Student: **Dragos Mihaita Iftimie**

Project: Zynq-7000 FPGA crypto mining profitability

1 – Introduction

The client has access to a big stock of Xilinx Zynq-7000 field programmable gate array and wants to explore the possibility of using it for crypto mining.
The Xilinx's FPGA products fit for both production and research/prototyping environments because they can be programmed via VHDL (a language used for hardware description, it allows fine control of the hardware so it can lead to better resources usage/increased performance at the cost of required programming time and skills) and C language.
Using Xilinx's software, Vivado HLS, a programmer with no FPGA programming background can program an FPGA using C language.
Vivado HLS, given the C code that describes the behaviour to be mapped in hardware, can translate the C code in VHDL.
Is important to notice that in order to achieve that the C code cannot be written using an imperative paradigm, as usually is.
The C code to be written won't be executed in a CPU (line by line) but will be analized by a tool and used to program some hardware; this means that the paradigm and the mental approach are different; this requires non trivial knowledge.
This approach is not optimal because, even though the translation can be controlled through several options, the tool can automatically take decisions that are not fit for the specific project.

Another important aspect about Zynq-7000 is that the board has, in addition to the FPGA, an ARM processor that can communicate with the hardware.
This allows to run an operating system (Petalinux, linux distribution released by Xilinx, highly customizable and has to be compiled from scratch) on the CPU and write in an high level programming language the least CPU-expensive (for example networking and protocol management) tasks while assigning to the hardware the most CPU-expensive tasks (for example the research of the solution for the next block of the blockchain).
This approach avoids waste of hardware of the FPGA for non CPU-intensive tasks, allowing to use all the hardware resources and increase the parallelization of the most expensive tasks.
The CPU can also run a baremetal OS that allows to continuesly run C code; this option is more optimal because there's no delay from a complete OS like Petalinux, but it takes more time to develop.
Since the cryptocurrencies to be studied (see below) are all Bitcoin-like, the interface that the mining function presents (the one to be translated in hardware) is the same for all of them.
The standard API that Xilinx gives to communicate between the CPU and the hardware are "unconfortable and low level"; it's worth it developing some personalized API's using the standard ones in order to communicate with the interface that the hardware exposes.

The client, for each crypto from a list of cryptocurrencies he trusts (Dogecoin, Garlicoin, Groeslcoin, Bitcoin), wants to know if the Zynq can handle the hashing algorithm (some of them may be ASIC resistant), how much electrical energy is needed for the process and how efficient the board is in researching the solution for the next block.
Since a miner runs without ever stopping, 3 full days of mining are enough to understand how many hashes per second the boards can do and how much energy is required.

The boards will get the mining work from a public mining pool server that conforms to the protocol Stratum v1; the software that resides on the CPU and is capable of networking will have to be a Stratum v1 client, will have to be able to decode the work recieved and to assign it to the hardware through the high level API that we developed.
Again, since the cryptocurrencies are all Bitcoin-like, the decoding process is the same; the only difference is a constant in a division (in the operation used to calculate the target the miner has to look for).

The client wants results from us as fast as possible (especially in the cryptocurrencies world time is money); once he has the needed informations, he will decide which crypto to mine (if any is profitable) using native VHDL and a baremetal OS for the CPU in order to achieve the best performances.

3 – Project goals

What the client expects from us is:

- implement the hashing algorithm of each cryptocurrency from the list in VHDL in order to understand if the Zynq-7000 has enough hardware resources to handle it;

- Estimate, for each minable cryptocurrency, how many Watt the FPGA consumes in order to work (the average of the 3 days test);

- Estimate, for each minable cryptocurrency, how many hashes per second the FPGA can calculate (the average of the 3 days test).

Using the power consumption, the hashes per second, the cryptocurrency network difficulty and the value of the cryptocurrency (the last two informations are public) the client will be able to understand if any of the cryptocurrencies is profitable and which one is the most profitable.
Based on our research, the client will decide if is worth developing a production Zynq-7000 miner or not.

4 – Project scope

The project scope includes:

Garlicoin, dogecoin, groeslcoin and bitcoin are the cryptocurrencies that need to be explored; this means that their hashing algorithms are the ones to be implemented in hardware.

Developing an high level language solution that can be run on Petalinux OS that manages the mining process.
The solution has to comply with Stratum v1 client protocol in order to recieve work, be able to decode and assign it to the hardware and submit solutions found from the hardware to the server.

