UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat d'Informàtica de Barcelona

# Securing the inter-domain routing system with blockchain

## Bachelor Thesis

## Software Engineering Specialization

Author: Guillem Bonet Arnaiz

Director: Albert Cabellos Aparicio

Co-Director: Jordi Paillissé Vilanova

Department of Computer Architecture

July 2019

# Abstract

Inter-domain routing security is of critical importance to the Internet since it prevents unwanted traffic redirections. The currently used protocol, the Border Gateway Protocol (BGP), is proven to have security issues.

In this project, we will test and evaluate IPChain, a blockchain solution proposed to solve these security issues. In this thesis, we will evaluate the feasibility of the project for solving this issue. To do it we designed and analyzed a set of experiments that try to emulate real-life conditions. We will also find bottlenecks and other issues that prevent the solution from performing in an efficient way.

# Resumen

La seguridad en el encaminamiento de dominios es de vital importancia para internet, ya que ayuda a evitar redireccionamientos de tráfico no deseados. El protocolo usado actualmente, llamado protocolo de puerta de enlace de frontera o BGP, no es seguro.

En este proyecto comprobaremos IPChain, un prototipo que usa blockchain para solucionar estos problemas de seguridad. En esta tesis, evaluaremos la viabilidad de este proyecto para resolver el problema. Para hacerlo hemos diseñado y analizado unos experimentos que intentan emular condiciones reales. También encontramos cuellos de botella y otros problemas que impiden al prototipo funcionar de manera eficiente.

# Resum

La seguretat de l'encaminament entre dominis és fonamental per al funcionament d'Internet, ja que impedeix redireccions de trànsit no desitjades. El protocol actualment utilitzat, el Border Gateway Protocol (BGP), té problemes de seguretat.

En aquest projecte, provarem i avaluarem IPChain, una solució que usa blockchain proposada per resoldre aquests problemes de seguretat. Avaluarem la viabilitat del projecte per resoldre aquest problema. Per fer-ho hem dissenyat i analitzat un conjunt d'experiments que intenten emular les condicions reals. També trobarem colls d'ampolla i altres problemes que impedeixen que el prototip funcioni de manera eficient.

# 1. Table of Contents

# 2. Context

## 2.1 Blockchain Technology

In order to understand our solution, we first need to have some basic knowledge of blockchain, if you already have it you can skip reading this section.

A blockchain is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties [2]. The main feature of blockchain is its ability to generate trust without a centralized source everyone needs to have faith in, which is the case in most situations. An example of a centralized authority for trust is physical money, which only has value because everyone trusts a central organization that says that a bill has a monetary value even though it is just a piece of paper.

A blockchain is essentially a data structure which contains a record of all the transactions that have ever existed in it. Anyone can verify the validity of every single transaction at any given time, and trust exists as only those transactions validated by the majority of participants are added to the blockchain. For a transaction to be valid, the user that wants to transfer his assets needs to sign it with his own unique private key which verifies the ownership of the assets. [2]

## 2.2 Problem Formulation

This project is part of the Bachelor Thesis for the Bachelor's Degree in Informatics Engineering at Facultat d'Informàtica de Barcelona (FIB) of Universitat Politècnica de Catalunya (UPC).

Blockchain is attracting a lot of attention among the security community since it provides means for exchanging information among a set of distrusting entities without the use of digital certificates and centralized control. Blockchain provides means for the distrusting parties to reach consensus in a distributed way. Formally, it is regarded as a new solution to the Byzantine Generals problem, well-known in fault-tolerant distributed systems.

Although at the time of this writing the main application of blockchain is financial systems, their use in the field of networking is being explored. Some successful systems exist such as Namecoin [3], which aim at building a secure naming system, providing similar functionality to that of DNSSEC.

The problem that we aim to solve with this technology is the following:

The internet is a huge network which at the same time is formed by smaller networks called autonomous system (AS). When a user wants to visit a webpage, which is found in a server in a different AS it must know somehow the path it has to follow to retrieve this information. This is done with Inter-Domain Routing, which basically tells our computer the path the data needs to follow.

The inter-domain routing system glues the different AS by using the Border Gateway Protocol (BGP), it does so by propagating the data containing information which explains how to get to every AS. This protocol has been used since 1994, and it has evolved over time to accommodate new requirements. Nowadays, this protocol is still not secure, which has caused some security issues mainly related to internet traffic redirection. This can cause services to be down, for example, on the 24th of February of 2008, Pakistan, in a misconfiguration in his attempt to block Youtube in the country, wrongfully directed all YouTube traffic to his country which resulted in Youtube being down for some time [4].

There are no widely deployed mechanisms, mainly because of political issues and high technical costs. As a result, the current inter-domain routing system on the Internet operates without proper security and relies on the manual and careful configuration. In this project, we will prototype a Blockchain used to secure the BGP to determine if it is suitable in a real-life scenario. So the main objective of this thesis is to evaluate if Blockchain could be a viable solution to the current BGP problem.

## 2.3 Stakeholders

The stakeholders of this project are the following:

- **Users of the internet**: The users of the internet will be directly benefited from this project, as they will be able to navigate a more secure and free network.
- **Network operators**: The network operators will have an easier task, as it should be harder to create a problem in the network by a misconfiguration, as nowadays a BGP error could lead to huge problems.
- **Network equipment manufacturers**: The companies that work in this field will be able to have products that provide better security just by implementing this technology in their products.

- **Blockchain Engineers**: People that work in this area will have a new area of impact, and this technology will have a new success example which helps increase its popularity.

# 3. State-of-the-art

The two main topics explored in this project are Blockchain and Inter-Domain Routing. I will now discuss the state-of-the-art in Inter-Domain Routing and some blockchain solutions that have already been proposed.

## 3.1 RPKI

This approach wants to use a public key infrastructure (PKI) approach with the objective of improving the Internet's routing infrastructure. It relies on a centralized authority which acknowledges the owners of IP prefixes and AS numbers (the identifier of an AS) with the use of digital certificates [5].

Some of the drawbacks of this solution are:

1. This solution needs a central authority which needs to be trusted by everyone.
2. RPKI cannot prevent all the possible attacks [6].
3. Economic interests delay its adoption [7].

There has been a poor adoption or RPKI as roughly 10% of the IPs are secured with it in February of 2019 [8], [9].

## 3.2 Blockchain Solutions

In The internet blockchain: A distributed, tamper-resistant transaction framework for the internet [10] a blockchain solution is suggested to overcome the problem of inter-domain routing, which is what the project aims to do.

Similarly, in An experiment in distributed Internet address management using blockchains [11], an Ethereum blockchain serves the purpose of decentralized management of IPs.

Both of the previous papers approached the solution in a more conceptual way, and no prototype has been developed.

Another example of this is found in Blockchain-based Public Key Infrastructure for Inter-Domain Secure Routing [12], where blockchain is used for the same purpose, and its focus is in providing an easy transition from current systems which would facilitate its adoption.

There is not much research in this field, so it is still a very unexplored topic. Much more research is still needed to determine the viability of this option as a substitute for the current inter-domain routing system.

## 3.3 Advantages of blockchain over RPKI

#### 3.3.1.1 Consistent vision of the state

Exactly like in Bitcoin, in the RPKI we need to keep track of the owner of each IP prefix (coins), e.g. to avoid the transfer of the same prefix to two different users (double-spending). In other words, we need to maintain a global vision of the state. Achieving this is easier in a blockchain when compared to the RPKI: the latter has to update state via specific protocols (RFC 8181), processing of CRLs and manifests, etc, while in a blockchain these mechanisms directly arise from its transactional nature.

#### 3.3.1.2 Simplified management

The RPKI is cumbersome to man-age, for example, users have to choose between two operation modes. Some actions are complex, like key rollover (RFC 6489 is specifically devoted to it in the RPKI), because it requires re-signing all downstream certificates starting from the one being replaced. On the contrary, a key rollover in a blockchain can be easily performed transferring a coin/asset to a new address (keypair). Other operations, such as the revocation of a transaction, do not require a dedicated sub-system (Certificate Revocation Lists (CRLs) in a PKI), but only adding a new transaction.

## 3.4 Other solutions to the Inter-Domain Routing problem

### 3.4.1 Prefix filtering

In a nutshell, prefix filtering is a whitelisting technique used to drop BGP announcements that are not correct. It will only send announcements of IPs that are their own or one of their costumers (as normally AS have a customer-provider relationship) [6].

### 3.4.2 Route Monitoring Services

Some companies have come up with products that monitor your network's BGP reachability, what they do is monitor if the traffic is sent correctly to your servers and alert you if they find any BGP misconfiguration. Some companies that provide this service are ThousandEyes[13] and BGPMon[14].

