haute école
neuchâtel berne jura

Hes·so
Haute Ecole Spécialisée
de Suisse occidentale
Fachhochschule Westschweiz
University of Applied Sciences and Arts
Western Switzerland

Bachelor Spring Project

HE-ARC 2016

Overclouds

Author:
Romain Claret

Supervisor:
Marc Schaefer

May 12, 2016

Abstract

Overclouds is a project whose goal is to create an anonymous and decentralized internet data sharing service right through the browser.

1 Description

1.1 English

The initiative behind the project is to create a new generation of internet data sharing tools, suited for today's paranoia for privacy on the internet and the preservation of knowledge for the next humanity generations.

The idea is to give the ability to the user to not rely on corporate servers, or farms of servers anymore. On Over Clouds, everybody and everything are now anonymous nodes, and they connect one to another freely and anonymously.

The network is a democratic mesh of nodes. The data is moving from a node to another across the network via other nodes and is ruled by the consensus of users.

We are aiming that users only need to have a standard Internet connection and a browser with JavaScript capabilities to use the service.

1.2 French

Must to the translation when the English part is validated

Contents

2 Preface

2.1 Introduction

Today The world and more particularly the digital world has an important concern for privacy. Indeed, Edward Snowden's revelations on NSA's massive spying[18] led to a massive media scandal. People started to feel that their digital privacy was at stake by the worldwide "spies", either the government, companies, or even unknown treats yet. Resulting that the internet community evolved and it became an important economical and political part.

New behaviors emerged Right into the web users, a noticeable split has been made, into two classes of people. Individuals who don't know how to protect their privacy on the Internet, and people who do know how to protect their privacy. For the first group, some are not aware of the global privacy status, some don't care and some don't know how to protect themselves. Concerning the second panel, we have some personal ethical problems, which led to this project.

The problem It's understood that people want to avoid advertising companies' and governments' tracking. It's also known that some people are scared that their stole private data could be exposed publicly. However, some private data must be sometimes public and some cases forced to be made public. From our humanistic and unpolitical point of view, we believe, that the data from terrorist groups (including their members and partisan) have to be denounced, made public and the locking the data into a secured safely. Why archiving and not just deleting them? We, again, believe that regardless how bad the data is (as seen today), it's still part of our history, and it's our duty to preserve them as a legacy for future generation to understand and learn from what we are mistakes today.

Intellectual Properties Read as IP. Our social and political evolution led to copyright laws, which prohibit the free sharing of any kind of data such as art and knowledge by default. Indeed, our culture specifies that any intellectual discovery or advancement is by default protected by copyrights (we will not discuss the process here neither the manipulation of the copyright

system). This led usually into knowledge or data retention, which makes us feel that the IP system is serious treat for our humanity legacy.

Economy However, it's also understood that with our economical system, people need to make a living out of the IP, which leads into higher protection for their data. Our digital method of protection is to encrypt the data with a digital key provided by the owner (generally companies). The encrypted data is then stored in data centers or on hard-drives (which could some times be bad for the long term preservation). Owners then have the choice of sharing their (copyrighted) material and are usually also choosing to use encrypted manners to distribute them. The transmission protection is to unable people from looking at them without owners' consent (usually money) and redistributing them with consent (not making money out of it). So, the data is protected for the storage, during transmission, and we also have DRMs technology that only descrypts the piece of data you are looking at on the fly. So, technically, the full data is never in clear anymore.

Game of cat and mouse Some people are protecting data, other are trying to break the protection to retrieve them. And they both use encryption technologies to secure their transmissions. Meaning that the owners are protecting their data, and the *thief* are also protection the stolen data to not by caught. At the end the same data is being transmitted anyway but never in clear. This procedure make us believe that something is wrong with the system and that it could be considered as a treat for the humanity global knowledge and culture.

Legacy We are confronted with another ethical problem. We are entering into a fully encrypted data era, which will make all our data appear as a bunch of random noises that for various reasons are bad for us. We would like you to think about how all our global knowledge is and will be sorted in the near future. Data such as art or knowledge, how will our next generations of humans be able to retrieve it in a few years? How can we be sure that the unbreakable keys (quantum proof, etc.) that we are making today will not be lost? Now think about the idea of randomizing (with encryption noises) our communication signals that we are sending into outer space? The signals that we are sending out to space are already today much different from what it looked like in the sixties. For example, purely analog signals (TV, FM

radios) are depreciated and got replaced with numerical transmission (DVB, DAB), and of course most of them are encrypted (pay-to-watch tv, pay-to-listen radios). Moreover, our communication technologies involve into higher frequencies and always fewer power consumption. All this is resulting into the fact that today, Earth radiates probably much fewer waves than before and seen as random noises.

Taking the wrong direction It's easily imaginable that soon a company will say: "Hey, we are specialized in transmitting encrypted data, nobody will ever know what you are doing, and when you are doing it. All you have to do is to buy from us, with a crypto-currency, a key every month.". See this has an evolution of the VPN services. We don't have a sharp opinion on neither it's a good or a bad thing. However, it will create a privatization of the data security, and it most likely to destroy any hopes of retrieving the encrypted data one day.

Overclouds The project aims into a new approach for protecting people's privacy and ensure a legacy for future generations. The main idea is that Overclouds is a consensus-driven anonymous network of nodes with storage and computation power. Each node is aware of other nodes, but they are unable by default to identify this owner on the main net (whatever the physical technology of communication at any given point of time). The consensus, as limitless power over the network. It can, for example, decide to disclose the physical location of particular nodes, if they considered malicious or bad for the rest of the network (such as terrorists, scammers, black hats, etc.).

Nice to have We also would like that Overclouds was designed to not act like random noises. Preferably, external and internal listener or watcher should see a nice mathematically driven signal. The mathemagical behind it would allow any source node to predict exactly how its data is will handled by default by the consensus. However, it should be unpredictable for other nodes, but still elegant to look at.

2.2 The Big Picture

Now that you have been introduced with the project. Let us present you our current vision for the final outcome of the project.

The consensus

2.3 Original design

During the project bootstrapping, global solutions and concepts emerged as the first overview of the project. Below is the result of the initial concept. However note that during the effective research and analyses, the project has evolved, sometimes resulting in new architectures and new recommendations.

2.3.1 The mesh of trust

Acting like a consensus of trusted nodes on a node network.

Certificates Each node has a unique nontransferable certificate, which can be regenerated as a new one. It is used to individualize nodes, and allow nodes to trust each other. The network is storing the certificates, and keep track of its proof-of-activity[3] ranking.

Indeed, the certificate level increases over time by providing proof-of-activity. The level is also influenced by the amount of trust given to other nodes from the network. Note that nodes alone are not aware of others trust interactions, they kept informed of the sum of nodes willing to share their data with it.

Identities Users can use any node from the network. For a user to identify himself, he needs to generate at least one unique identity. Identities are created from an existing node that is already part of network. Each identity has a public and private key, a parent node (hardware of generation), and optional information (languages, avatar, name, etc.) for internal applications to the network.

An identity cannot be alternated. The user must generate a new one with the previous one was banned, and restart the process of acquiring trust from the network. Depending on situations, they must also need use another node.

Network requirements A node doesn't need an identity to be able to connect to the network. It connects automatically and integrate the mesh of nodes by giving storage and computational power. However, an identity

requires a node to connect to the network and interact with it. So, a node works without an identity, but an identity always needs a node.

Democracy Identities are able to create votes and of course votes for submitted proposals, which are creations or modification of the rules ruling every transaction on the network. Each identity are weighted by default to the initial vote unit and can vote once. However the consensus can decide to give more weight or votes to specific identities. By default, nodes can be used only once to give a vote (except if the consensus decides else-wise).

Bans Certificates and identities can be banned from the network after a trial or directly from the consensus. A flag, seen globally by the network, is rise for the banished nodes or identities. During a trial, a random amount of random identities are asked to vote on the event that led into the trial.

Flags Node can flag specific certificates or nodes on the network and apply rules on them, such as filters for minimum certificate level required to be able connect to them as a relay. The flags are then used by the network, and route communications depending on the nodes' preferences.

For example, in the case of a node receiving data from another node that is not matching its filter, the data would be rejected at entrance. In the case of spam, which assumes that the attacker knows what destination (that he sees as void) to target, the destination node will indeed consume power to deny requests. A solution has to be find for case of a figure and prevent spam.

Another example, the node rerouting. A node can decide to not relay data. In this case, the data is either sent back, which can result in a load problem. Either the data is lost, which is in the case of a UDP-like protocol bad. In the case of a TCP-like protocol, the node would be searching for another node to go through. The second option could on another hand surcharge by searching new paths.

Storage Data is stored across the network. It is spread on the network as encrypted chunks belonging to an identity, the private and public keys for the data is also spread across the network and belongs to the network. The data and its keys have redundancy chunks, also spread across the network.

