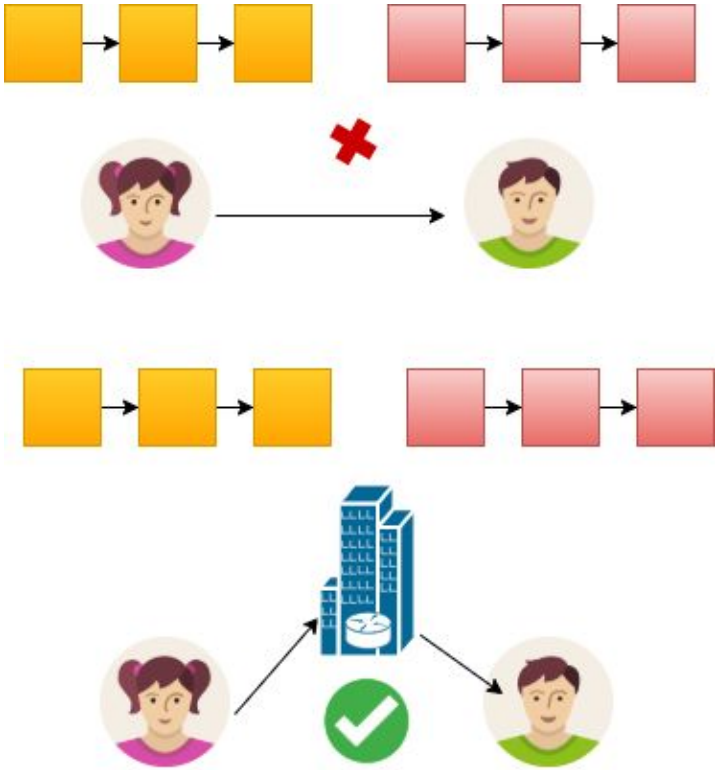
Design and Development of Tools and Techniques for Improving Security in Blockchain Interoperability

Roshan Singh (214101043)