Obviously, this solution is not optimal as the problem has already occurred although they can help your company improve their reaction time if it happens.

### 3.4.3 Internet Routing Registry

Another option to help prevent these problems is the Internet Routing Registry (IRR) [15], which is a database that contains the information of where each domain is found. This can help fix inconsistencies in the information sent over the BGP protocol, so basically, it is used to validate the received information.

This solution is not secure as misconfiguration can also be made by the AS when updating the data.

# 4. Scope

The main goal of this project is to represent a first step towards the understanding of the properties of blockchains and their applicability in the Internet infrastructure, specifically securing the allocation, delegation, and bindings of IP addresses.

There is already an existing project [16] which assigns IP prefixes to different internet entities using blockchain so that we are able to verify if the BGP message we are receiving is legit or not. This project has also been prototyped. We will first understand what the proposed solution so far is, and we will test its performance under different conditions so that we are able to conclude whether its real-life applicability is viable or more improvements need to be made.

## 4.1 Possible obstacles and solutions

### 4.1.1 Prototype design

One of the possible problems that we could encounter is found in the prototype, it is possible that the prototype is not able to reach optimal results due to coding problems rather than

problems in the formulation of the solution. If this happens, we would need to thoroughly review the code in order to optimize it.

### 4.1.2 The technology is not capable of solving the problem

It is possible that after developing a solution and testing it, we find out that it is not viable to use blockchain for this purpose in the current state-of-the-art or that it doesn't bring a significant improvement to the current system. Rather than a problem, this would be a conclusion to the work, which would leave room for improvement once blockchain is able to overcome its limitations.

### 4.1.3 Testing limitations

We could find that we are not able to emulate a real-life scenario for the testing of the project due to limited computational power, in this case we would need to find testing alternatives that could approximate to a real-life scenario as much as possible, as testing is a crucial part of this project as it is required to understand the viability of the solution.

### 4.1.4 Results interpretation

Once we create our prototype and we test it, we need to correctly interpret the results we find. We should take into account how similar to a real-life scenario our testing is and be able to understand if the results are positive or not. Also, we need to carefully select the statistical methods and testing methods used so that the interpretation of the results is accurate.

## 4.2 Methodology and tools

As this project is a research project and it is likely to find problems that need to be overcome, adaptability is a crucial aspect of its development, so the better-suited methodology is agile, this way we will be able to find and solve the problems that are found faster.

As we are a small team, we will hold a weekly meeting to discuss the week's accomplishments and set a goal for the coming week. This progress will be documented accordingly so that we can easily know where we are. There is no need for complex methodologies or tools as teamwork is very easy to coordinate in a team of 3 people, so weekly meetings should provide a successful methodology, to set them up we will use Google Calendar so none of the assistants forget about said meetings.

There is also be a Github repository where all the code of the project is found in order to better keep track of the progress and be able to collaborate in the coding task successfully.

# 5. Task description

This project started in February of 2019 and will finish in July of 2019, it will be divided into 3 differentiated sections, and each part will require that the previous tasks have been completed. Now I will explain for each one the period in which it will be done (the length of which will be approximately the same for all parts), what are its objectives and the resources that will be needed to do them.

There will also be a part dedicated to write the project documentation and prepare the presentation.

## 5.1 Initial documentation

During the process where the GEP course is taught, some time will be invested in creating the initial documentation for the project, which basically introduces the project, creates a schedule and evaluates its cost.

This part of the project will be carried out during the first month of the project, which is March 2019.

| Task | Estimated duration (h) |
|---|---|
| First assignment | 30 |
| Second assignment | 15 |
| Third assignment | 20 |
| Fourth assignment | 25 |
| Total | 90 |

## 5.2 Understanding the current status of the project

This is the first step for being able to contribute to this project, or any project, is understanding the current state of development and learning the technologies involved with it as well as their current state-of-the-art.

To be able to do this a lot of resources will be useful, the main source of information will be scientific papers related to the topics, for example, the existing paper on the project [16], previous bachelor thesis on this project, and papers about the state-of-the-art of the used technologies (Blockchain, BGP, …). A big part of this is also the meetings with the director and co-director of the thesis which are familiarized with the project and can easily help solve some doubts that may (and probably will) appear during this or any learning process.

This part of the project will be carried out in parallel with the previous step during the first month of the project, which is March of 2019.

| Task | Estimated duration (h) |
|---|---|
| Read papers on the project | 50 |
| Read papers on the involved technologies | 50 |
| Meetings | 20 |
| Total | 120 |

## 5.3 Experiment design and coding

The main goal of this thesis is testing if blockchain is a viable solution for securing BGP, so most of the work will be related to testing and evaluating the current prototype. Once the process of learning is finalized and how the prototype works is understood well, it means that we can start to work on writing the code for the prototype and solving its bugs, and in the design of the experiments that will be done and studied in order to answer the main question of this thesis.

The resources that will be required for this are the previously acquired knowledge on the topic, the current prototype, and also there will need to be a discussion with the supervisors

in order to decide which experiments make sense to do to test the real-world applicability and how they should be done. When all the resources are obtained, it will come to write the code that will run these experiments.

This part of the project will be carried out during the second month of the project, which is April of 2019.

| Task | Estimated duration (h) |
|---|---|
| Coding of the prototype | 50 |
| Experiment design | 50 |
| Meetings | 20 |
| Total | 120 |

## 5.4 Testing and conclusions

When we have designed and coded the experiments, they will need to be executed and measured, once we obtain the results, we will need to do a statistical analysis and a comparison to current BGP measures. This way we will be able to evaluate if the project has an application in real-life.

The resources required for this section are the previous section experiment design and coding basically, but we might also need more testing resources such as more computers or network equipment if we consider that the testing environment is not enough to simulate real-life conditions. Also, knowledge of statistical analysis will be needed in order to be able to provide accurate and well-analyzed results of the tests.

This part of the project will be a bit longer than the others, because there might be the case where after analyzing the experiments done, the need of more experiments or the redesign of existing ones is needed so that a more thorough conclusion can be obtained, so it will be carried out during the third and the first week of the fourth month of the project, which is May and the first week of June of 2019.

| Task | Estimated duration (h) |
|---|---|
| Testing | 40 |
| Statistical analysis | 60 |
| Time margin for possible problems | 30 |
| Meetings | 20 |
| Total | 150 |

## 5.5 Project documentation and presentation

The last week of June will be dedicated to writing the documentation of the project which shouldn't be a very highly time-consuming task as all the project work will be done and only writing will be required. After that, there will be time to prepare the presentation of the thesis which will be done at the start of July.

| Task | Estimated duration (h) |
|---|---|
| Writing documentation | 20 |
| Preparing presentation | 40 |
| Total | 60 |

To better understand and visualize the task distribution and its dependencies, a Gantt chart has been created.

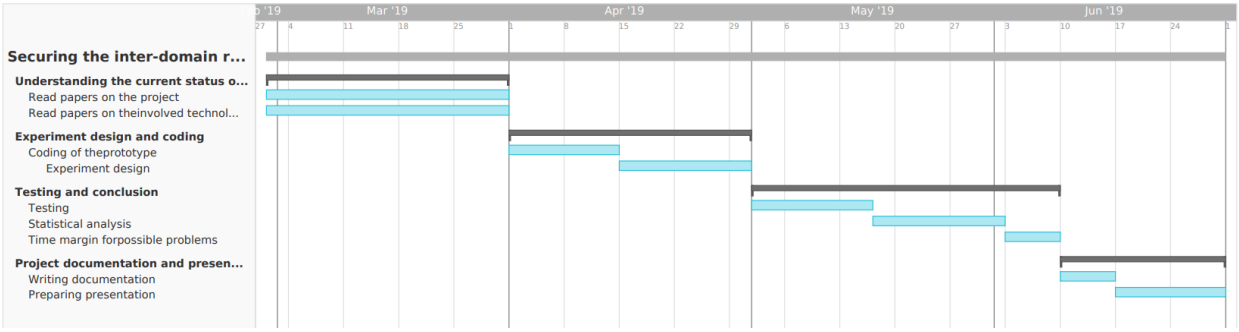


*Figure 1 Gantt chart for the project planning*

# 6. Alternatives and action plan

In these sections, we will discuss how the possible obstacles mentioned in the "Possible obstacles and solutions" section could affect the schedule, and how they can be solved.

