# Hardware acceleration in Ravencoin and its core X16R algorithm: A feasibility study

# Ravencoin及其核心X16R硬體加速可行性評估

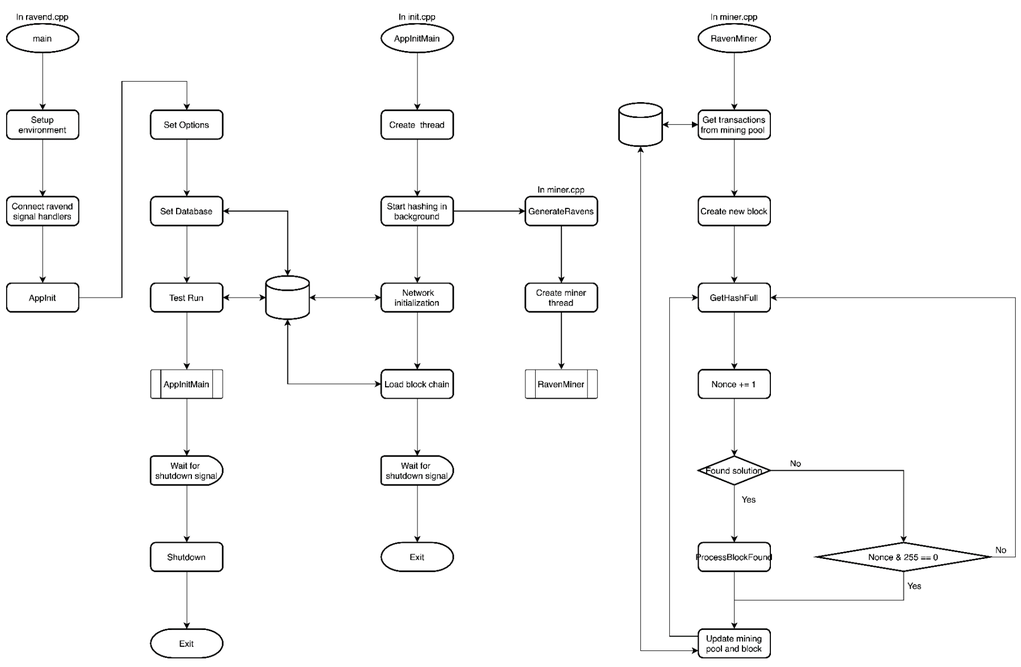
組別：A66　　指導教授：黃之浩　　組員：潘逸軒、林宗暐

## I. Abstract

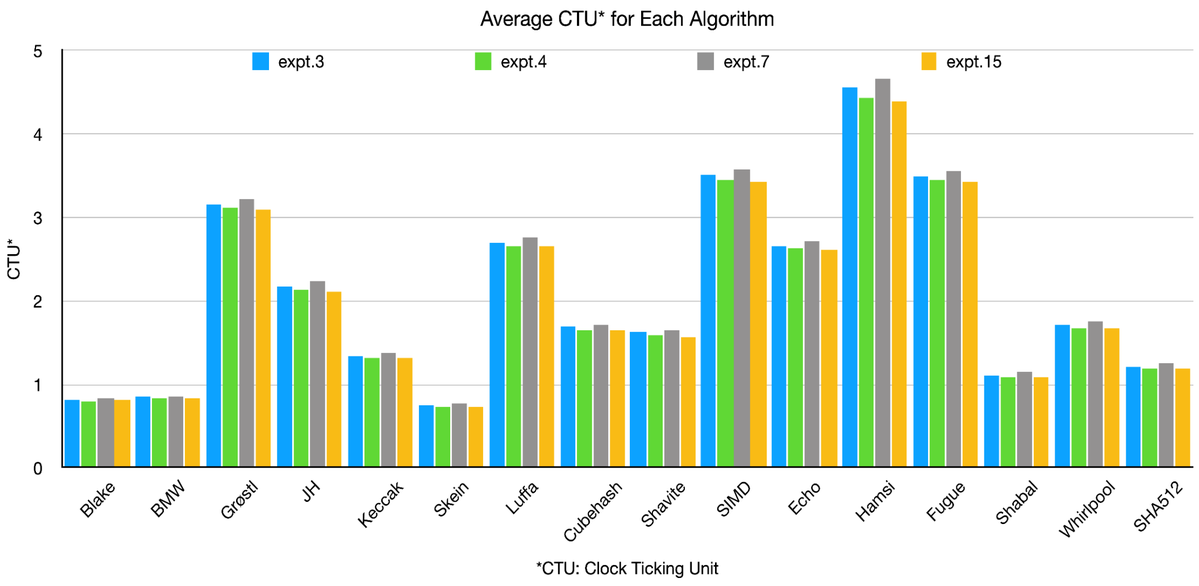
In this studies, the first conclusion is the difficulty in hardware implementation due to several factors, including Ravencoin's highly complicated main program, largely usage of high-level language with portion of functions incomplete. Secondly, there are several relatively slow algorithms under current speed tests and those could be potentially accelerated based on current studies. X16Rv2 algorithm is found to be feasible in speeding up either by adopting parallel programing or instruction pipeline. Therefore, Ravencoin could be hardware accelerated by incorporating computer and FPGA; the former is responsible for main program while the latter is designated for X16R computing.