The project scope does not include:

Developing a solution that manages the mining process in C that can be run on a baremetal OS.
Implementing the hashing algorithms directly in VHDL, Vivado HLS will be used to translate hardware behaviour written in C to VHDL; this accelerates our research because the implementation of the hashing algorithms is open-source and written in C language.
This means that with small changes to the avaliable open-source solutions we can translate it in VHDL.

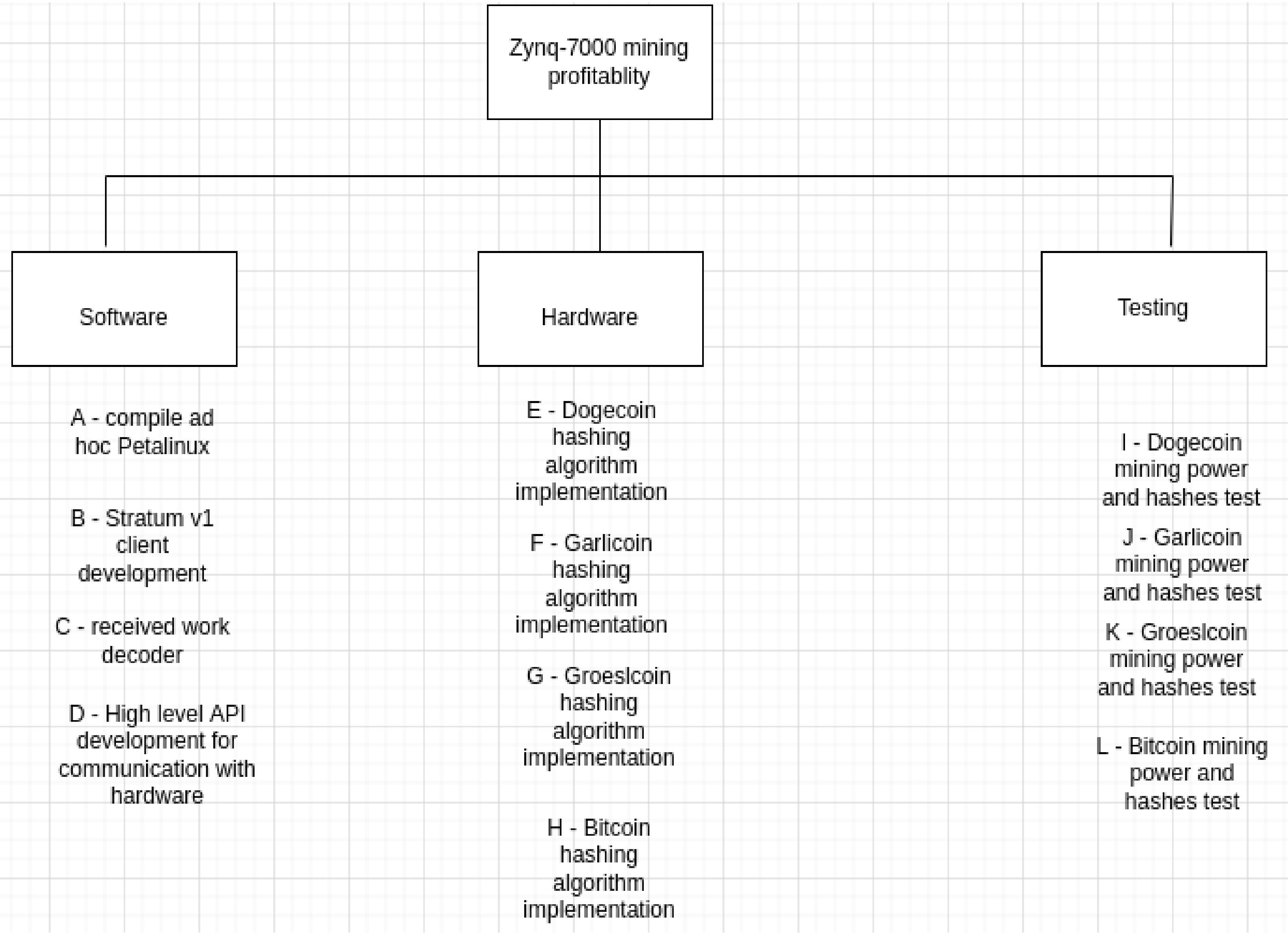
5 – Requirements

The main requirement that have not been well discussed yet is a non functional one: the client wants us to finish our research as fast as possible.
That’s why we are not using optimal solutions, it would take way more time and right now the client just wants to have an idea of which cryptocurrency can be profitable.
A production and optimal development will be held only after our research and if the client thinks is worth it.