## 6.1 Prototype design

If the prototype solution is not able to reach its goal due to coding problems it could be an issue, to solve it, the prototype coding part will be mostly done in the first half of the month, so that if problems are found there is still time to fix them, so rather than a solution, we will prevent this issue from extending the deadlines by approaching it in advance so there is time to solve it. Also if more issues than expected are found, we would need to change the scope of the thesis to those problems, as well as reduce the testing part so that the project is feasible in the time given.

## 6.2 The technology is not capable of solving the problem

In the scenario were after developing and testing the solution we conclude that the project is not able to improve BGP security or it does it but with bad performance, we would need to evaluate why, this is regarded as part of the testing and conclusion part, and it will not modify the schedule and the same amount of time would be required if the results were positive.

## 6.3 Testing limitations

If the testing environment is not able to meet the requirements needed to emulate real-life, we would need to find more resources (computers and network equipment) or redesign the experiments, this is the reason why the last part of the schedule is 1 week longer than the others, so that if further tests need to be done or the existing ones need to be redesigned, this can be done without extending deadlines, so the same approach of trying to finish the work in the first 50% of the scheduled time will be taken so that we have time to correct and/or improve.

## 6.4 Results interpretation

The results interpretation is not a trivial task, so we have to make sure that the testing limitations of the previous point are solved, and that we do a good and unbiased statistical analysis. To overcome this possible action, we have to prevent it by making sure that the testing limitations are solved, the experiments are well-designed and the statistical analysis of the obtained data is correct. As discussed previously any of these problems could be solved in the last week of the third section, which is dedicated to it.

# 7. Budget and sustainability

## 7.1 Self-assessment

I think that accurately identifying and solving sustainability problems that your project might have is a crucial skill, nowadays, this topic is becoming more relevant as something need to be done to solve global warming.

After doing the survey I realized I didn't have much knowledge of the technical ways to evaluate the sustainability of a project, but through the identification of costs and sustainability of this project, I managed to learn further how an accurate evaluation can be done, and how each project needs to have an assessed evaluation of its economic, social and environmental impacts. This way, we can prevent unnecessary negative impacts on society, and make sure that we provide the most sustainable solution, which is a very relevant quality.

By doing the survey and completing this part of the document I learned how to evaluate the sustainability of a project and provide ideas that could make it more sustainable, to take into

account the social impact of a project to see how it will benefit to the well-being of society, to measure the project's economical sustainability and understand that uncertainty affects it and in which way.

In conclusion, with this newly acquired skills I am now more prepared to develop sustainable projects from an environmental, economic and social point of view, which is a crucial skill for an engineer and more so with the current world.

## 7.2 Budget

In a project like this, there are many costs that come from many different sources, I will break it down in tables divided by source.

### 7.2.1 Human Resources

| Role | Hours | Price per hour | Estimated cost |
|---|---|---|---|
| Project author | 540 | 10€ | 5400€ |
| Project director | 180 | 16€ | 2880€ |
| Project co-director | 180 | 16€ | 2880€ |
| Total | | | 11160€ |

The hours have been calculated according to FIB estimation of hours work per credit, and the director and co-director have been given 8 hours a week approximately. This cost is equally distributed among all tasks.

### 7.2.2 Direct costs

| Product | Price | Units | Useful life | Estimated cost |
|---|---|---|---|---|
| Computer | 900€ | 1 | 5 years | 90€ |
| AWS servers | ~0,3€/h | 3-5 | - | ~100€ |
| Total | | | | 190€ |

The estimated cost for the computer corresponds to its amortization, and it's calculated assuming that the project lasts 6 months. The computer will be used for all the tasks with equal load, and the AWS servers will be used for around 2 weeks approximately during the

testing phase of the project (testing task in the Gantt chart) and its cost has been calculated approximately as the testing doesn't have a very strict time duration.

### 7.2.3 Indirect costs

| Product | Price | Units | % of use | Estimated cost |
|---|---|---|---|---|
| Internet | 35€/month | 1 | 30% | 10,5€ |
| Electricity | 55€/month | 1 | 10% | 5,5€ |
| Motorcycle | 800€ | 1 | 20% | 20€ |
| Transport | 20€/month | 1 | 25% | 5€ |
| Total | | | | 41€ |

It has been assumed that the motorbike has an estimated useful life of 4 years (as its second hand) and that only 20% of the times it is used during this 6 months it is related to this project. All this costs are equally distributed among all tasks.

### 7.2.4 Unforeseen contingencies

As this is a research project and it is likely that some miscalculations in the predictions have been made, it has been assumed that there is a contingency of 15%.

| Source | Cost | Contingency |
|---|---|---|
| Human Resources | 11160€ | 1674€ |
| Direct costs | 190€ | 28,5€ |
| Indirect costs | 41€ | 6,15€ |
| Total | | 1708,65€ |

### 7.2.5 Incidents

There are 2 main events that could cause a cost variation:

1. The computer breaks and a new one needs to be bought, this can happen with a probability of 5%.

2. The motorcycle breaks and the author is left without transport, in this event, a public transport card would need to be bought to use as transport. This can happen with a probability of 10%.

| Incident | Probability | Price | Cost |
|---|---|---|---|
| Computer breaks | 5% | 900€ | 45€ |
| Motorcycle breaks | 10% | 100€ | 10€ |
| Total | | | 55€ |

### 7.2.6 Total cost

| Source | Cost |
|---|---|
| Human resources | 11160€ |
| Direct costs | 190€ |
| Indirect costs | 41€ |
| Contingency | 1708,65€ |
| Incidents | 55€ |
| Total | 13154,65€ |

## 7.3 Budget monitoring

In order to monitor the budget estimation accuracy we will note the costs and time spent in each task after its completion, by doing this, we will be able to see if the prediction we made is accurate.

If the estimation was not correct, by tracking it task by task we will be able to determine which tasks took more time and/or money than we expected, this will help us see why, justify it, and not commit the same error in the future.

That being said, the contingency cost of the project should contain the possible unexpected costs, therefore we should not fail to stay inside the budget limit stated in the previous section.

## 7.4 Sustainability

### 7.4.1 Economic Dimension

The cost of this project is not very big, and most of it comes from the human resources needed to complete it, which for a Bachelor thesis this an inevitable cost. When it comes to the other costs, they are quite low, as this project does not require a lot of resources.

In the present, the costs of the issue targeted are mainly covered by the Local Internet Registries (LIR) fees, which are paid to the Regional Internet Registry (RIR) which is responsible for maintaining the IRR servers.

Our solution would potentially solve the security issue of BGP, therefore, no centralized servers would be needed so this energy consumption would not be required, also, as our solution uses proof-of-stake as a consensus algorithm it does not require a big computational power which would elevate the energy consumption of each node of the Blockchain, as in Bitcoin.

### 7.4.2 Environmental Dimension

The only resources needed for this project are a computer and the use of 3 to 5 servers during a 2 weeks period, so its energy consumption is very low therefore it has a low environmental impact.

As it is not a very resource-hungry project, there is no need to minimize its impact, also it is not viable as a computer to develop is required and servers to test a real-life scenario are very important for the task.

As discussed in the previous point, the current solution involves some centralized servers, and our solution will potentially remove this need, so it has a positive environmental impact.

### 7.4.3 Social Dimension

By doing this project I think I will achieve a greater knowledge in blockchain and understanding of the internet protocols, I will also learn how a research work is done, and this could potentially make me be more interested in research work.

As discussed in previous parts of the documents, some problems have been created by the lack of security on this protocol which has affected millions of users of the internet by not letting them access their website of interest, our solution will bring more security to this

protocol and will contribute to a more decentralized internet, which will be more free, so its social impact will be the security and freedom given to the users.

There is a real need for this project from the social point of view, as now there are problems that have not yet been solved, and affect the users of the internet directly.

# 8. Technical background

To understand the current solution and how it works we need to understand a few concepts. First of all, we will look at the overview of how the prototype works, after understanding the big picture we will move on to understanding in more detail the relevant parts required for understanding the rest of the document.

We will also discuss the advantages of using blockchain in this context.

## 8.1 Prototype implementation overview

As we discussed at the start of the document, this prototype is basically a blockchain which records transactions of IP addresses between its participants. The prototype is built in python, and it has two main processes running:

- The blockchain, which is in charge of handling all the logic required for the correct functioning of the blockchain. It will do things like block creation, verifying incoming blocks, creating transactions, executing the consensus algorithm, etc. This is the main process of the prototype and will be discussed later in the document.
- The process for communicating the blockchain logic with the other nodes, this process is in charge of receiving and sending the messages used to communicate the nodes into the network. All the messages are broadcasted to every node in the blockchain to ensure the correct functioning of the distributed network. This is done with a peer-to-peer network (P2P).