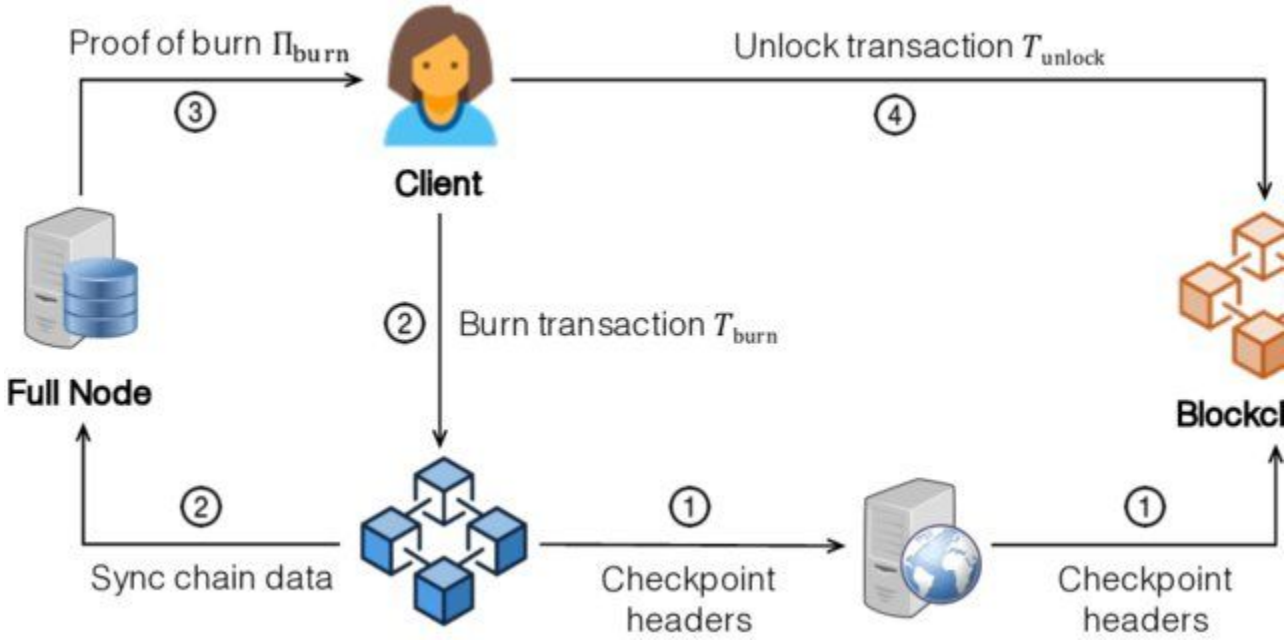
Thesis Supervisor - Prof. Sukumar Nandi

1. Introduction to Interoperability Problem in Blockchains



1. Blockchains can't inherently communicate with each other
2. Exchanges are not desirable
3. Cross Chain bridges can help here

2. Cross Chain Bridges



Source : https://www.researchgate.net/publication/348563271_Horizon_A_Gas-Efficient_Trustless_Bridge_for_Cross-Chain_Transactions/figures?lo=1

3. Problem Statement

“The public blockchain ecosystem lacks of proper tooling framework for management and monitoring of cross-chain bridges ”

“Design and Develop cross chain bridge management framework ”

4. Significance of the Problem

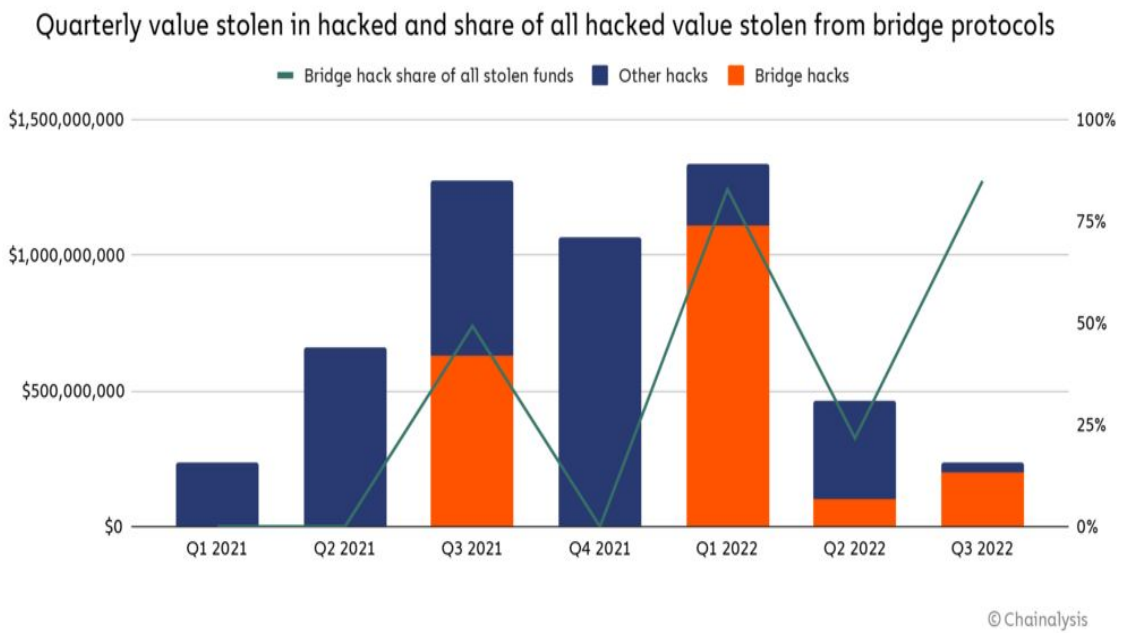


Image Source : https://blog.chainalysis.com/reports/cross-chain-bridge-hacks-2022/

Hack	Year	Losses
Ronin	March,2022	600 Millions USD
Nomad	August 2022	200 Millions USD
Wormhole	February 2022	375 Millions USD