Data owners The owning rights are given and managed by the network to a specific identity. The owner can give as he wish the reading, writing, and executing rights to any nodes or identity on the network. He can also set a public access for certificate or trust levels. The ownership is of course revocable or transferable by the consensus. However the owner can also transfer the ownership to another identity. Both parties must accept the transfer. Note that he cannot transfer blamed data.

Blames A node can anonymously blame chunks or nodes and leave a reason for the blame from list of multilingual generic reasons. Note that the consensus can also create new categories. Each node can blame a specific data only once. An blaming identity is then linked to the note used to blame, by this mean it cannot vote more than once per data. Plus the first identity to use the node gets the blame validated.

A blame is telling the network that a node or a chunk is not appropriate to the other nodes. Multiple blames on a node may result into a ban of its certificate. Multiples blame on a specific chunk or chunks belonging to the same data resumes into a revocation of all rights given to to nodes even the owner.

Data Tribunal Once the required amount of blames reached the network select unrelated random identities and asks them to rate the blame. The digital judges would be able to read the reasons left during the blaming phase. However they are not able to read the content of the data itself. Except is the consensus decides otherwise. Owners can ask for a second trial if they think the judgment was unfair and add a generic argument. For the second trial, different unrelated random nodes will have to rate the blame again. The decision from the second trial is definitive. The data is either archived, either the owner and related nodes get their rights back.

Internet Service Providers They should not be able to interpret the network activity. They are only aware of encrypted tunnels made to random nodes. Like the Tor network, the gateway nodes never the same. It allows a censorship protection.

Internal crypto-currency Nodes are automatically retrieving units of the internal crypto-currency with their proof-of-activity. The network owns the

currency. Rewards are given to identities for good behavior and participation. The currency is transferable to unbanned identities. However, an identity has no interaction access to its balance during the trial phase. If the identity is banned, its currency balance is returned to the network. The use of the crypto-currency is not really clear for the moment, but it could be used as fuel like on Ethereum[19].

Backdoor The project is not friendly for 3rd party authorities like governments, police investigations, companies etc. However the consensus has virtually unlimited power over the network and can model the its democracy as it is pleased. We can easily imagine that the consensus decides to disclose all the pedophiles from the network with the goal that they would be punished by the *real world*. The consensus decides what is right or wrong, and morality.

Artificial Intelligence Based on today's technology it's unlikely to see a very smart AI emerge inside the project. However, we could imagine applications like self-preservation, meaning that the network could learn and decide by itself with the consensus is right or wrong.

Communication The speed and size of the transactions should be compliant with the any bandwidth. For example, the network should be able to work on a network of ALIX node bidden to a Xbee connection. Or networks from emergent 3rd world.

3rd parties Depending on the technologies used on the project, we could, in a first time, use 3rd party services like Tor, Github, Twitter, Bittorrent trackers, etc. (note the public status and censorship of the example). The security could be compromised during the bootstrap phase in some cases because the ISP and others services could target and track nodes' activities.

Compromised users In the case of malicious software presence on a system used by the node solutions can be taken into account. Assuming that there is less than X% (exhausting value to estimate at this phase of the project) of malicious software designed for the network. It's indeed difficult to protect people from malicious people. We could add security layers, like a Pin or a passphrase, but if the user is running a key-logger, it will always be

insecure. But since the node can only be accessible from a unique hardware (certificate linked to the hardware), the stolen key could not be as useful as planned. However, the system could be also compromised by someone or something physical like the RUBBER USB[28], in which case the hardware protection could be bypassed. Now we could think of security that only shows a virtual keyboard, but a specific program could sniff the mouse positions and actions. A solution could be to use a USB-key as key, but it could also be replicated if the key is writable. We could use an external hardware, but it would impact Overclouds' public attractivity. Moreover, in the end, how to be sure that the company making the encrypting hardware will not be hacked, resulting into the release of the algorithms for generating the keys? Another solution is to control the hardware and the software, assuming that there is no way for an outer or internal entity to know what's the key. This last option would mean that Overclouds would have to be privatized somehow, and it would impact nature and vision of the project, by making part of the project proprietary.

Certificate or Identity Clones The network doesn't allow clones using the network at the same time. The consensus will decide which one is the real one, and the clone will not be ignored by the network, no peers would accept a connection from it.

In the case an identity is stolen, in the current state of the concept, the attacker would have full access to the identity's assets. However a solution to avoid this concern would be to link an identity to an unique node. Forcing the user to have different identity for each node it connects to. The attacker would have to have a clone of the identity key and a clone of the node certificate, which increase the difficulty of the attack. But it's still possible if the attacker has access to the original hardware and have the technical knowledge to emulate the hardware running the clone of victim's node certificate. To increase again the security and solve this problem, we would have to add an extra layer of security with an additional secured hardware such as a NitroKey[50]. Now, those solutions are considered extreme, in general, going this far into security is not necessary. However, if those solutions enter into consideration, we could predict an important impact on new users willing to join the network.

Note that the consensus could be able to revoke a key or certificate. A protocol for asking the consensus to revoke an identity could be implemented.

Or simply asking a lot of people to blame the stolen identity or certificate.

Unanswered questions

- Should we take into account that the wired Internet speed only improves? ... Probably ...
- Should we start from a programmable network such as Ethereum or MaidSafe? Or should we start from scratch? ... Make, buy or adapt study ...
- Would it be possible to allow nodes to run programs on the network like on Ethereum or with an API like on Maidsafe[43]. ... Probably, it could be interesting to make bots for content sharing, selling, etc. ...
- Is it possible to guaranty that a node will be able to connect to the network with a random node? What about firewalls? Would connections only be based on TOR hidden service help? or I2P? or Freenet? or services as such? ... The idea of only using a browser could be in jeopardy. ...

2.4 Objectives

TODO

2.5 Specifications

TODO

2.6 Management

TODO

2.7 State of the Art

For the project initiation, it was important to do research with the goal of targeting the needs for existing knowledge and technologies. Those information could potentially be used to help achieve this project. This subsection will expose the research done.

2.7.1 Similar products

To be straight forward. A comparable project working right from the browser without the help of any third party or background software is nonexistent. At least not from the public knowledge available with my search keywords.

2.7.2 Existing Networks

The most common form of networks approaching our project's vision are called *Darknets*[4] and they started to emerge during the years 2000ish[12]. They are all aiming to encrypt data transmissions and protect network's users from being spied on and bypass censorship.

Freenet[9, 10] Description from the official website [22]

> Freenet is free software which lets you anonymously share files, browse and publish *freesites* (web sites accessible only through Freenet) and chat on forums, without fear of censorship. Freenet is decentralised to make it less vulnerable to attack, and if used in *darknet* mode, where users only connect to trusted nodes (real life friends, etc.), is very difficult to detect.
>
> Communications on Freenet nodes are encrypted and are routed through other nodes to make it extremely difficult to determine who is requesting the information and what its content is.
>
> Each user contributes to the network by giving bandwidth and a portion of their hard drive for storing files. Files are encrypted, so generally the user cannot quickly discover what is in his *datastore*. Chat forums, websites, and search functionality, are all built on top of this distributed data store.

I2P[21] Description from the official website [31] Originally IIP[32].

> The Invisible Internet Project is an anonymous network, exposing a simple layer that applications can use to anonymously and securely send messages to each other. The network itself is strictly message based, but there is a library available to allow reliable streaming communication on top of it (a la TCP). All communication is end to end encrypted (in total there are four layers

of encryption used when sending a message), and even the end points (*destinations*) are cryptographic identifiers (essentially a pair of public keys).

MaidSafe[43] Description from the official website [42]

> The SAFE (Secure Access For Everyone) Network is made up of the unused hard drive space, processing power and data connection of its users. It offers a level of security and privacy not currently available on the existing Internet and turns the tables on companies, putting users in control of their data, rather than trusting it to organizations.

Tor[15] Description from the official website [61] "Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security."

ZeroNet[67] Description from the official website [66]

> Real-time updated, P2P websites using Bitcoin cryptography and the BitTorrent network. Zeronet is decentralized, open source software in Python aimed to build an Internet-like computer network of peer-to-peer users. It is not anonymous by default, but users can hide their IP address by using Tor which uses Bitcoin cryptography and the BitTorrent network.

Project Maelstrom Description from the official website [6]

> BitTorrent wants your help creating a P2P-powered web with Project Maelstrom. (Beta on Windows only) The Maelstrom Network - currently under hectic development - is gearing up to be able to provide users and developers a joined interface to each other. Unlike some distinct offerings out there, this isn't a social network, and it never will be. All your information is for your eyes only until you allow an application to use it. We're trying to get web applications to a first class status on the web, similar to how an application on your computer is tightly integrated into the rest of the computer.