In Figure 2, we can see a diagram displaying the architecture of the solution. The logic explained in the following paragraphs is in charge of managing all the components but the P2P, as this one is in a separate process as just mentioned. The only component that will not be explained is the OOR interface, which is an interface used to communicate with OpenOverlayRouter [17], and it is not relevant for our work.

We will now look at the functioning of the blockchain logic process. This process represents a node of the blockchain, which can contain one or more participants, which are represented

as a public and private key pair saved in the keystore. It is constantly running in a process, this process is constantly running an infinite loop which has different parts which will be looked into detail now.

The main loop is in charge of executing the three main parts of the logic, which are the Distributed Key Generation (DKG), the BLS and the block generation and processing. The main objective of the blockchain is to record transactions in the chain, it does it by adding blocks that contain transactions to the chain. Any blockchain requires some way to reach an agreement between nodes on who creates the next block and whether the created block is accepted or not a block into the chain, this is known as the consensus algorithm, and each blockchain has its own. The other nodes need to be considered untrustworthy as anyone could act maliciously, this is due to the fact that the code is running in an unknown machine and it could be modified with a malign intention.

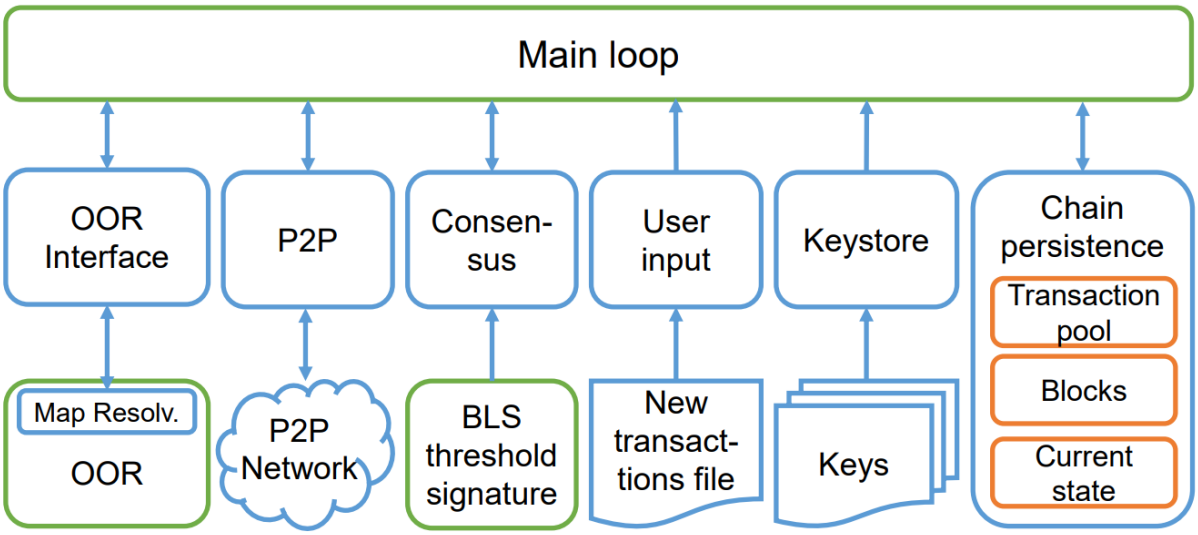


*Figure 2: Solution architecture*

In our blockchain, the consensus algorithm is proof-of-stake, which means that those with more stake, in our case more IP addresses, will have a higher probability of creating a block and adding it to the chain. This choice was made before the beginning of my thesis, and the reason for it is that as it is not in the interest of nodes that own more IP addresses that the internet misfunctions. Furthermore, it is very difficult to achieve control of the chain as it would require a node to own more than a majority of the world's IP addresses.

The proof-of-stake algorithm of our solution is implemented as follows:

A random participant of the blockchain is selected, this participant then creates a block and broadcasts it to the network. Once the other nodes receive a new block, they need to verify

it and if it is correct, add it to the chain. This process will be explained in more detail in the following sections.

### 8.1.1 Random Number Generation

Although the previous explanation is very simple, the complexity of the problem lies in the random number generation, which needs to be secure and it is also required that the generated number is the same for every node. To achieve this a threshold signature scheme is used as the source of randomness, this idea has been extracted from the DFINITY blockchain [18].

A (k-n)-threshold signature scheme is a cryptographic protocol in which any given subset of k participants out of the total n can create a valid signature [19]. This scheme needs the different parties to have an individual private key known as share and a common public key known for every party, the nodes will then be able to sign a message, and the message signature will not be valid until at least k participants have signed it.

To generate a random number, the participants will sign a message which is created with data from the previous block, once the message has a valid signature, this signature will be hashed, and this hash will be the generated random number. By doing this process, this number will be the same for everyone and will be different for every block, this is why it will be used to select a signer for the next block.

This process uses two different concepts that also need to be understood: the Distributed Key Generation (DKG) and the Boneh-Lynn-Shacham (BLS) signature scheme.

#### 8.1.1.1 Distributed Key Generation (DKG)

Distributed Key Generation is a process used to create a public key and a set of private keys in a distributed way and without any required trusted third party. Any of the parties are able to discover the (virtual) secret key, with which you could encrypt any message, without access to at least threshold private keys. Also, the secret key is never computed at any moment during the protocol which would make it not secure given that any node can be trusted. [20] This process is used in our prototype to create the public key and the individual private keys for all the participating nodes required for the threshold signature scheme explained in the previous section.

The threshold signature scheme will not involve all the participants of the blockchain as it would require an enormous amount of computational power and bandwidth which would take too much time and load, also taking this measure does not compromise the security, so

a configurable parameter defines how many participants the threshold signature will have, and also another parameter will define the threshold for the signature to be valid.

#### 8.1.1.2 Boneh-Lynn-Shacham (BLS) signature scheme

The BLS signature scheme is used to verify ownership of signature, many signature schemes exist, but BLS is known for its short digital signatures relative to its security when comparing it to other existing signature schemes. This is useful when these signatures need to be exchanged using the network, as it will require a much smaller bandwidth. [21]

When at least k participants of the (k-n)-threshold signature are in the same state of the blockchain, they create a message which depends on the last block data (which should be the same for everyone) and sign it with their own individual private key, then this message is broadcasted to every node, this is known as a share. When a node has received k different shares, it is ready to verify the signature, which will be valid if everything worked correctly, then, after hashing the valid signature the node obtains the generated random number that is used to pick the new signer.

### 8.1.2 Block generation

The block generation process is quite simple, if the node has been chosen as this block's signer it will start this process. The node will create a block with the required data, the most relevant fields are the previous block hash and the transactions (if any), then it will sign this block with his private key and broadcast it to the network. Now the other nodes are able to verify the block using the signer node public key, and check that no error has been made (on purpose or not) before adding it to the chain.

New transactions are sent to the network, and if verified correctly they are saved in the transaction pool until this process begins. Once a node receives a new block, it must delete the transactions that were added to the block which he already saved in his own transaction pool before in order to avoid duplicate transactions which would result in invalid blocks.

# 9. Experiments

The objective of this work is to test if the solution would work successfully in a real-world scenario. When we thought about the possible drawbacks of the solution, two main concerns came to mind. First of all, a political concern which would be a big reason for determining the solution's success, if any organization could achieve a monopoly (more than (k/n)% of the addresses in a (k-n)-threshold signature scheme) it could take control of the chain and

the chain would not be trusted. This is because the owner of the monopoly could then decide which blocks get added to the chain as he signs the majority of them.

Secondly, from the technological point of view, this solution would be running in a lot of different network-related machines, and its efficient functioning needs to be ensured if it is implemented in real-life.

We designed three experiments in other to test if its implementation could succeed. The outcome files of the experiments, as well as the code used to generate them, is available in a public repository [22]. The code of the blockchain solution is also publicly available [23].

## 9.1 Trust in the internet

This experiment looks at the distribution of stake in the blockchain based on real data, this experiment should give us an impression of how difficult it could be to achieve control of the blockchain, which is required in order to mislead the users of the internet on which is the legitimate owner of an IP.

### 9.1.1 Why

Proof-of-stake consensus algorithms come with weakness: monopolies. If a participant was to control enough assets to be able to accept a new block into the chain without needing the consent of any other participant, he/she could create any transaction that he desires without consent. Given that this scenario is possible, the validity of the data in the chain would be in danger because trust would no longer be granted in the blockchain, because, as explained before, incorrect information could be added to the chain.