## II. Ravencoin Main Structure

Ravencoin區塊結構於比特幣基本一致，以MerkleRoot連結區塊頭與交易內容，與上一區塊的hash值一同hash，構成區塊鏈。其挖礦主流程複雜，研究整理如下：



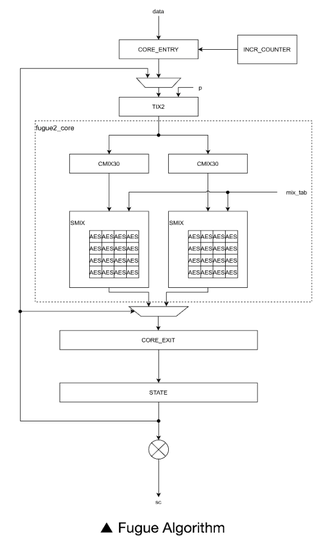

## III. X16R Algorithm Speed Test



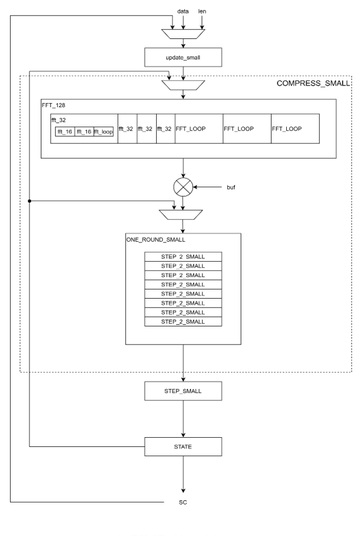

我們對X16Rv2及其子文件改寫，使X16Rv2可獨立編譯運行，以進行測速實驗。重複運行千萬次後，我們得出屬於X16Rv2的數個演算法，平均運行時間顯著並且穩定的較長，所得數據趨勢與X16R原始論文接近。

## IV. X16R feasibility study on FPGA

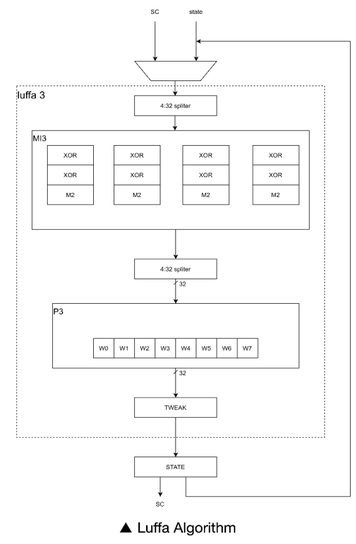
經研究，Ravencoin主程式使用高階語言特性且仍在開發，較難以硬體實作。其運算核心X16R，部分演算法花費較多時間，然發現皆可進行平行運算或指令管線化嘗試加速。因此，我們認為由電腦負責主程式而FPGA進行X16R運算，Ravencoin存在硬體加速可能。