Diaspora* Description from the official website [13] " The community-run, distributed social network. diaspora* is based on three key philosophies: Decentralization, Freedom, and Privacy. "

FlowingMail Description from the official website [20]

> FlowingMail is the name of a new decentralized, secure and encrypted email protocol. The most used email systems rely on a central server that receives, stores and forward the messages: FlowingMail is decentralized and does not rely on a central server to deliver the encrypted emails. The scope of the FlowingMail protocol is to hide the information being transmitted and the parties involved in the communication. The main component of the FlowingMail protocol is a Kademlia Distributed Hash Table (DHT), which is responsible for storing the encrypted emails while they are in transit and the certificates of the participants in the FlowingMail network.

Bitmessage[63] Description from the official website [5]

> Bitmessage is a P2P communications protocol used to send encrypted messages to another person or to many subscribers. It is decentralized and trustless, meaning that you need-not inherently trust any entities like root certificate authorities.

Retroshare Description from the official website [51]

> RetroShare is free software for encrypted filesharing, serverless email, instant messaging, chatrooms, and BBS, based on a friend-to-friend network built on GPG. It is not strictly a darknet since optionally, peers may communicate certificates and IP addresses from and to their friends.

MediaGoblin[64] Description from the official website [46] "MediaGoblin is a free software media publishing platform that anyone can run. You can think of it as a decentralized alternative to Flickr, YouTube, SoundCloud, etc."

Movim Description from the official website [48]

> My Open Virtual Identity Manager is a distributed social network built on top of XMPP, a popular open standards communication protocol. Movim is a free and open source software licensed under the AGPL. It can be accessed using existing XMPP clients and Jabber accounts.

The IPFS Project[2] Description from the official website [35]

> The InterPlanetary File System is a new hypermedia distribution protocol, addressed by content and identities. IPFS enables the creation of completely distributed applications. It aims to make the web faster, safer, and more open. IPFS claims to be a Permanent Web with a new peer-to-peer hypermedia protocol.

Serval Project[25] Description from the official website [54] "Serval is a telecommunications system comprised of at least two mobile phones that are able to work outside of regular mobile phone tower range due thanks to the Serval App and Serval Mesh."

Open Garden Description from the official website [24]

> Open Garden's technology creates a software-based network, also known as a peer-to-peer wireless mesh network, among participating mobile devices using WiFi, Bluetooth LE, and other technologies. Open Garden's innovations include: seamless device discovery and pairing, offline identity, a proprietary network protocol for addressing and routing messages off-the-grid, distributed algorithms for managing mesh networks, advanced traffic management (multi-hop, store and forward), and battery use reduction.

Hyperboria[29] Description from the official website [30] "A community of local Wifi initiatives, programmers, and enthusiasts. They are running a peer-to-peer IPv6 network with automatic end-to-end encryption, distributed IP address allocation, and DHT-based Source Routing."

2.7.3 Transfer Protocols

TODO

2.7.4 Protection

TODO

2.7.5 Cryptography

TODO

2.7.6 Hardware

TODO

2.7.7 Block-Chains

So much hype in this, but what is it? Everybody relate it mainly to *Bitcoin*[53], indeed *Bitcoin* introduced this technology (which is its main innovation), but *Bitcoin* is not equivalent to chain-block.

Indeed, the main idea is that no one controls or owns the chain of blocks and forges a system for electronic transactions without relying on trust. A block contains a timestamp and information linking it to a previous block.

Note that a block looks like digital objects that record and confirm when and in what sequence transactions enter in the block chain.

Blocks created by network users with specialized software or specially designed equipment. Block creator are known as "miners" to reference the gold mining. Bitcoin showed us a pretty amazing evolution in the mining procedure; it was designed at the start by Satoshi Nakamoto for CPUs, then it quickly involved into GPU mining then into programmable chips (FPGA) then now it goes into burned circuits (ASIC).

In a crypto-currency system, miners are incentivized to create blocks to collect two types of rewards: a pre-defined per-block award and fees offered within the transactions themselves, payable to any miner who successfully confirms the transaction. Every node in a decentralized system has a copy of the blocks chain; it avoids the need for a trusted authority to timestamp transactions. Decentralized block chains use various timestamping

schemes, such as proof-of-work or more recently with PeerCoin the proof-of-participation.

Bitcoin [53] Why did everybody already hear the word *Bitcoin*? It is the first successful implementation of a distributed crypto-currency as described partially by Wei Dai in 1998[65]. The foundation of Bitcoin is the assumption that money could be anything (object, record, stake, etc.) accepted as payment for goods or services by a consensus (country, social, economical, etc.). Designed with the idea of using cryptography as proof of existence and transfer of virtual assets (proved to exist). Rather than relying on a central authority (trusted third party), Bitcoin is decentralized, meaning that it works with the network consensus. It uses the peer-to-peer technology to operate with the transaction management and verifying that the virtual assets is carried out collectively by the network.

Ethereum [19] Seen today has the new way to use the block-chains technology. It uses the currency has fuel to execute turing-complete smart contracts. Contracts, see as autonomous agents, are programs that run on the Ethereum Virtual Machine. The EVM is being part of the protocol and runs on each client contributing to the network; they are all doing and storing the same calculations. Note that it's not efficient to compute in parallel redundantly, but it offers a consensus for the computed results.

Others We can find a lot of forked crypto-currencies from Bitcoin; everybody is trying to make the success theirs. However, no major changes have been made to them expect the genesis block (the first block that determines how long will be the chain, etc.). We will just cite some of them that have some special modifications. Note also that they don't provide whitepapers.

Lite Coin[41] The major differences with Bitcoin are the time process focus to generate new blocks of 2.5 mins vs. 10 mins for Bitcoin, the use of the Scrypt[11] library and the maximum cap of coins is 84 million (4 times more than Bitcoin).

Dodge Coin [44] It started as a "Joke Currency" but it got capitalized... Its particularity is to have no limits in coins produced, however, the per block reward decreases.

Peer Coin [38] Based on the paper of Scott Nadal and Sunny King [39] for the Proof-of-Stake Peer Coin was born.

2.7.8 Decentralized applications

TODO

2.7.9 Reputation Management

TODO

2.7.10 Operating Systems

TODO

2.7.11 Technologies

TODO

3 Analyses

3.1 Block-Chains

3.1.1 Worth it?

It's important to note that with incoming quantum computers (predicted to appear wildly in 20ish years), the mining structure, the security and the anonymity must change from today's perspectives. As for today, the block-chain technology is at its hype, meaning that we see it has the best thing in the world.

However, from now the hype will decrease and maybe a new technology will emerge or/and the block-chains technology will evolve or be modeled to go in a direction we didn't expect yet.

Yes, from today's perspective, the timeframe is pretty significant, it's worth the interest.

3.1.2 What's next in crypto-currency?

As of today, considering that the technology of block-chains won't change, and it still in use for crypto-currency, it could take two types of path.

One of the paths is the neverending death and birth of crypto-currencies. Indeed, once the mining is no more profitable, the security sharply decrease because miners are verifying the transactions and are playing the role of consensus for validating transactions. Miners are mining as long as the devices allow a profit (power consumption, device rentability, etc.). In the best case, where the hardware technology follows the requirements of computational power to solve the increasing difficulty of mathematical problems. (Note that we are currently brute-forcing the solutions.) And based on the model of crypto-currency of Satoshi Nakamoto, Bitcoin, at some point in time, the maximum amount of coins will be reached, and the network won't generate coins (rewards) anymore. At this point, the only income of the miners will be the transaction fees. If the transactions fees are not high enough to motivate the miners to continue mining (and verifying/validation the operations), the currency will die due to the lack of security. So the miners will move to new profitable crypto-currency (note that they have a pretty advanced hardware for mining at this point, which will help them to start pretty well).

The second path is the modification of the source code of the actual crypto-currencies to make it compliant with the market evolution. For example, increase the maximum amount of coins, or make public keys quantum proof. Indeed, currently, the **ECDSA** is not quantum proof (however the hashing is at the moment, but SHA3 is ready, just to be safe). The problem is ECDSA, which during a transaction send the public key, and theoretically, a quantum computer can guess the private key from it. However, the address is still secure because it's the hashed public key.

But the second path is **killing** the concept of a stable currency based an expendable raw material stock, and the social and economical results are pretty hard to define. A secondary question would be: What will happen, if tomorrow, we find a new gold mine, which holds the same amount of gold already retrieved (doubling by this mean the maximum quantity of gold available), and with a retrievable difficulty level a lot decreased, so it's again profitable to mine?

So, we don't know if it will be a next big crypto-currency. In my opinion, I would bet on Ethereum. But again, it's personal.