Even though this situation is not in the interest of IP addresses holders, because the ownership of their IP addresses would not be trusted too, it is possible that malicious purposes could be derived from it.

### 9.1.2 How

This experiment is a Data Science experiment. The sources used to extract the data are the following:

- Center for Applied Internet Data Analysis (CAIDA): This organization, based on the San Diego Supercomputer Center, conducts network research and maintains many sources of data. We extracted data of the relationship of the autonomous system (AS) with countries and companies.

- iptoasn.com: This website provides data on the relationship of IP address with AS. This data is not available officially anywhere, but there are many different sources that provide this information. We do not expect this information to be 100% accurate but it should give a good enough estimate for our research purpose.

Each AS is associated with one or more blocks of IP addresses, and this AS belongs to a country and its owner (companies, organizations, individuals, etc). To create the graphics we basically merged these two sources data in order to find the relationship between IP and country or company. All the percentages were calculated based on the number of IP addresses which are assigned, as there are some that are unassigned or not publicly routed.

### 9.1.3 Results

The results are divided into two sections, one section looks at the data grouped by company and the other by country.

#### 9.1.3.1 Trust by companies

First, we will analyze the data found in Figure 3, which displays the percentage of assigned IPv4 addresses by company, showing only those with more than 1%. We choose to analyze IPv4 and IPv6 data separately in order to get more detailed data. We can see that the company with more IP addresses is N0. 31, Jin-rong Street. This company is related to ChinaNet, the only ISP in China, and because of the enormous population of China, it is not strange to find it in the first place. Most of the

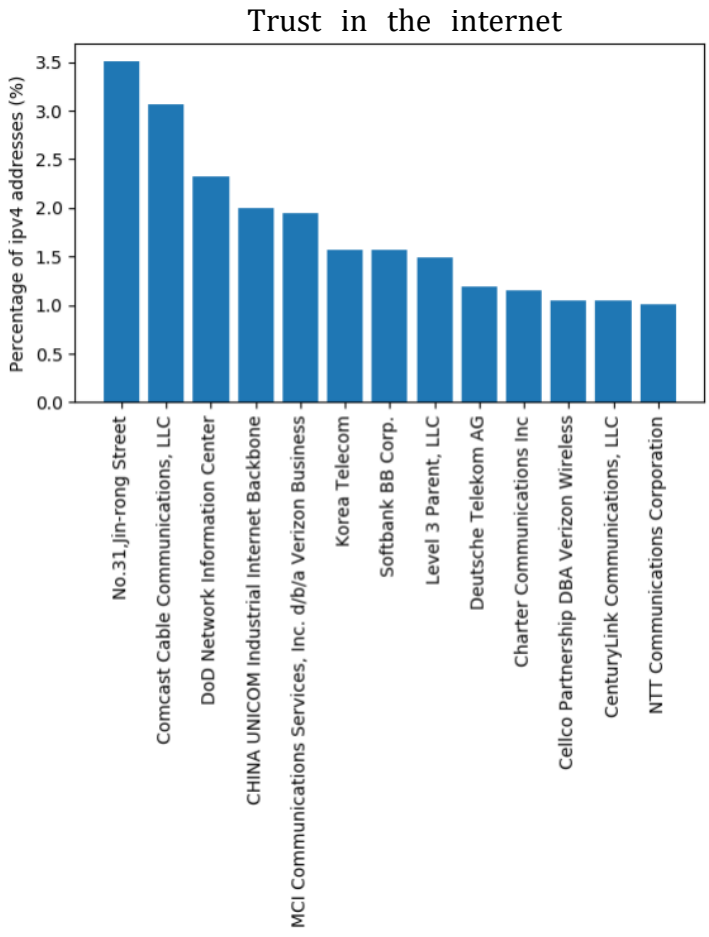


*Figure 3: Percentage of IPv4 adresses by company (more than 1% only)*

companies in the graph have some relation with networking, so it makes sense that they own a big percentage of the global IPs.

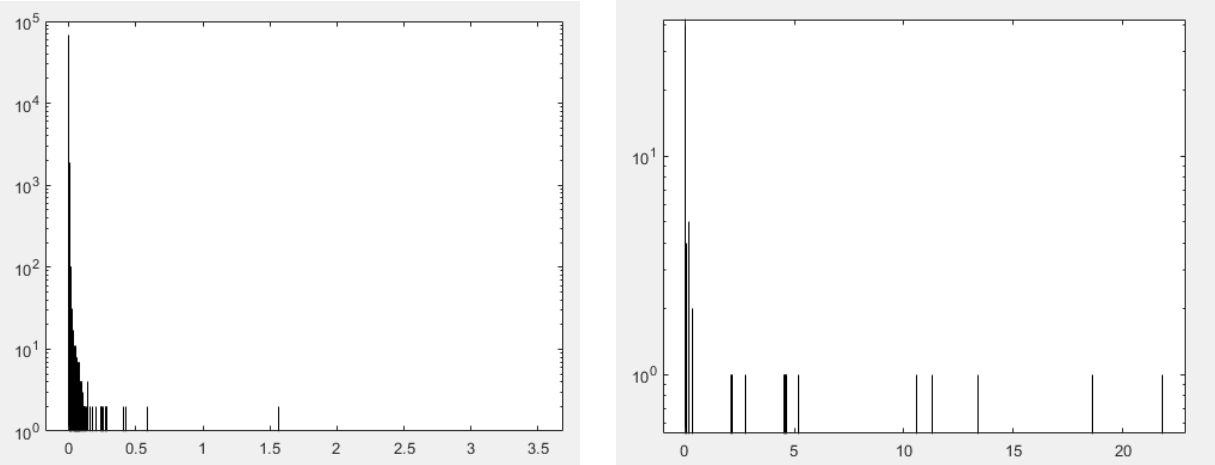


*Figure 4: Number of companies in the Y axis (log scaled) and percentage of IPv4 and IPv6 (zoomed) respectively in X axis.*

We can see from the information that it is not feasible at the moment that any of the companies own the monopoly and therefore are able to control the chain.

In Figure 5 we can see that for the IPv6 data, the ranking changes, this is because the number of IPv6 addresses is significantly bigger than the one of IPv4 and because IP assignments are done in larger chunks. In this case, the company with the most stake is at ~22%. This is not a problem for our solution, it only means that the threshold of the (k,n)-threshold signature of the consensus algorithm will need to be set to a percentage bigger than this.

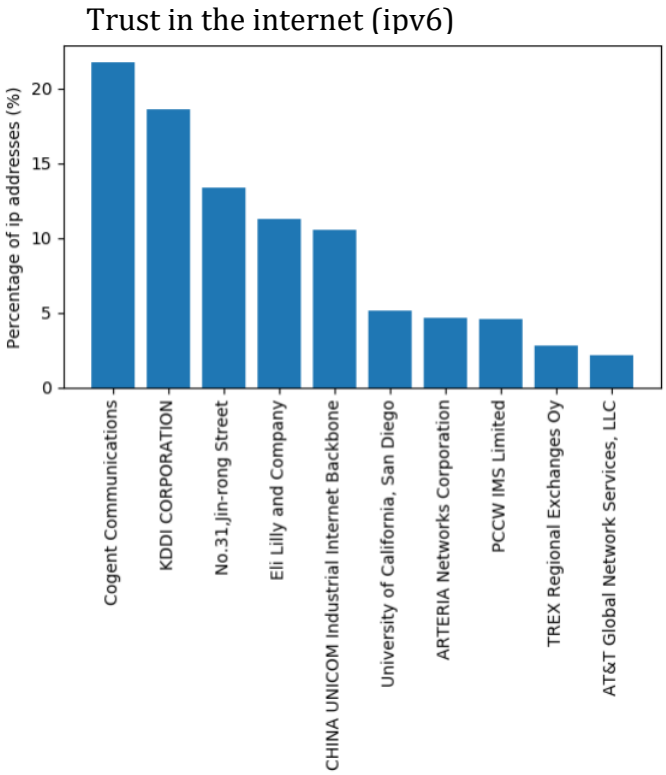


*Figure 5: Percentage of IPv6 adresses by company (more than 1% only)*

In Figure 4 we see a histogram displaying the data distribution. With it, we are able to understand the data distribution of the IP addresses, in which we can see that

most of the companies have a very low percentage (< ~3.5%) and we can see that in the IPv6 very few companies (< ~20) have a high percentage of the IP addresses which is also the case in the IPv4.

#### 9.1.3.2 Trust by countries and continents

For the country and continent experiment, we found the data, which basically groups the companies by country, to be quite different. In Figure 6 we can see that the country with the most IP addresses is the United States with 40%. This is still an unsuficient percentage in order to be a threat to the blockchain design.

