caller of a function, since it represents the very first account in the complete call chain, rather than the most recent one.

5. Attacks

Double spending

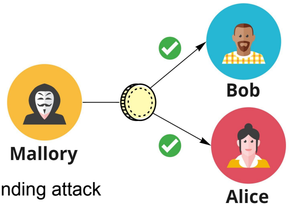


Figure 1 Double-spending attack

Phishing

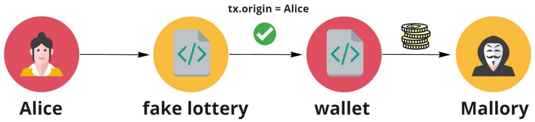


Figure 2 Phishing attack through a malicious lottery contract

6. Countermeasures

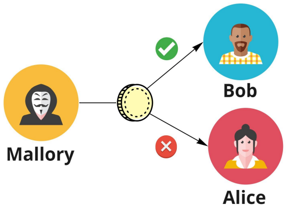


Figure 3 Averted double-spending

Private state validation in GoQuorum requires transactions to be shared with all participants of a private contract but compromises privacy.

Regulator nodes and **Off-chain validators** detect invalid transactions but exposes data and introduce third-party dependence.

Zero Knowledge Protocols (ZKP) prevent double spending while maintaining privacy.

msg.sender instead of *tx.origin,* since it represents the direct caller.

Static and dynamic analysis tools such as Mythril, Porosity and Remix Analyzer detect vulnerable code.

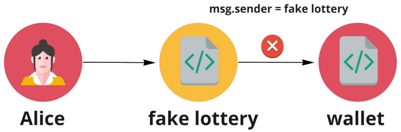


Figure 4 Prohibited attack due to detection of the direct caller