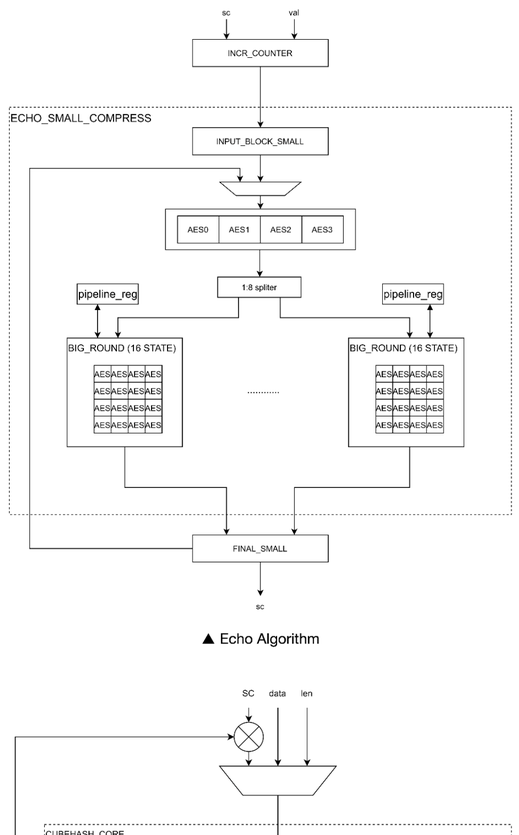

▲ Fugue Algorithm



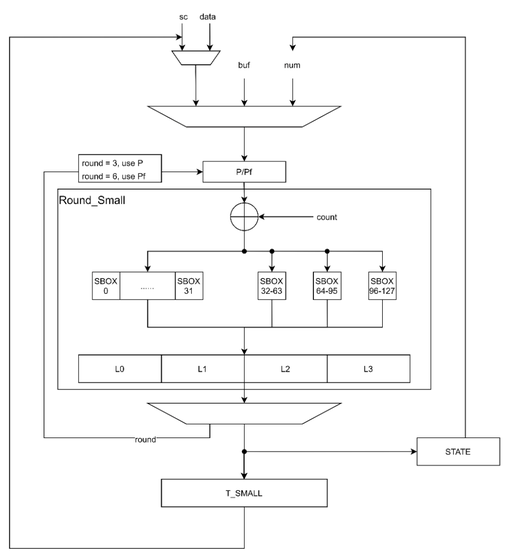

▲ SIMD Algorithm



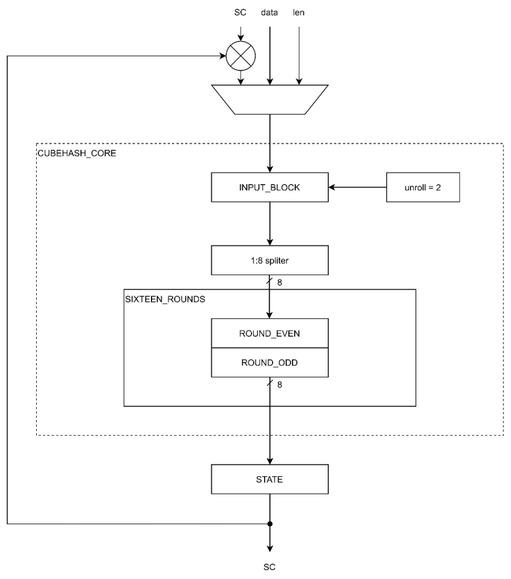

▲ Luffa Algorithm



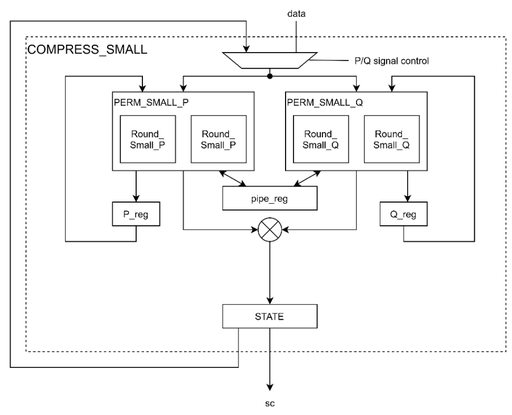

▲ Echo Algorithm




▲ Hamsi Algorithm




▲ Cubehash Algorithm




▲ Grøstl Algorithm

## V. Conclusion

我們認為Ravencoin之核心X16Rv2以硬體加速甚為可行，雖Ravencoin主程式難以完整硬體實作，然透過電腦與FPGA合作運行，仍可實現Ravencoin挖礦的硬體加速。