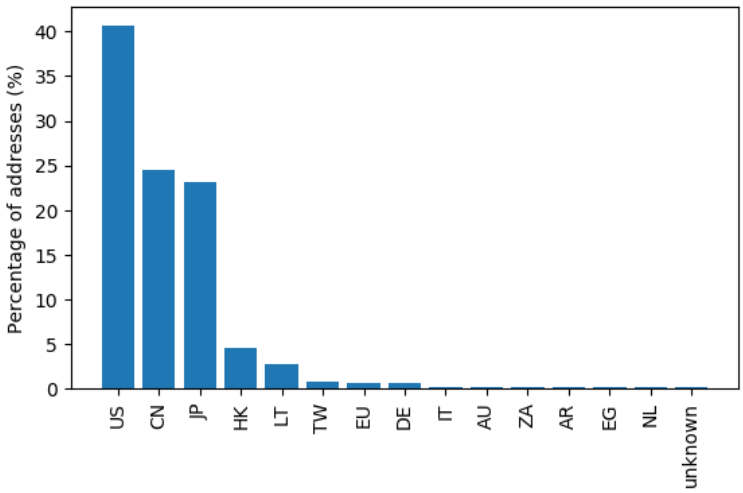


*Figure 6: Percentage of IP adresses by country (top 15)*

In order to better analyze the data, we decided to create a graphic displaying the data grouped by Regional Internet Registry (RIR), a RIR is a regional aggrupation which supervises the assignation and registration of resources such as IPs or ASs. The RIRs are more or less a reflection of the continents, as they are divided in ARIN (North America), RIPE NCC (Europe, Central Asia, Russia, and West Asia), AFRINIC (Africa), APNIC (East Asia, Oceania, South Asia, and Southeast Asia), and LACNIC (the Caribbean and Latin America). We also added the US, China, and the European Union to better understand their stake in the blockchain.

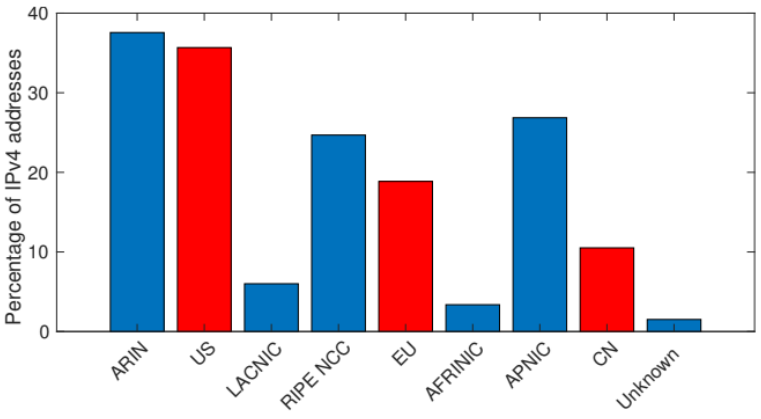


*Figure 7: Percentage of IPv4 addresses by RIR and some relevant agroupations.*

This data is found in Figure 7, and we can see that the RIR with most stake does not go over the 40% barrier. As discussed with previous data, this is not a threat to the security of the blockchain. The red bars display the data for a significant country or aggrupation which is inside the previous blue bar, so each red bar is a subgroup of the previous blue bar.

In Figure 8 we can see that the distribution of IP addresses by country resembles the one on the previous section, most countries own a little percentage of the IPs.

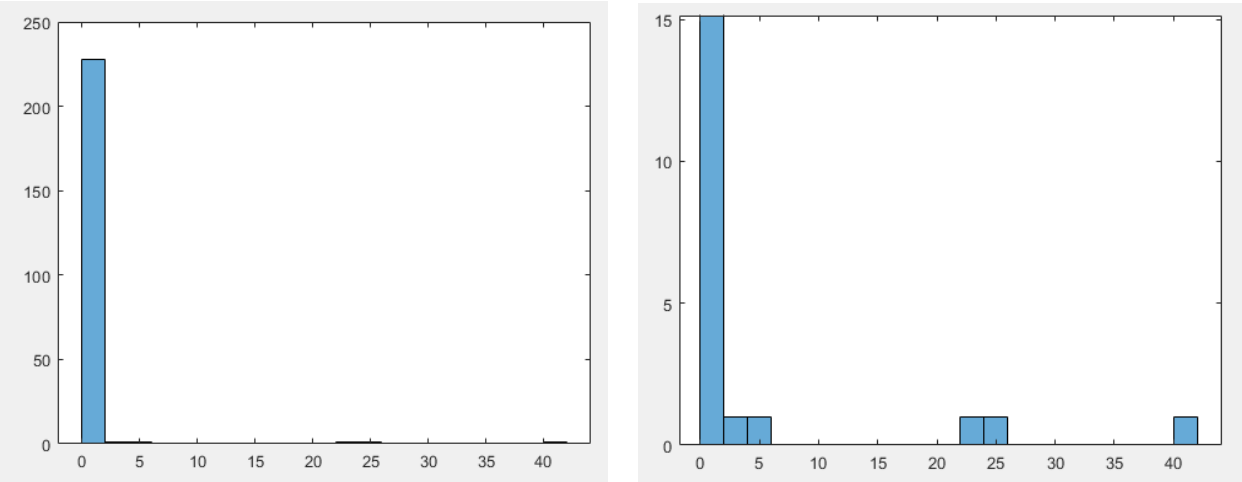


*Figure 8: Number of countries by percentage (Histogram), normal and zoomed version respectively*

## 9.2 Block creation performance evaluation

This second experiment was designed to test whether or not the part of the prototype in charge of creating blocks is technologically feasible in the real world. The block creation is the base of the prototype so ensuring that it runs fast is key to the project's performance.

### 9.2.1 Why

As explained in the technical background section, the purpose of the blockchain is to record the transactions, and this is done in using blocks which contain them. It is required then that our blockchain is able to record transactions at a speed equal or greater than the one required in a real-world scenario. We set it to be of at least 30 seconds per block, which should be fast enough.

We tried to emulate a realistic setup to test the block time and we extracted a series of data from the experiments that we considered useful to determine its real-life applicability.

Another purpose of this experiment is to check the current prototype efficiency and visually see where it loses its efficiency.

### 9.2.2 How

To measure the blockchain in conditions as realistically as possible, we rented 10 virtual machines (VM) from Amazon located all over the world (Canada, Ireland, Mumbai, North California, North Virginia, Sao Paulo, Singapore, Sydney, Tokyo, and Frankfurt) so that the network conditions were similar to those of real life. The VMs are not very powerful, they have a virtual processor which is inside an intel processor up to 3.3 GHz and 2GiB of RAM memory. If applied in real-life, this prototype should run in network equipment like routers, which are also not very powerful. We believe that the conditions of the experiment are realistic enough to get a good indicator on the block time.

To do the test we simply run the prototype at the same time in all VMs without any transactions, with around ~100 participants per node, so a total of about ~1000. These nodes started creating blocks without transactions, so they did the DKG, BLS, and block creation process. They repeatedly created blocks as soon as the shares were ready instead of a fixed block time which is the typical approach in blockchains. While doing this, measures on the time were taken and the data in the next section was extracted. The data is taken from many different runs of the experiments were at least 100 blocks were created in total. This is done in order to minimize the impact of external influences such as network speed, which could vary at different points in time.

### 9.2.3 Results

We did two types of tests, first of all, we measured the block time for different thresholds for the BLS, and secondly, we performed profiling of the python code in order to find were the prototype spent the time. We will now look at the data extracted from each experiment.

#### 9.2.3.1 Minimum block time by threshold

For this experiment, we used 100 participants in the BLS and did tests with 20, 35, 50, 65, and 80 participants as the threshold. In Figure 9, we can see the results of the test. We first thought that the block time would increase as the BLS threshold increases, but the results showed otherwise, and the reason for this is explained in the next section. The block time is around ~6.2 seconds with a low difference in the results for each threshold.

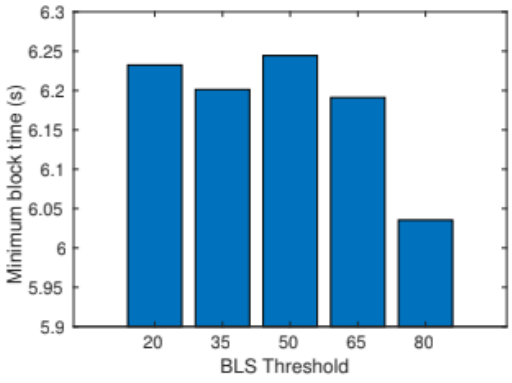


*Figure 9: Block time by BLS threshold*

The block time is faster than it is required and this proves that this part of the prototype is perfectly suitable for a real-life scenario, nevertheless, in this experiment, other key functionalities of the prototype were not evaluated and this does not yet prove the full viability of the project.

