

An Engineering Framework for the Generation of Robust & Verifiable Smart Contracts (GRV-SC)

A Smart Contract is an immutable executable piece of code that resides on a blockchain network to automate digital workflows by incorporating business logic. Smart Contracts are complex, error prone, and difficult to understand.

A single mistake in defining business workflow or exploitation of one security vulnerability have shown to incur significant economic loss (Millions \$) or penalties. The implementation of intelligent verification mechanisms for smart contracts will greatly increase trust in Blockchain applications and as such this PhD will develop a model driven approach that incorporates innovative methods for specifying and validating robust contracts.

The GRV-SC framework offers developers a cross-platform single stop solution by providing a Smart Contract Designer, Validation Tools and a Test Execution Environment as part of an automated workflow.

It ensures the security, resilience, extensibility, and risk management of Contracts development at pre-deployment step via Smart Contract Modeling, and automated formal verification methods.

Post-deployment stage provides a set of auto-generated test scenarios that validate the contract's privacy and scalability on real ledger networks. This Smart Contract lifecycle management is designed using versatile set of technologies.

Why GRV-SC

- Reduced Learning Curve for SC coding
- Visual Modeling & Verification
- Code Reliability, Correctness, and Robustness before blockchain deployment
- Reusability & Recommendation of Existing Test Cases
- A prototype framework specification and validation of Smart Contracts across multiple ledger technologies.