3.1.3 Predicted evolution in block-chains

This subsection will be pretty short because at the moment, this technology is only starting to decedent the hype slope, and the only real evolution that pops out recently is the first version of **Ethereum**[62] (2013a) and more recently (2016) the Homestead version of Ethereum [16].

The particularity of Ethereum is that use the currency as fuel to run smart contracts on the EVM (Ethereum Virtual Machine) using the power of each node on the network to do a calculation, and creating a consensus on the output. This technologies evolution has for example created a startup company named *Slock.it* and an alternative "currency" *DAO* (which is unmineable) that allows the IOT (internet of things) to interact with the crypto-currency Ether. It allows, for example, to control a lock, in a hotel, a door could be locked until a client paid the door to open.

3.1.4 Proof-of-Work

Read as PoW[17, 36]. It's a protocol aiming to reduce the risks of DDOS attacks and family abuses by requiring that the client has done some computational work (processing time) before sending a request. It was a solution developed mainly for our financial world of transactions.

3.1.5 Proof-of-Stake

What is a stake? It's globally something that holds. In our case it's more like a flag can keep a land (a claimed property).

Proof-of-Stake?[39] Read as PoS. Usually in block-chains PoW, miners validate the transactions that came first depending on their CPU power. Note that the more CPU power you have (GPU, FPGA, ASIC, etc.) larger your influence is.

POS is the same thing but with different paradigms:

In one of them, Stakeholders validate with something they own (raw material like an internal currency). And put simple, everybody has a certain chance (proportional to the account's balance) per amount of time of generating a valid raw material.

In another, we are not working with the amount of raw material owned, but with their age (for example, the raw material is multiplied by the time that it was unused) which gives a weighting factor. However with this

paradigm, a collusion attack is pretty important, because we could have a super linearity by accumulating aged raw materials.

There are other different types of approaches but we will not details them all because they are not the best of consensus algorithms. (elitism, identity, excellence, storage, bandwidth, hash power, etc.)

Now, on the security side By using raw material (sort of digital assets) defined by the consensus PoS avoids a Sybil[23] attack. Which is is a technique where the attacker is trying to compromise a system by creating multiple duplicate or false identities. It is resulting into including false information, which then can mislead the system into making not intended decisions in favor to the attacker. By the way, PoW protects itself against a Sybil attack by using computational resources that exist extra-protocol.

However, in PoS' traditional approach, we have two major problems. The first is Nothing-at-Stake, and the second are Long range attacks.

Nothing-at-Stake The dominant problem is that smart nodes have no discouragement from being Byzantine[40]. Indeed, signatures are very easy to produce and they won't lose any tokens for being Byzantine. Another problem is that nodes with digital assets could never spend.

A solution to this would be to have a security layer on deposits, which would cancel Byzantine deposits. To achieve this, we would need to store information about nodes and their immoral behaviors (which are decided by the consensus) so the consensus would be able to punish them. Now, this works only if the transactions are not hidden (with the proof of malicious actions). Also, we should note that this security layer would ask more power for the consensus during the use of punished accounts. Slowing down the consensus is not acceptable because it acts as the authority and by this mean should be the cheaper to operate in power. Punishing the attackers with power consumption is fair.

Compared to PoW, where attackers aren't receiving compensations for their computational power (which is a disincentive). The PoS' security layer is trying to disincentive attackers by removing their digital assets. It could be an interesting social experiment, however, in our human's economic point of view, attackers should be pretty well disincentivized.

Long Range Attack In this type of attacks, the attacker controls account with no digital assets and is using them to create competing version of transactions. This attack is touching both traditional PoS, and the deposit security layer (as long as authentication ends in the genesis block).

The solution here would be to force nodes (and clients) to authenticate the consensus (for example with its state) by signing with the nodes that have something at stake currently, and nodes must have an updated list of nodes with deposits. It's usually called the *weak subjectivity* method.

Ghost From the full name, Greedy Heaviest-Observed Sub-Tree protocol, introduced by Yonatan Sompolinsky and Aviv Zohar[56], it allows the PoW consensus to work with much lower latency than in the blockchain protocol from Satoshi Nakamoto [53], and of course keeping it secure. Indeed, in blockchain based PoW, a miner is rewarded for each block found so the other miners can continue to mine on top of it. However, when a miner produces an orphaned block (a block that exists in the chain), they are not rewarded for their work, plus the consumed power was in vain because the work is unused by the consensus.

Here comes the solution, Ghost, which includes orphaned blocks. It introduces the notion of rewarding orphaned blocks to miners and increasing the security of the consensus with increased validations of a block in the block-chain.

Casper Now there is a friendly ghost in town, it's Casper[8]. This protocol is based on Ghost, and must be integrated into Ethereum for the Serenity[7] version (final), however the Metropolis version must go out before. We should also note that they released the Homestead version on 14th March 2016 (about a month before this Report was released). It will work on the smart contracts.

Finally In comparison to PoW, PoS is much cheaper to secure, transactions speed is greater and it is maybe the stepping stone for the scaling of the block-chain technology.

3.2 Proof of Activity

The protocol from Bentov, Lee, Mizrahi and Rosenfeld [3] which is implemented into PeerCoin (and its clones), is considered as an hybrid of the PoW and PoS. The nodes are doing PoW work by mining blocks and at the same time with the PoS (meaning that the block-chain includes both types of blocks).

The procedure

- The PoW miner mine.
- Block is found, the network is notified and creates a template. (multiple templates are possible)
- The block hash is used to find random owners by using its hash as numbers to determine owners (nodes from the network).
- Turn by turn each chosen owners sign the key with the key of the block.
  - If a chosen owner is unavailable, the process paused. (it's not a problem this concurrently miners are still mining and generating new templates with different owners)
- At some point in time, blocks will be signed and the reward will be given to the miner and the owners.

Continues data exchange In order to reduce the data traffic, each template does not include a transaction list during the signing process itself; it is the last owner (signer) that is adding it when creating the block.

3.2.1 Attacks on block-chains

Block-chains is designed to be controlled by the consensus of nodes. It means that it can not be owned not controlled by a third party. Until now this goal has been pretty well achieved. However, experiences showed that the system is not perfect.

The 51% attack It's the most interesting (in a social experiment point of view) and rewarding attack for the attacker. Indeed, if the attacker controls at least 51% of the consensus, it is possible to manipulate transaction by validating malicious transactions. Pools owners can do this. Note that as it is today (for actives crypto-currencies), it's not more possible to mine on your own and be profitable, miners are forced to join pools and distribute the work and rewards between them. Meaning that it creates a vicious circle, the more miners are in a pool, the more power it has. The more power it has, the more reward are generated. Finally, this results in attracting, even more, miners because they also want a bigger and easier reward for mining, which leads to the security risk of malicious pool chief who will control the currency and the transactions. All around the internet people are always saying that it's dangerous, in fact, they are asking others to stop making a profit for the good of others, which is a human self-fish reasoning. Can't wait to see this case of a figure.

Spam attacks The idea here to make a lot of transactions to the victim's wallet (by its addresses) and paralyze the legit transactions and by this way its incomes. Indeed, the network will have to process all the spam transactions as well as the legit transactions, meaning that the a delay is added before receiving the legit transactions. In some cases, like for Wikileaks[60], which is depending on this funds to live, it's pretty bad. Plus, since a lot of transactions appear in a block, its value increase and miners will jump on it to get the reward, meaning that the legit transactions are but a bit behind because generally they have a lower reward. But usually, the current crypto-currencies have an anti-spam solution. They have a minimum fee and they increase the fee after each new transactions.

DDOS on exchange platforms The profit behind this type of attacks is to either steal wallets or ask a reason to release the servers. The crypto-currency is only affected by the depreciation of its value in "real" money because are not able to trade, and they are more likely to switch to another exchange platform or currency.

Special dedication to Mining malwares It's funny to see that hacking is evolving with the hype. Now instead of having zombie computers doing nothing waiting for DDOS attacks or whatever they are used to. They are

now mining coins (generally connected to a pool). How smart is that? I personally think that it's amazing!

3.3 Consensus

Read this subsection as a teaser from the final project analysis on the consensus concept. Indeed, the time allocated for this research and analyze was null, however knowledge grows over time even if the research was trageting something else.

3.3.1 Consensus != Block-chains

The block-chains technology being very popular nowadays, it sometimes can put eye cups on our field of decisions.

Block-chains have indeed proved that it works as a consensus. However, a consensus with highly fault tolerant networks and overcome the Byzantine (Two Generals Problem) is not something that only block-chains have.

Just for taking one example, Maidsafe[43] uses another technology to obtain a consensus[49]. Instead of using the whole network to validate a transaction, they give the consensus role to a random group of nodes.

Comparing They both have pros and cons of course.