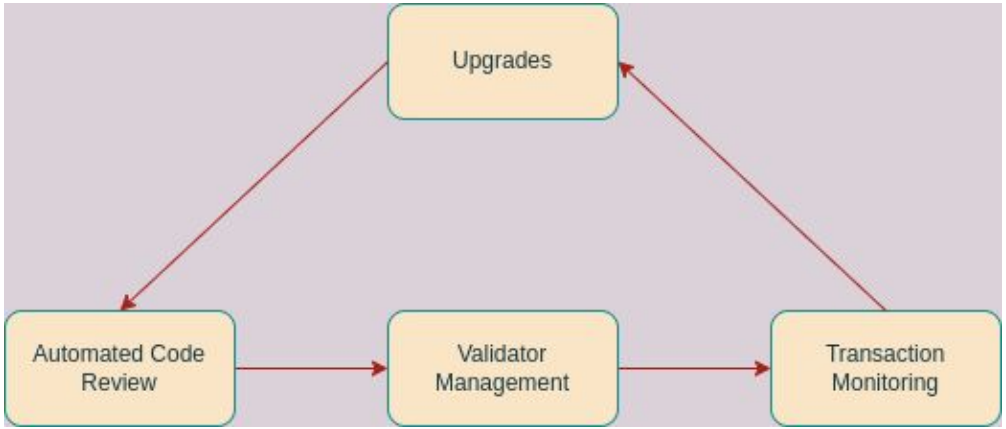
Bridge Hack - 69%, Total Losses- 2 Billion USD

5. Literature Survey

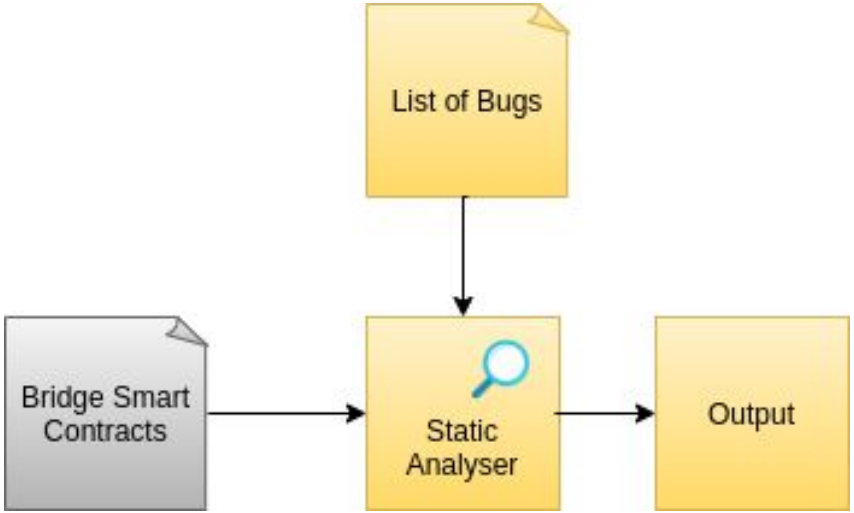
Papers Considered for Study			
Sl. No.	Title	Year	Venue
1	Not Quite Water Under the Bridge: Review of Cross-Chain Bridge Hacks	2022	Preprint
2	A Survey on Blockchain Interoperability: Past, Present, and Future Trends	2021	ACM Computing Surveys
3	Trustless, privacy-preserving blockchain bridges	2021	Preprint
4	Blockchain Gateways, Bridges and Delegated Hash-Locks	2021	Semantic Scholar

Key Takeaways
Insufficient Code Auditing
Improper Validator Management
Lack of Monitoring tool