6.1 – Deliverables and outcomes

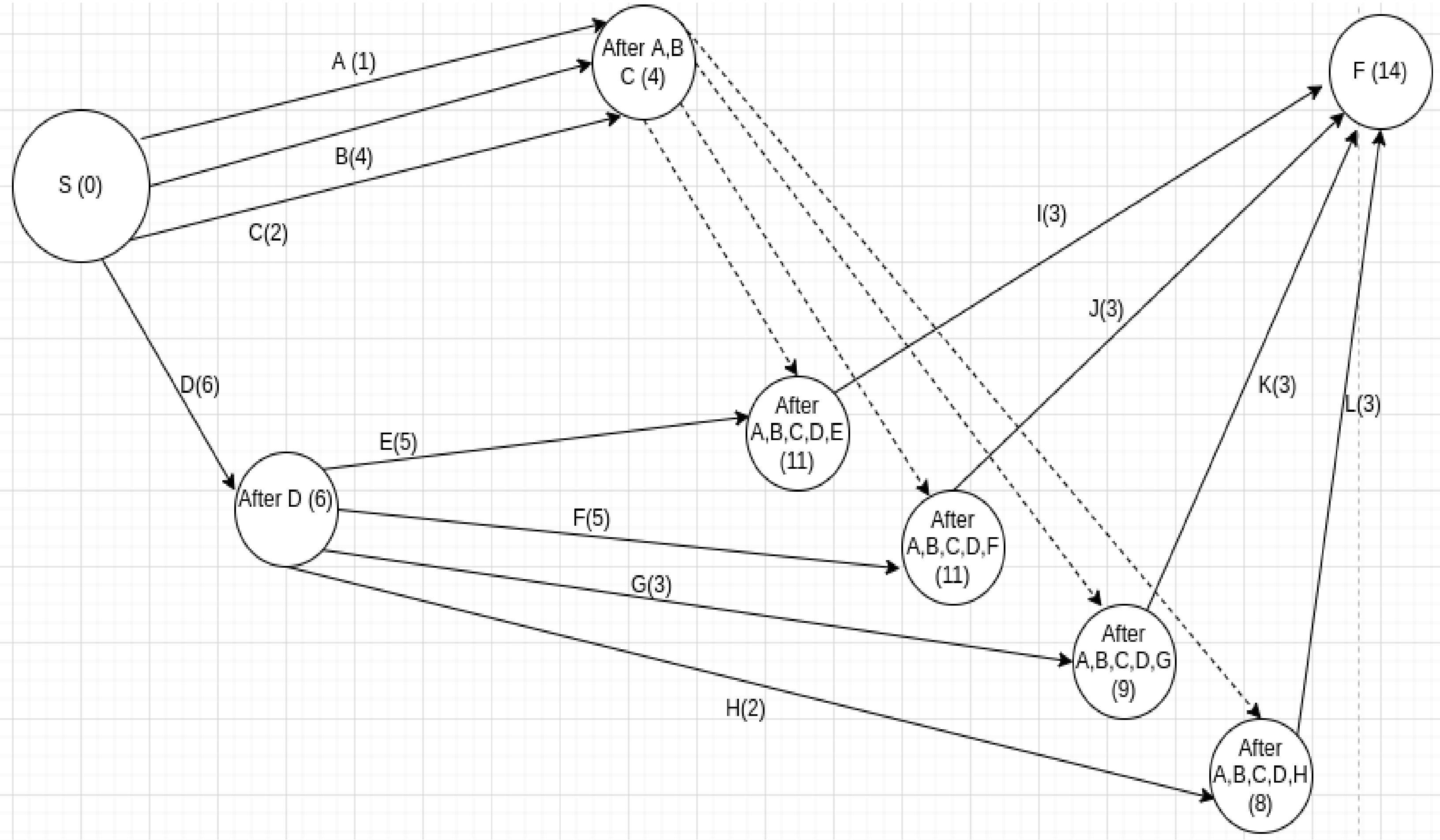
The main deliverables are informations.
The client doesn’t need the software we will develop but just the results of the research, since if he will decide to continue the developing, our software is not optimal.
The client will recieve the list of minable cryptocurrencies, from the list of cryptocurrencies he gave us.
For each cryptocurrency in the list of minable, he will recieve how many watts the FPGA needs to work and how many hashes per second the FPGA can perform.

