# Decompiling Ethereum EVM ByteCode for Static Analysis

Supervisors: Martin Nyx Brain <martin.brain@city.ac.uk> and Michał Król <michal.krol@city.ac.uk>

Ethereum ( https://ethereum.org/ ) is one of the most exciting block chain technologies as it is not just a cryptocurrency but also supports smart-contracts. These are programs that are written in a variety of programming languages and compiled to EVM ( https://eth.wiki/concepts/evm/evm ), a byte-code format similar to JVM, before they are run on the blockchain. The security of these contracts is vital as they can control significant amounts of cryptocurrency.

This project is to write a decompiler (or extend an existing decompiler such as https://github.com/MrLuit/evm ) so that it can convert EVM byte code into C that can be handled by the CPROVER tools ( http://www.cprover.org/cprover-manual/cbmc/tutorial/ ).

Skills: understanding of low-level programming, system architecture and operating systems, good understanding of the C programming language, interest or knowledge of Ethereum, cryptocurrency or blockchains.

Drop In with Martin: Wednesday 1st December 14:00–16:00, e-mail <martin.brain@city.ac.uk> to book a slot!

To discuss the project with Michał Król <michal.krol@city.ac.uk> either email or contact via MS Teams.