# Exploit smart contracts

#### Student name: Zhuohao Liang (Z.Liang7@newcastle.ac.uk)

#### Student number: B170243845

#### Supervisor: Dr. Changyu Dong [(changyu.dong@newcastle.ac.uk)](mailto:(changyu.dong@newcastle.ac.uk))

**Project Aim:**

1 survey common exploits of smart contracts

2 implement demonstrators of exploits on Ethereum testnet -- note some old exploits may have been fixed

3 (optional) find new exploits Priority will be given to Computer Security and Resilience students.

**Project Objectives: bullet points. summarising what you're hoping to achieve in order to fulfill your overall aim. Include personal objectives as well as technical objectives.**

I propose to review the available literature on example of current smart contract exploit and how can they been resolved. In this review, I will achieve the following three goals:

1. master the program language: solidity
2. ?set up own private chain on ethereum testnet
3. Give some resolution to exploit which are still not fixed.

**Description: 2 or 3 paragraphs explaining what the project is about. Indicate where the main focus of the project lies.**

Ethereum and complex blockchain programs are new and highly experimental. Therefore, you should expect constant changes in the security landscape, as new bugs and security risks are discovered, and new best practices are developed.All users on the blockchain can see blockchain-based smart contracts. However, this will cause all vulnerabilities, including security holes, to be visible. If the smart contract developer neglects or tests insufficiently, and the code of the smart contract causes loopholes, it is very easy for hackers to exploit and attack. And the more powerful smart contracts, the more complex the logic is, and the easier it is to have logical loopholes. At the same time, the smart contract language Solidity itself and the contract design may have loopholes.

As reported by Motherboard, researchers from the National University of Singapore (NUS), Singapore's Yale-NUS College and the UK's University College London (UCL) have discovered a total of 34,200 smart contracts which contain vulnerabilities ripe for exploit.In such situation,I will survey common exploits of smart contracts,explaining its code example,then pick some of them,try to implement how to deal with these exploits.(develop plugin like google extension to detect code exploits,based on remix-ide )

**Initial areas of research: what are you planning to do first?**

Study the basic knowledge of smart contract:how to deploy with solidity program language;

how to install suitable IDE to compile and run contract.

(how to set up own private chain on Ethereum?)

(how to develop google plugin?)

**Expected outcomes: what will you produce by the end of the project?**

1. Investigation on common smart contract exploits,show a list of them and some case of classic code example,following the solution.
2. Choose some recently unresolved exploits,present own resolution and prevention.