6.2 – Work breakdown structure


Zynq-7000 mining profitablity
Software
Hardware
Testing
A - compile ad hoc Petalinux
B - Stratum v1 client development
C - received work decoder
D - High level API development for communication with hardware
E - Dogecoin hashing algorithm implementation
F - Garlicoin hashing algorithm implementation
G - Groeslcoin hashing algorithm implementation
H - Bitcoin hashing algorithm implementation
I - Dogecoin mining power and hashes test
J - Garlicoin mining power and hashes test
K - Groeslcoin mining power and hashes test
L - Bitcoin mining power and hashes test

Activity	Complexity (working days)	Sequencing
A	1	-
B	4	-
C	2	-
D	6	-
E	5	After D
F	5	After D
G	3	After D
H	2	After D
I	3	After A,B,C,D,E
J	3	After A,B,C,D,F
K	3	After A,B,C,D,G
L	3	After A,B,C,D,H

7.1 – Network diagram



7.2 – Project schedule and milestones

Team:
Dragos Iftimie – programmer and Xilinx’s tools expert
Daniel Rajer - programmer
Rimantas Jolinas - programmer and Xilinx’s tools expert
Agostino Del Gaudio - programmer and Xilinx’s tools expert

During the weekends the team will not work.
The activities I-J-K-L are not splittable, the tests about the average power consumption and hashes per second must last 3 days.
It’s important to notice that those activities may not happen if the Zynq-7000 cannot handle the hashing algorithm of the respective cryptocurrency.

What	Start	End	Who
First meeting, explain the project, the scope and the goals to the team	April 28 2022	April 29 2022	The whole team, Dragos Iftimie will lead the session
Activity A	May 02 2022	May 02 2022	Daniel Rajer
Activity C	May 03 2022	May 04 2022	Daniel Rajer
Activity D	May 02 2022	May 03 2022	Rimantas Jolinas Dragos Iftimie Agostino Del Gaudio
Activity B	May 05 2022	May 10 2022	Daniel Rajer
Activity E	May 04 2022	May 06 2022	Dragos Iftimie Agostino Del Gaudio
Activity F	May 06 2022	May 10 2022	Dragos Iftimie Agostino Del Gaudio
Activity H	May 04 2022	May 06 2022	Rimantas Jolinas
Activity G	May 09 2022	May 11 2022	Rimantas Jolinas
Activity I	May 11 2022	May 13 2022	Dragos Iftimie
Activity J	May 11 2022	May 13 2022	Agostino Del Gaudio
Activity K	May 11 2022	May 13 2022	Daniel Rajer
Activity L	May 12 2022	May 14 2022	Rimantas Jolinas
Project completed	May 14 2022		

8 – Resources

The team, in order to work, needs basic office furniture (personal computer, electricity, internet connection…).
Other than that the team will need a maximum amount of 4 Zynq-7000 and 4 electrical power consumption measurers; it may also happen that none of the cryptocurrencies are minable so there will be no need for the zynqs and the measurers.
The team will also need some open source code, for example the C implementation of the hashing algorithms.
During the development of the software for activity B and C, the team may look for open source code (widely avaliable online) in order to be faster.
3 (not 4 beacuse Daniel Rajer will not work on it) Xilinx Vivado licenses will be needed in order to perform activities E-F-G-H.

Finally, for the testing part, an external mining pool server will be used to get the work to mine (for example https://aikapool.com/).
We also need some good vents in order to not melt the boards during the tests.

9 – Project expenses and expected benefits

Since our team is specialized in Xilinx products involved projects, we already have enterprise licenses for their software.
This doesn’t mean that this project won’t contribute to the expense that we had years ago (a license can cost up to 4000 dollars) in order to buy the license, just… the actual client won’t pay the whole cost (see the economical concept ‘amortization’); for more details ask the accounting section.
The external pool mining server is free and the client will provide us 4 Zynq-7000 for the project.
We’ll need to buy the power consumption measurers, it’ll cost up to 20 euros each one, and some vents to cool the boards 20-30 euros each one.
The main cost is work. Our team is specialized in that field and has not easy to find competencies. More than that, the team will work hard in order to finish everything as fast as possible, they’ll need to be well payed.