#### 9.2.3.2 Where is this time spent?

In this experiment we decided to present the data differentiated in two different graphics, one corresponds to the profiling of the prototype when the node has been selected to create a block, and the other when the node is not selected to create the block.

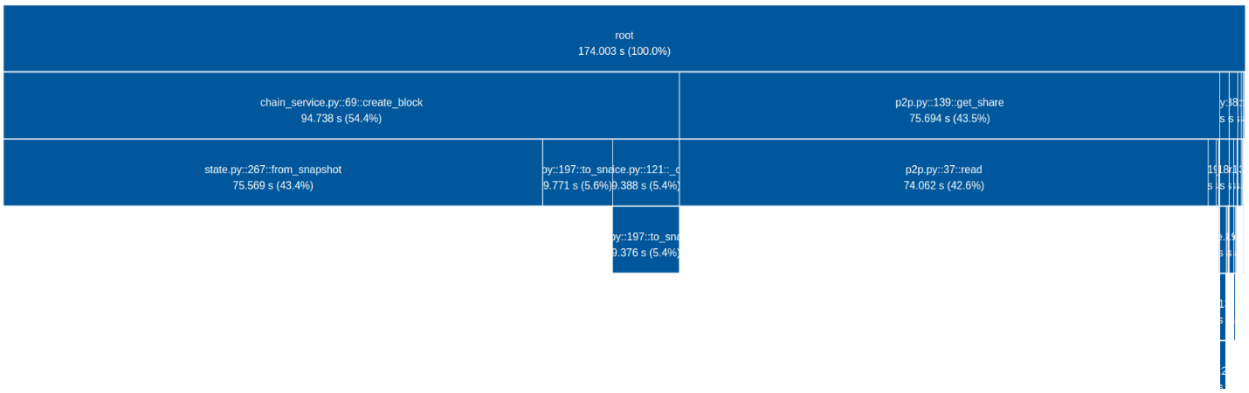


*Figure 10: Icicle displaying the time spent in different functions when the node has been selected to create a block.*

In Figure 10 we can see the graph which displays the time spent in the python code when a node has been selected to create a block, we can see that the time is spent basically in two different functions: the get_share function, which is in charge of asking the p2p process for new shares data, and the create_block function, which creates the block and broadcasts it to the network.

Thanks to this data we could identify and efficiency issue which explains the results in the previous tests, we found that the cryptography functions for processing shares are very

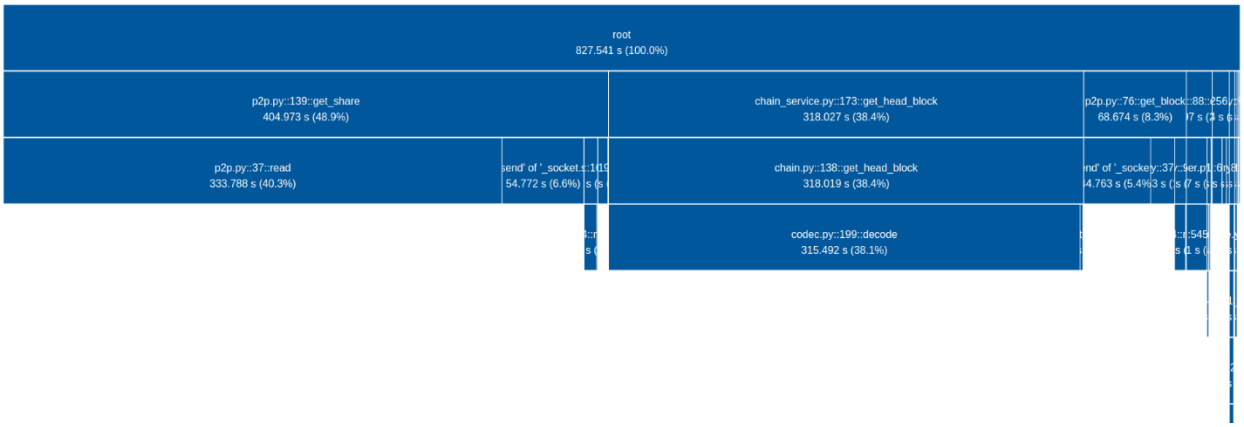


*Figure 11: Icicle displaying the time spent in different functions when the node has not been selected to create a block*

lightweight, but the get_share function consumes a large amount of resources, and our code reads all the shares regardless of if it has enough shares (threshold shares) to compute the next random number, and this caused the block time for different thresholds to be roughly the same.

In Figure 11 we can see the same graphic as in Figure 10, but this time the node has not been selected to create a block. The time percentage for the get_shares function is practically the same, but the other two more time-consuming functions are get_head_block and get_block, the first one is a function that is run at every iteration of the infinite loop, which means that this time is actually time were the node is waiting for a block to be received, and the get_block function asks the p2p process for new incoming blocks and is also done at every iteration until a new block is received. This part of the prototype is therefore not as important, as the bottleneck of the is found in the block creation, and this is why this process spends some time waiting without actually doing any computation.

The main problem found in this experiment is that the communication between the p2p process and the blockchain is done in a synchronous way rather than asynchronously, and this has a big impact on efficiency.

Both datasets are extracted from multiple block creation process to reduce the impact of external variables.

## 9.3 Overall performance

The objective of this test is measuring the capability of the prototype to achieve a functioning performance which is able to withstand real-life conditions.

### 9.3.1 Why

We did this test in order to test the real-life applicability of the prototype with all of its features running. Our plan is to see if it would be able to support a load similar to the one found in the current BGP protocol. We found that the current average BGP update messages per second are ~15 according to the BGP Instability Report [24]. Even though not every BGP update message means that a transaction in the blockchain will be made, we used this value as an upper bound, meaning that, if the prototype is able to achieve it, it will also be able to achieve the required real load, which will be less.

### 9.3.2 How

To do this we deployed the prototype in the same configuration as the previous test, so 10 VMs located around the world, and this machines will automatically create transactions at speed equal to 15 transactions per second. This time we set a block time of 40 seconds in order to avoid synchronization issues and better emulate a real-life scenario, so each block should contain an average of 600 transactions.

### 9.3.3 Results

The prototype managed to achieve a speed of about 8 transactions per second, which is below the threshold we set previously. To explain why we did profiling of the prototype and we will now evaluate the data obtained. As in the previous experiment, the data is presented in two different figures, one for the profiling when the block is received and the other for when the block is created.

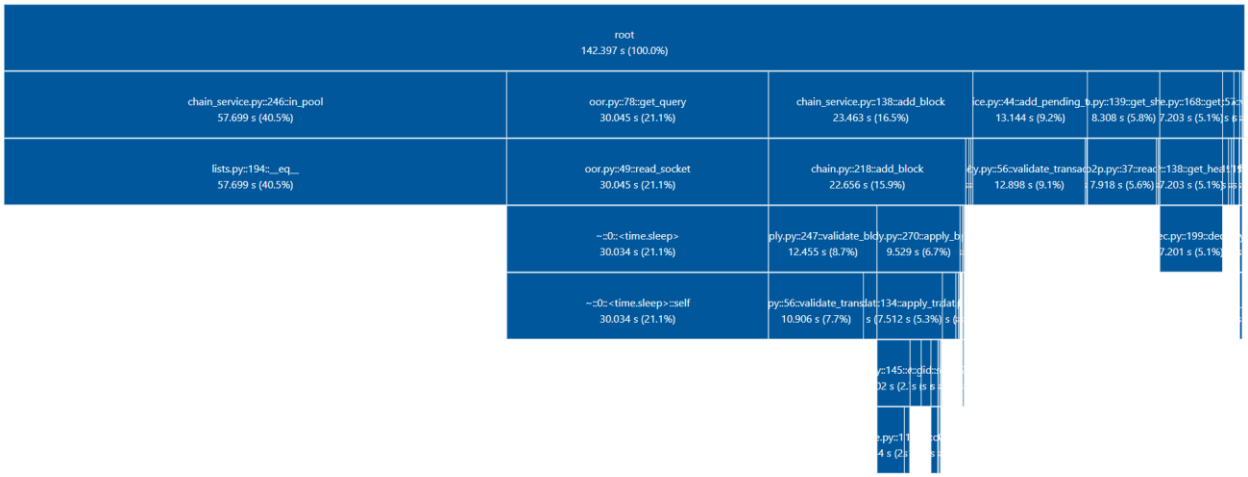


*Figure 12: Icicle displaying the percentage spent in each function during the block receiving phase.*

In Figure 12 we can see that the biggest sections of the time are found in the in_pool, get_query and add_block functions. The get_query suffers from the previously detected problem of the synchronous sockets, the other functions are a result of different problems.