- Block-chains
  - Pros: Shared global record of all transactions.
  - Cons: The chain can be gigantic (Bitcoin more than 60GB at the moment), and the file must be synced between all network's 6000 plus. Network speed. nodes[1].
- MaidSafe
  - Pros: Bandwidth speed limitations only. Low data storage consumption.
  - Cons: Small groups of nodes are playing the role of consensus for transactions. Nodes could never be aware of transactions that happened elsewhere if they are not related to them at any point of time.

3.4 Communication

TODO

3.5 Cryptography

Privacy Being an integral part of Overclouds, a research has been made to find the best type of client-side cryptography (right from the browser as the highest priority). We were looking for a fair middle ground between performance and security.

3.5.1 From Scratch VS Libraries

1st Question Is it possible and does it exists right from the browser?

We started looking at what is done in JavaScript and we found an interesting list of *premium* libraries (maintained by prestigious organizations) such as Stanford Javascript Crypto Library[57], MDN[45], W3C[55], Google Closure[26], or msrCrypto[47].

Then we looked at other crypto libraries such as forge[14], jsHashes[37], crypto-browserify[58], etc...

2nd Question The natural question that followed was: is it worth make it ourselves?

The answer came pretty quick while navigating across numerous forums. It's a pretty bad idea if we don't have a team dedicated to it and a pretty strong community to test it out. Even big companies such as Microsoft or Google are struggling a bit on the last part.

However, for the fun of it, we looked at solutions to start a homemade cryptography library. We found two interesting potential starting points to make it work with the browser, a Symmetric Encryption sample [34], or a procedure for Digital Signatures[33].

Decision Shortly after the second question, it was pretty clear that it won't be possible to create our own cryptography library in the time given. So we decided to find the *best* library out there for our project.

3.5.2 Comparison of some JavaScript Cryptography Libraries

Based on the following tables we can notice that **sjcl**[57], **crypto browserify**[58], and **forge**[14] algorithms have been optimized for defined objectives.

talk about the tables and graphs

See Table 1 Related Figures 1, 2, 3, 4
See Table 2 Related Figures 5, 6, 7, 8
See Table 3 Related Figures 9, 10

3.5.3 A killer

After taking time doing research about the above algorithms, we came across a pretty amazing algorithm: **BLAKE2**[27, 52].

BLAKE2 outperforms MD5, SHA-1, SHA-2, and SHA-3 on recent Intel CPUs and it has **no known** security issues. Plus SHA-1, MD5, and SHA-512 are susceptible to length-extension.

It is a *new* algorithm designed specifically for **performance** and is multifaceted **BLAKE2s** (optimized for 8to32-bit) and **BLAKE2b** (optimized for 64-bit)

3.5.4 Now what

If we look at the graphic 11, BLAKE2 is dominating the two best above. **rusha** is close behind it, and forge's *sha256*. Plus we can note that the curves display a nearly completely linear performance.

Also on at the table 4 with the figure 12, we notice that BLAKE2 is in its own category.

3.5.5 What about OverClouds

We can note that we are not really interested in SHA1, because of potential security flaws. SHA256 is much better for us. However, BLACK2 is pretty amazing. We will try to make it work in the following implementation.

Now, if it doesn't work for whatever reason, we will certainly go with forge, crypto-browserify, or sjcl. The problem with forge and crypto-browserify is that we must trust a company or an individual. With sjcl however, we trust an institution.

4 Implementations

4.1 Communication

TODO

4.2 Cryptography

TODO

5 Evaluation

5.1 Tests

TODO

5.2 Results

TODO

5.3 Technologies Recommendations

TODO

6 Conclusion

TODO

7 Bibliography

References

[1] Ayeowch. GLOBAL BITCOIN NODES DISTRIBUTION.

[2] Juan Benet. IPFS-Content Addressed, Versioned, P2P File System. *arXiv preprint arXiv:1407.3561*, (Draft 3), 2014.

[3] Iddo Bentov, Charles Lee, Alex Mizrahi, and Meni Rosenfeld. Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. 42(240258):1–19, 2013.

[4] Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman. The Darknet and the Future of Content Protection. *Digital Rights Management Technological, Economic, Legal and Political Aspects*, pages 344–365, 2003.

[5] Bitmessage. Bitmessage.

[6] BitTorrent. Project Maelstrom.

[7] Vitalik Buterin. Slasher Ghost, and Other Developments in Proof of Stake, 2014.

[8] Vitalik Buterin. Understanding Serenity, Part 2: Casper, 2015.

[9] I Clarke and Et Al. A distributed decentralised information storage and retrieval system. *Undergraduate Thesis*, 1999.

[10] Ian Clarke, Oskar Sandberg, Brandon Wiley, and Tw Hong. Freenet: A distributed anonymous information storage and retrieval system. *Designing Privacy Enhancing ...*, 23:46–66, 2001.

[11] COLIN PERCIVAL. STRONGER KEY DERIVATION VIA SEQUENTIAL MEMORY-HARD FUNCTIONS. 2012.

[12] Laurie Delmer. *L'emergence au sein d'internet de communautes virtuelles et anonymes, Freenet et i2p*. PhD thesis, Universite catholique de Louvain - Departement des sciences politiques et sociales, 2009.

[13] Diaspora. Diaspora*.

[14] Inc. Digital Bazaar. forge, 2016.

[15] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. *SSYM'04 Proceedings of the 13th conference on USENIX Security Symposium*, 13:21, 2004.

[16] DR. GAVIN WOOD. ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER HOMESTEAD DRAFT. 2015.

[17] Cynthia Dwork and Moni Naor. Pricing via processing or combatting junk mail. *Advances in Cryptology—CRYPTO'92*, pages 139–147, 1993.

[18] Snowden Edward. Snowden Digital Surveillance Archive.

[19] Ethereum. Ethereum Homestead Documentation, 2016.

[20] FlowingMail. FlowingMail.

[21] Real Foodists. The Underground Internet. 2003.

[22] Freenet. Freenet project.

[23] G. Lawrence Paul Sundararaj1 D. R. Anita Sofia Liz2. Anti-Sybil Mechanism against Bogus Identities\nin Social Networks. *International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)*, 01(02):123–127, 2014.

[24] Open Garden. Open Garden.

[25] Paul Gardner-stephen. The Serval Project : Practical Wireless Ad-Hoc Mobile Telecommunications. (June):1–29, 2011.

[26] Google. Closure Library, 2015.

[27] Jian Guo, Pierre Karman, Ivica Nikolić, Lei Wang, and Shuang Wu. Analysis of BLAKE2. *Springer International Publishing Switzerland 2014*, 8366(8366):402–423, 2014.

[28] Hakshop. Rubber Ducky USB.

[29] Hype. Hyperboria Whitepaper.

[30] Hyperboria. Hyperboria.

[31] I2P. The Invisible Internet Project.

[32] IIP. Invisible IRC Project, 2003.

[33] Inc. Info Tech. Digital Signature in the Browser, 2014.

[34] Inc. Info Tech. Symmetric Encryption Sample, 2014.

[35] IPFS. The IPFS Project.

[36] Markus Jakobsson and Ari Juels. Proofs of work and bread pudding protocols (extended abstract). *Secure Information Networks*, pages 258–272, 1999.

[37] Paul Johnston. jsHashes, 2015.

[38] Sunny King and Scott Nadal. Peercoin, 2012.

[39] Sunny King and Scott Nadal. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. *Ppcoin.Org*, 2012.

[40] Leslie Lamport, Robert Shostak, and Marshall Pease. The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems*, 4(3):382–401, 1982.

[41] Litecoin. Litecoin Wiki, 2011.

[42] MaidSafe. MaidSafe.

[43] MaidSafe. MaidSafe.net announces project SAFE to the community, 2014.

[44] Max K., Patrick Lodder, and Ross Nicoll. Dogecoin Core, 2013.

[45] MDN. MDN Web API Crypto, 2015.

[46] MediaGoblin. MediaGoblin.

[47] Microsoft. MSR JavaScript Cryptography Library, 2015.

[48] Movim. Movim.

[49] Lambert Nick. CONSENSUS WITHOUT A BLOCKCHAIN, 2015.

[50] Nitrokey. Nitokey.

[51] Retroshare. Retroshare.

[52] Ed. Saarinen, M-J. and Jean Philippe Aumasson. The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC), 2015.

[53] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.

[54] Serval. Serval Project.

[55] Ryan Sleevi and Mark Watson. Web Cryptography API, 2014.

[56] Yonatan Sompolinsky and a Zohar. Accelerating Bitcoin's Transaction Processing. Fast Money Grows on Trees, Not Chains. *Eprint.Iacr.Org*, pages 1–31, 2014.

[57] Emily Stark, Michael Hamburg, and Dan Boneh. Symmetric Cryptography in Javascript, 2012.

[58] Dominic Tarr. Crypto-Browserify, 2013.