6. Proposed Solution

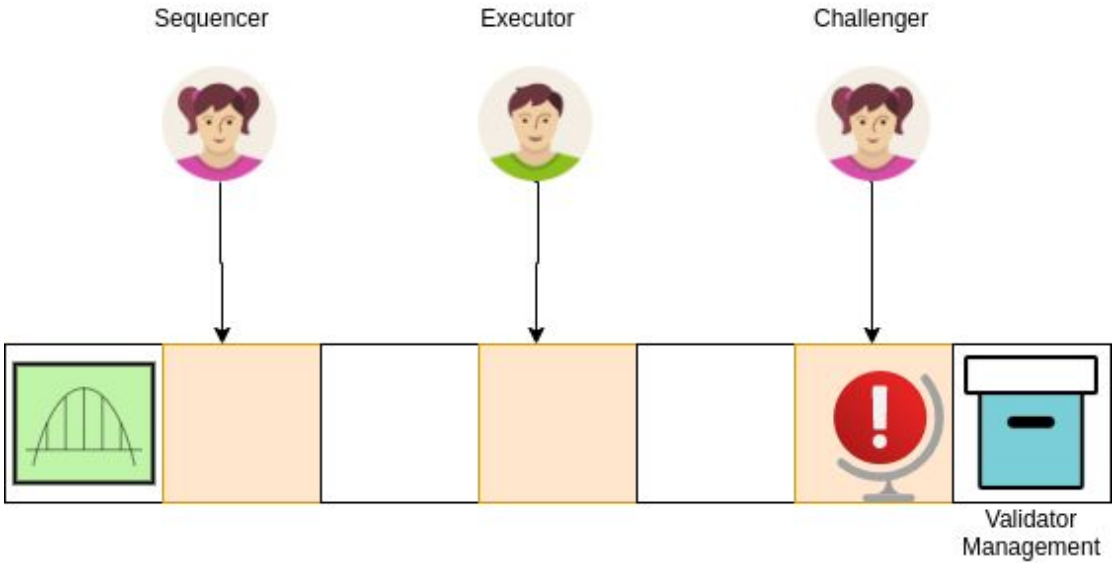


7. Static Code Analysis

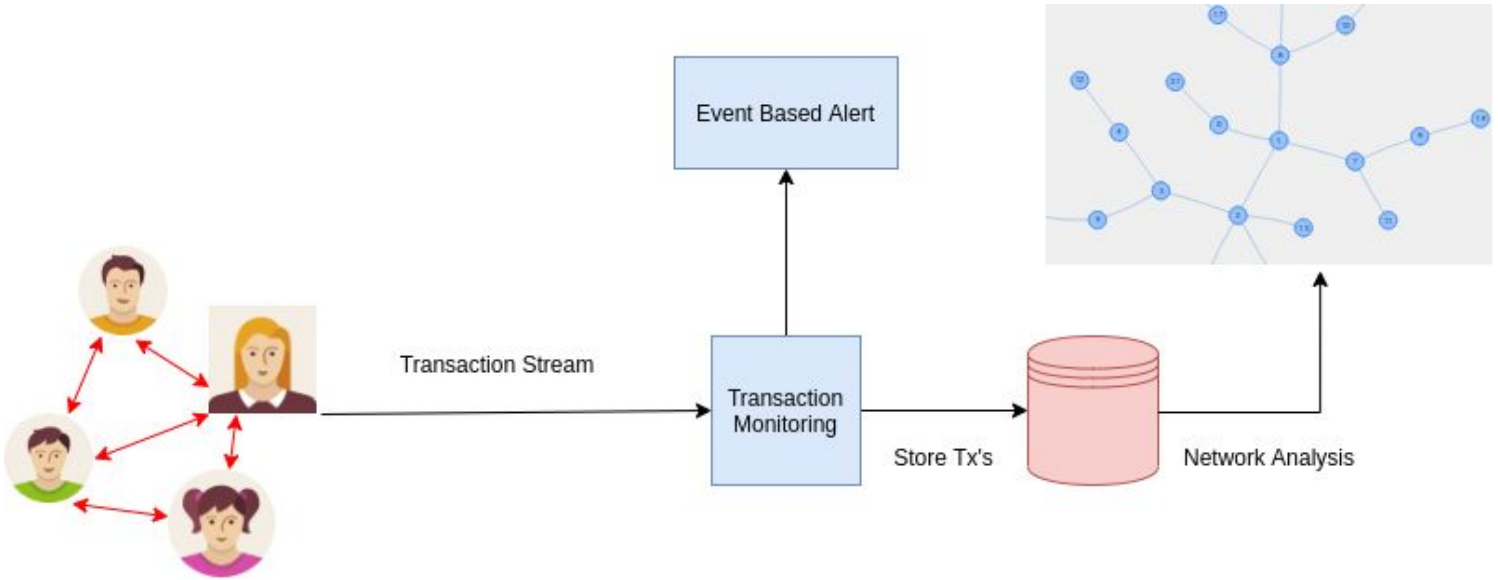


Detectors
Locked Ether
Fake Deposit
Privilege Escalation

8. Validator Management



9. Transaction Monitoring



10. Future Works

Development of an integrated bridge monitoring and maintenance tool

i) Implementation
ii) Testing

Development and comparison of efficient validator management strategies