The in_pool function simply checks if a transaction is inside the transaction pool, which is an array of transactions, this limitation makes it hard for the prototype to complete all the required transactions required to achieve the 15 transactions per second mark. Even though this limitation exists, it is also safe to say that it could be easily solved by implementing the transaction pool with data structure more efficient when checking whether an element is in it or not, for example, a hashtable or a set.

The add_block function is also expensive. The explanation we found for it, is that partly due to the local database in charge of keeping the blockchain data, this process is not very fast. We believe that alternate solutions which are able to store the data in a more efficient way could be found to this problem.

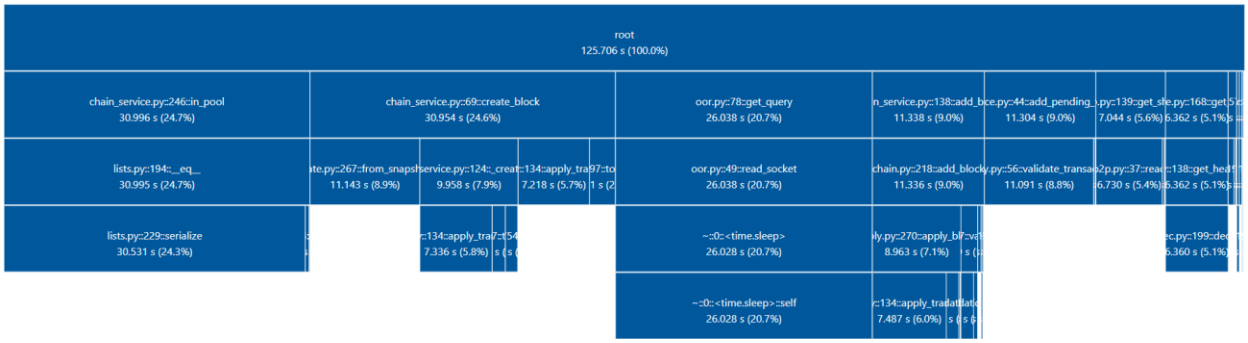


*Figure 13: Icicle displaying the percentage spent in each function during the block creation phase.*

In Figure 13 we see that the graph for the block creation is not very different, the previously mentioned functions also have a big impact in this part, and solving this issues would also speed up the block creation process.

So, although the results are not totally favorable, we are in an order of magnitude close to what is expected, and thanks to the profiling we were able to identify some issues which made the solution less efficient and were limiting its processing capabilities. Thankfully, these issues seem to be relatively easy to fix and the prototype should be able to function at 15 transactions per second effortlessly once they have been solved.

# 10. Conclusions

From the tests we did, we can draw two main conclusions. First of all, we can see that the actual scenario of the IPs distribution could be easily supported by our prototype, as the biggest monopoly currently existing is of the 40% of the stake. This would only mean that the threshold of shares would need to be higher than that. Also, looking at the future, if this situation evolved, the prototype allows this value to be changed. The monopoly problem should not become a threat to the architecture of the chain until the biggest stake is able to reach at least 80% of the IP addresses, which is very far from the actual data. In a scenario with a 80% threshold, it could happen that nodes participating in the threshold signature got disconnected during the process. In this situation, it would be hard to reach the threshold and consensus. If this happened another threshold signature would need to be created, using the previously explained DKG process, and it is time-consuming.

Secondly, we found the block time test results were good enough to be able to meet the requirements, but we found some issues in the overall performance experiments. The main issues that explain this are two: the socket calls are blocking, so asking for data to the communication process is done synchronously and this impacts the speed of the process. Also, we found the data structure of the transaction pool to be inefficient when checking if a transaction is found in it. This issue can be solved by using a set as the data structure used for the transaction pool.

We also found another issue in the database performance, which we consider that could be faster. Nevertheless, we consider this issue to be minor as it doesn't affect the performance as much as the others.

Our evaluation shows that the prototype can reach 8 transactions per second, which is in the same order of magnitude of our requirements (15 tx/s). By solving them, we can easily overcome this limitation.

In conclusion, once the mentioned issues are solved, we believe that the prototype will prove potential in solving the BGP protocol in a secure, fair and efficient way. The purpose of this thesis is to provide to the organizations in charge of managing the routing system of the internet with data and an early proof-of-concept which allow verifying that the proposed solution can potentially meet the requirements of the system.

# 11. References


[1] J. Paillisse *et al.*, "IPchain: Securing IP Prefix Allocation and Delegation with Blockchain," May 2018.

[2] M. Crosby, P. Pattanayak, … S. V.-A., and undefined 2016, "Blockchain technology: Beyond bitcoin," *j2-capital.com*.

[3] "Namecoin." [Online]. Available: https://namecoin.org/. [Accessed: 26-Feb-2019].

[4] "Pakistan hijacks YouTube | Dyn Blog." [Online]. Available: https://dyn.com/blog/pakistan-hijacks-youtube-1/. [Accessed: 25-Feb-2019].

[5] R. Bush and R. Austein, "The resource public key infrastructure (RPKI) to router protocol," 2013.

[6] S. G.-C. ACM and undefined 2014, "Why is it taking so long to secure internet routing?," *cs.princeton.edu*.

[7] X. Liu, Z. Yan, G. Geng, X. Lee, S.-S. Tseng, and C.-H. Ku, "RPKI Deployment: Risks and Alternative Solutions," 2016, pp. 299–310.

[8] "Statistics — RIPE Network Coordination Centre." [Online]. Available: http://certification-stats.ripe.net/. [Accessed: 25-Feb-2019].

[9] "Regional Internet Registries Statistics - RIR Delegations - World - Autonomous System Number statistics - Sorted by number." [Online]. Available: https://www-public.imtbs-tsp.eu/~maigron/RIR_Stats/RIR_Delegations/World/ASN-ByNb.html. [Accessed: 25-Feb-2019].

[10] A. Hari, T. L.-P. of the 15th A. W. on Hot, and undefined 2016, "The internet blockchain: A distributed, tamper-resistant transaction framework for the internet," *dl.acm.org*.

[11] S. Angieri, A. García-Martínez, B. Liu, … Z. Y. preprint arXiv, and undefined 2018, "An experiment in distributed Internet address management using blockchains," *arxiv.org*.

[12] A. Gómez-Arevalillo, P. P. workshop on, and undefined 2017, "Blockchain-based public key infrastructure for inter-domain secure routing," *hal.inria.fr*.

[13] "BGP and Route Monitoring | ThousandEyes." [Online]. Available: https://www.thousandeyes.com/solutions/bgp-and-route-monitoring. [Accessed: 26-Feb-2019].

[14] "Route Monitoring | BGPmon." [Online]. Available: https://bgpmon.net/services/route-monitoring/. [Accessed: 26-Feb-2019].

[15] "IRR Overview." [Online]. Available: http://www.irr.net/docs/overview.html. [Accessed: 26-Feb-2019].

[16] J. Paillissé, A. Rodriguez-Natal, … V. E.-I. draft-paillisse, and undefined 2017, "An analysis of the applicability of blockchain to secure IP addresses allocation, delegation

and bindings," *ietf.org*.

[17] A. Rodriguez-Natal, J. Paillisse, … F. C.-I., and undefined 2017, "Programmable overlays via OpenOverlayRouter," *ieeexplore.ieee.org*.

[18] T. Hanke, M. Movahedi, and D. Williams, "DFINITY Technology Overview Series, Consensus System," May 2018.

[19] V. S.-I. C. on the T. and and undefined 2000, "Practical threshold signatures," *Springer*.

[20] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, "Secure Distributed Key Generation for Discrete-Log Based Cryptosystems," 1999, pp. 295–310.

[21] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," 2001, pp. 514–532.

[22] G. Bonet, "IPChainTests Repository," 2019. [Online]. Available: https://github.com/Guillembonet/IPChainTests.

[23] "blockchain-mapping-system." [Online]. Available: https://github.com/OpenOverlayRouter/blockchain-mapping-system.

[24] "The BGP Instability Report." [Online]. Available: http://bgpupdates.potaroo.net/instability/bgpupd.html.