[59] Dominic Tarr. Performance of Hashing in Javascript Crypto Libraries., 2014.

[60] TheBitcoinNews. Bitcoin Spam Attacks, 2015.

[61] Tor. Tor.

[62] Vitalik Buterin. A Next-Generation Smart Contract and Decentralized Application Platform. 2013.

[63] Jonathan Warren. Bitmessage: A Peer-to-Peer Message Authentication and Delivery System. page 5, 2012.

[64] Chris Webber. GNU MediaGoblin Documentation. 2016.

[65] Dai Wei. B-Money, 1998.

[66] ZeroNet. ZeroNet.

[67] Zeronet. ZeroNet, 2016.

8 Annexes

8.1 JS Cryptography Library Graphs

Add other crypto libraries using **Dominic Tarr**'s benchmark set [59].

The graphs from the following figures have been made by **Dominic Tarr** [59]

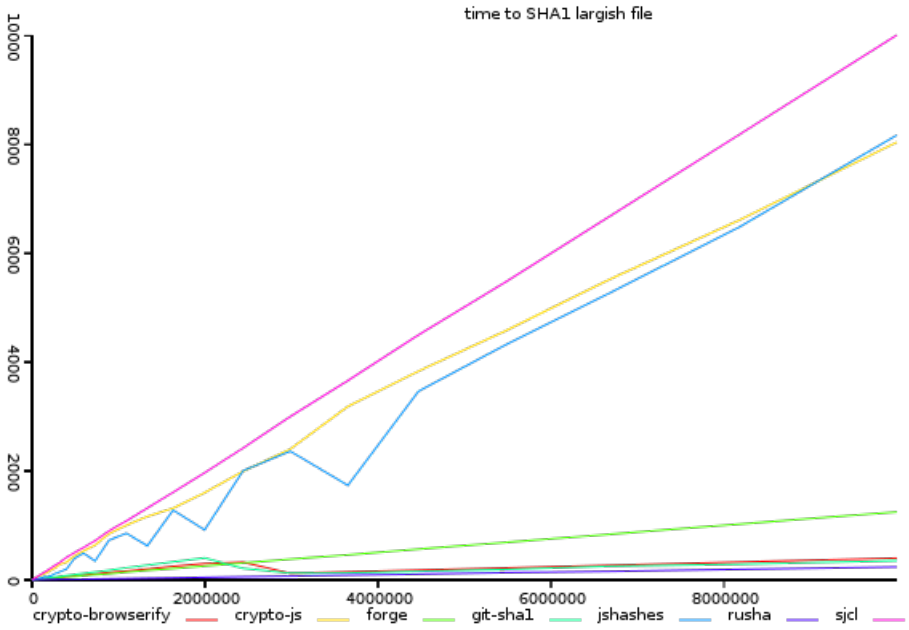

Figure 1: *y-axis shows total time taken, lower is better*

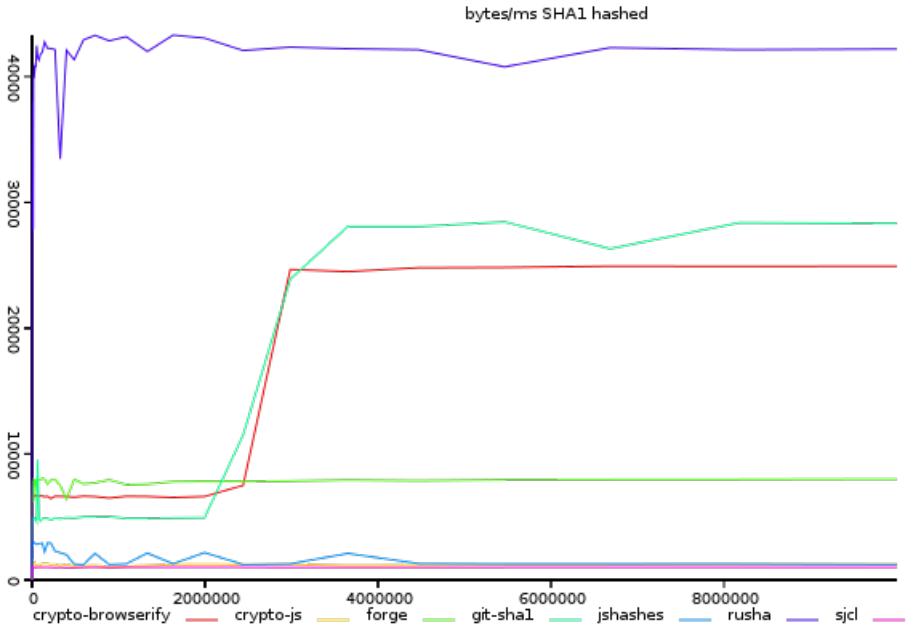

Figure 2: *y-axis shows size/time, higher is better*

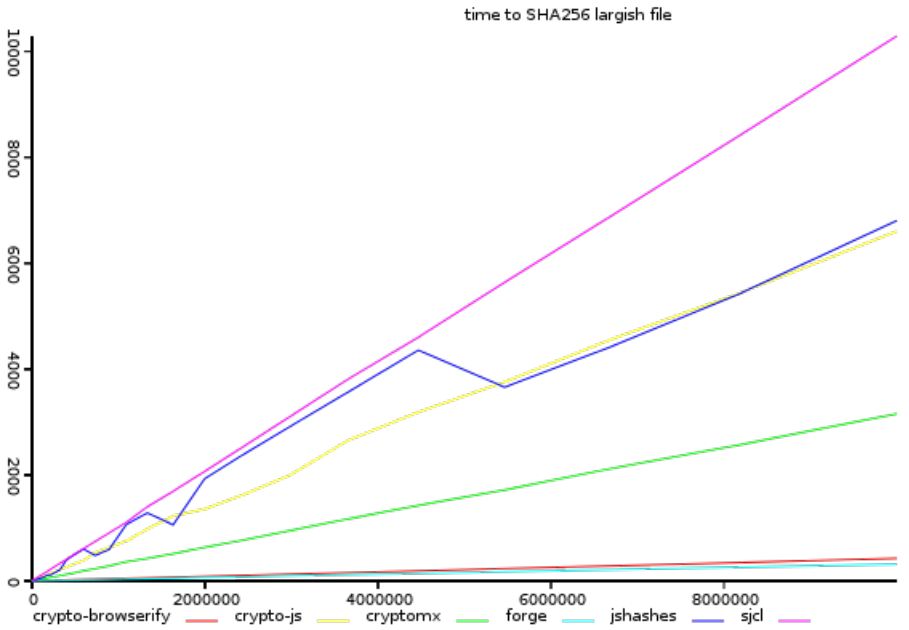

Figure 3: *y-axis shows total time taken, lower is better*

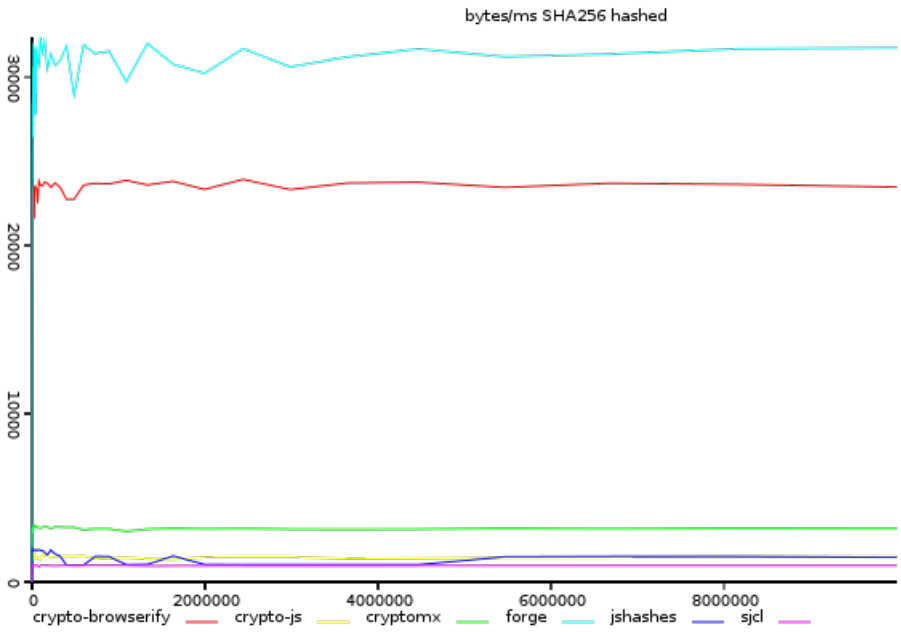

Figure 4: *y-axis shows size/time, higher is better*

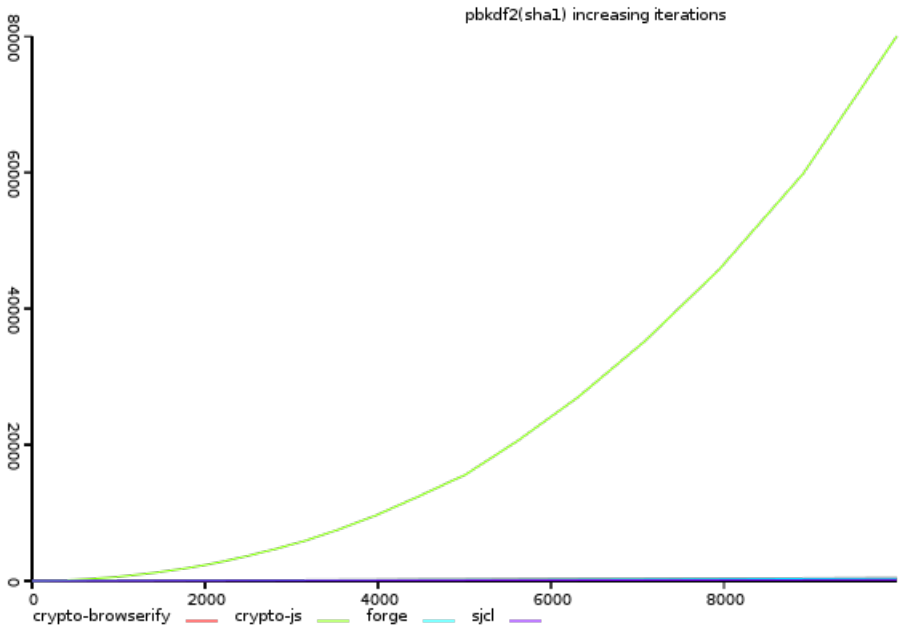

Figure 5: *y-axis shows total time taken, lower is better*

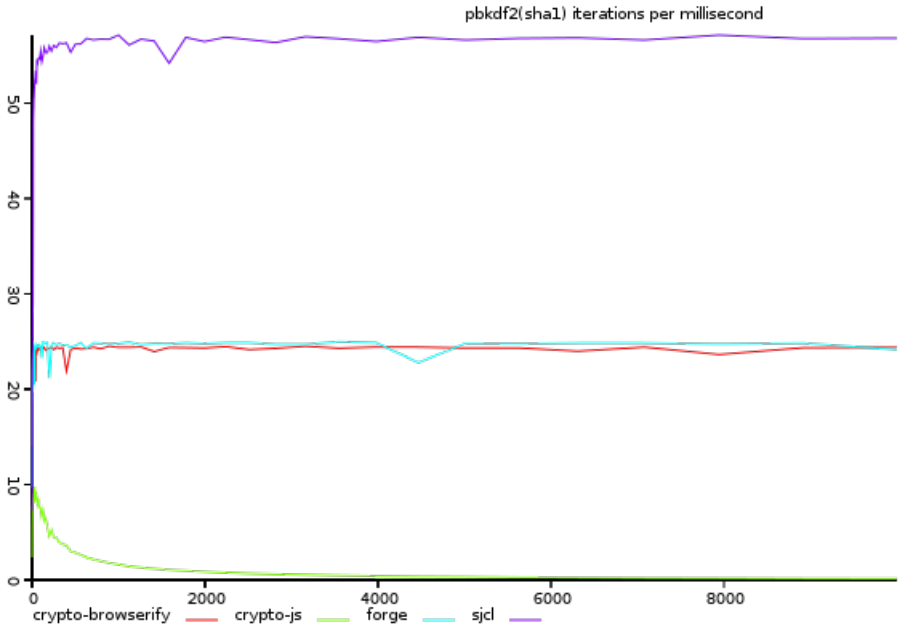

Figure 6: *y-axis shows size/time, higher is better*

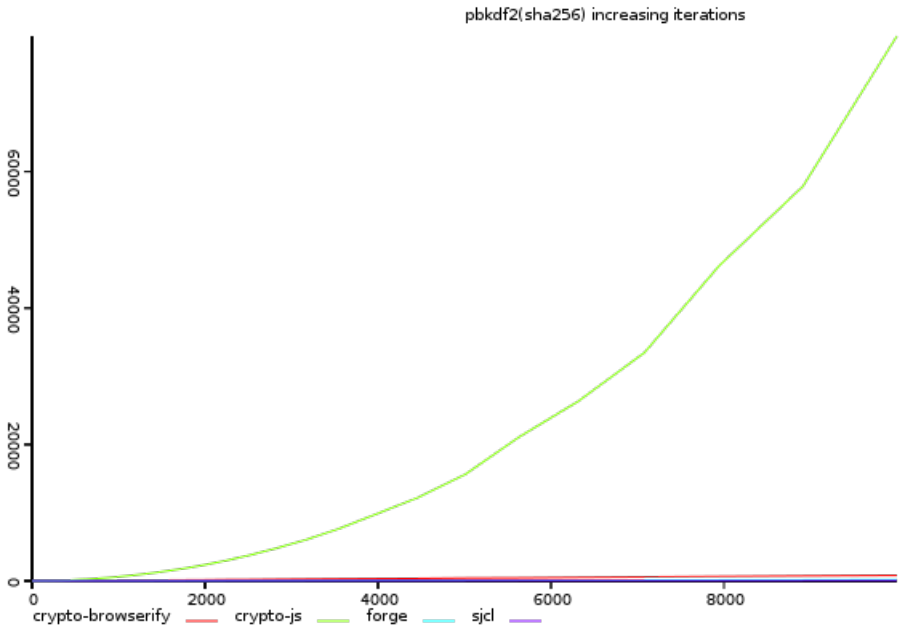

Figure 7: *y-axis shows total time taken, lower is better*

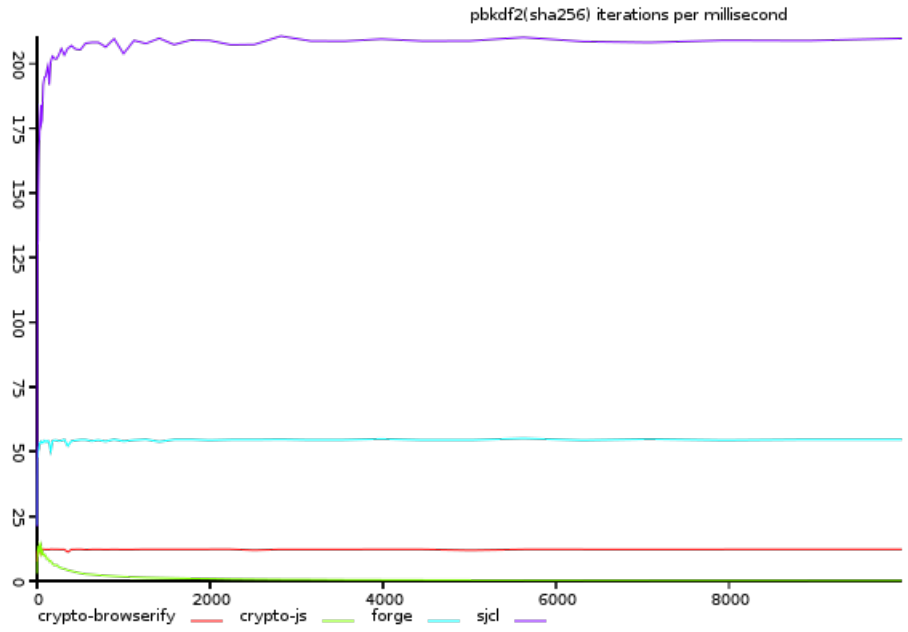

Figure 8: *y-axis shows size/time, higher is better*

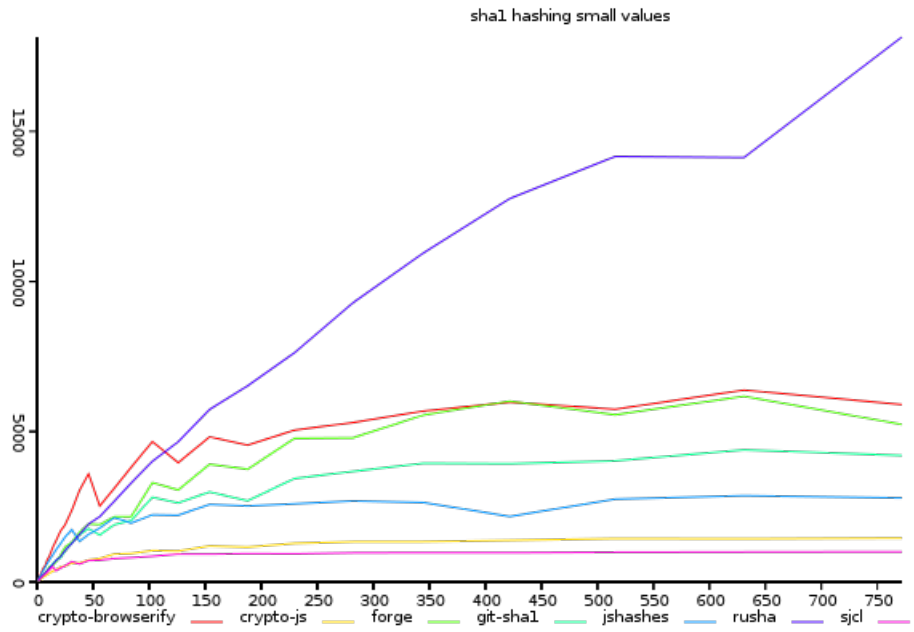

Figure 9: *y-axis shows size/time, higher is better*

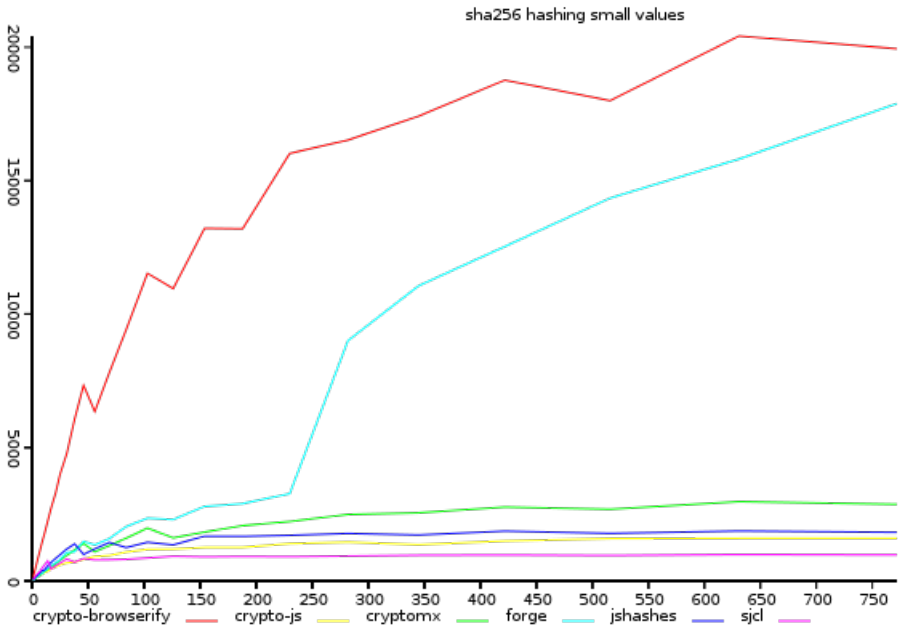

Figure 10: *y-axis shows size/time, higher is better*

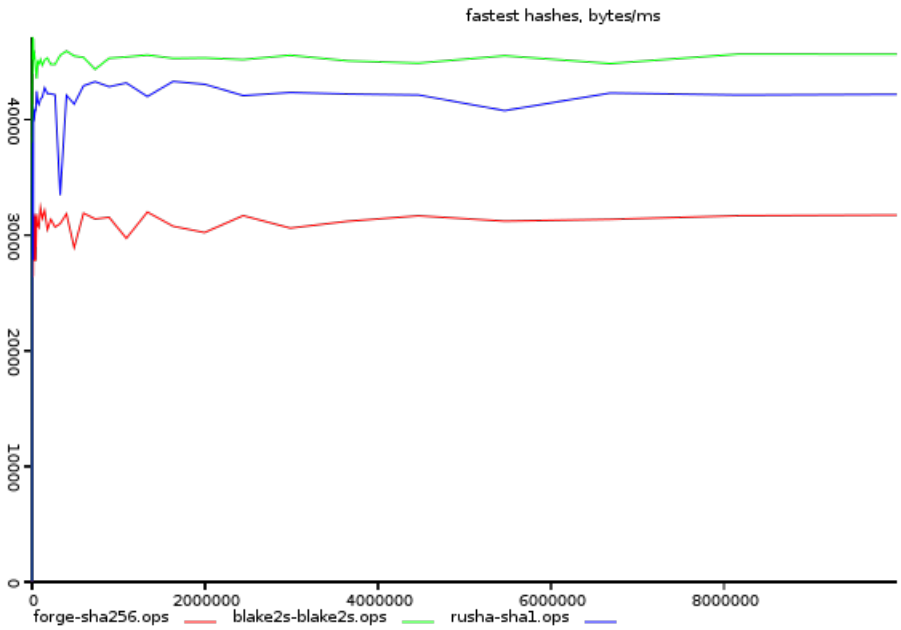

Figure 11: *y-axis size/time, higher is better*

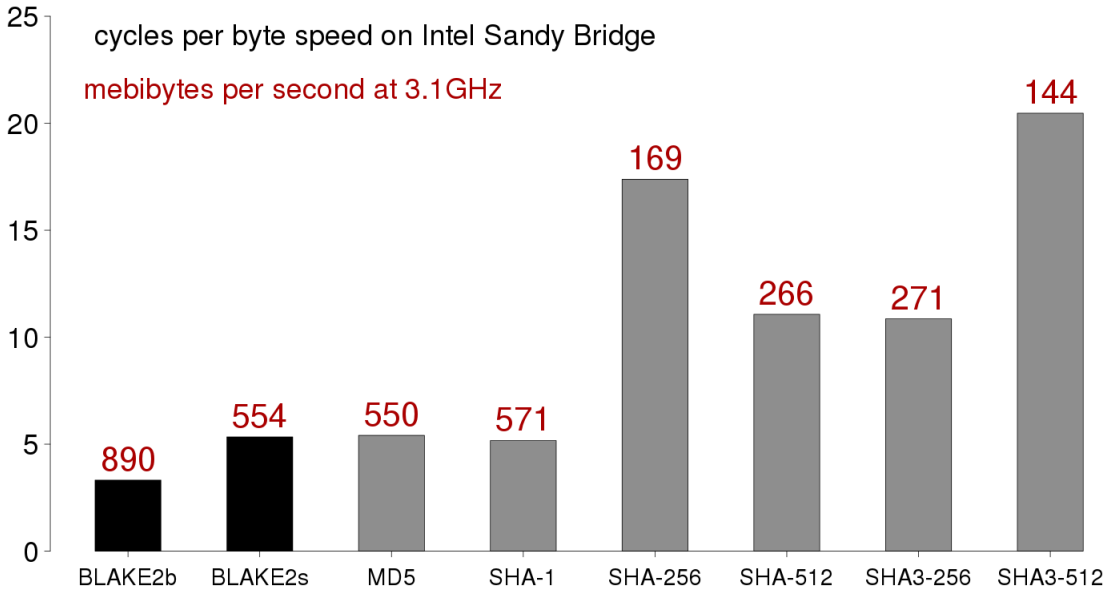

Figure 12: *lower is better*

8.2 JS Cryptography Library Tables

Add other crypto libraries using **Dominic Tarr**'s benchmark set [59].

The following tables have been made based on **Dominic Tarr**'s[59] benchmarks.

Table 1: Hashing 0-10MB Files /milliseconds based on [59]

Libraries	Sha1 (size)	Sha1 (hash)	Sha256 (size)	Sha256 (hash)
sjcl	- - - -	- - - -	- - - -	- - - -
crypto-js	- - -	- -	-	- - -
forge	+	+	+ + + +	+ + + +
crypto-browserify	+ +	+ +	+ + +	+ + +
crypto-mx	null	null	+	- -
git-sha1	+ + +	+ + +	null	null
jshashes	-	-	- -	- - -
rusha	+ + + +	+ + + +	null	null

Table 2: Key Derivation (pbkdf2) based on [59]

Libraries	Sha1 (time)	Sha1 (size)	Sha256 (time)	Sha256 (size)
sjcl	+ + + +	+ + + +	+ + + +	+ + + +
crypto-js	- - - -	- - - -	- - - -	- - - -
forge	+ + + +	+ +	+ + + +	+
crypto-browserify	+ + + +	+ +	+ + +	- -

Table 3: Hashing Small Files /milliseconds based on [59]

Libraries	Sha1 (size)	Sha256 (size)
sjcl	- - -	- - -
crypto-js	- -	- -
forge	+ +	+ + +
crypto-browserify	+ + +	+ + + +
crypto-mx	null	+
git-sha1	+	null
jshashes	-	-
rusha	+ + + +	null

Table 4: Fastest Hashes /milliseconds based on [59]

Libraries	Sha1 (size)	Sha256 (size)	blake2s (size)
rusha	+ + + +	null	null
forge	null	+ + + +	null
blake2s	null	null	+ + + +