Team 16: Biweekly Report 3 – Friday December 2nd Blockchain – Atos

Written by: Sadir Abdul Hadi, Kristelle Feghali, Alexandru Chiriac

Overview

This past week was very useful for the progression of our project, we did some experiments with bitcoins, ethereum and digital signatures. However, we encountered many problems while experimenting and not everything we tried succeeded. We feel we are making progress even though we are still researching other technologies. Our goal for the moment is to choose between ethereum and bitcoin, and that's why we will continue our experiments with both for the moment. We mostly tried experimenting with digital signatures, ethereum, and "uploading" hash references to the bitcoin blockchain. We've also worked on improving our website's content, by modifying its structure and adding more information to it.

Meetings

Meeting #1 - Monday, November 21st 2016 // Meeting with our supervisor
Attendees: Antoaneta Serguieva, Sadir, Kristelle, Alex

We talked with Antoaneta about our progress and future deadlines.
We particularly discussed our idea, the Notary Public, which our supervisor felt is very useful.
Finally, our next meeting will be on Monday 5th or 12th of December, as she might be away.

Meeting #2 - Monday, November 21st 2016 // Group meeting - Agreed on the weekly sprint
Attendees: Sadir, Kristelle, Alex

This meeting had the purpose of splitting our workload. Kristelle has been assigned with working on the website, learning how to get a reference to a document with a hash function, somehow "uploading" that reference on the blockchain and verifying its existence. Alex was tasked with helping with the design aspect of the website, learning how to digitally sign a document, uploading it to the blockchain and eventually getting the document signed several times. Sadir had the mission to organize the content of the website, find out about timestamping a document, research the different ways to "upload" a document to the blockchain and also get the signatures time stamped.

Meeting #3 - Wednesday, November 23rd 2016 // Meeting the client
Attendees : Sadir, Kristelle, Alex

During this meeting, we've finally chosen the name of our idea: Blockdocs. Furthermore, we noticed that the majority of Proof of Existence applications, which constitutes a part of our idea, use bitcoins. Hence, we started researching the technical part of it and succeeded in creating a Testnet using Block.io.

Furthermore, we succeeded in creating a hash of a document using python. The code uses the hashlib library and the md5 algorithm to create a digest of a document. The next step was to upload this digest to the blockchain.

Meeting #4 - Thursday, November 24th 2016 // Lab session
Attendees : Sadir, Kristelle, Alex
This meeting proved to be very productive as we succeeded getting test Bitcoins and making transactions using them. We have also successfully used some of the features of Block.io's API which is one of the many bitcoin wallets. Our TA also asked us to build a use case for our app so we quickly sketched one to get a better understanding of what our app would be used for. After learning the basics of using bitcoins, we started considering Ethereum as an alternative as our TA suggested. During the final minutes of this meeting we split roles such that we could make an approach towards understanding Ethereum.

Meeting #5 - Monday, November 28th 2016 // Group meeting - Agreed on the weekly sprint
Attendees: Sadir, Kristelle, Alex
This meeting also had the purpose of organizing our workload and sharing knowledge that we've gathered during the previous week so that we could help each other on various tasks if possible. This meeting raised a couple of questions: What happens if there is a collision between hash functions uploaded on the blockchain? Can this even be possible? What if the hash address already exists on the blockchain? We decided to look out for information and answers towards these questions.

Meeting #6 - Tuesday, November 29th 2016 // Group meeting
Attendees: Sadir, Kristelle, Alex
During this meeting we talked about the tasks we have to do and updated each other with what we did individually. We worked on uploading a digest to the bitcoin blockchain using OP_RETURN, which did not succeed. Furthermore, we experimented with signing a pdf document using java libraries however this proved unsuccessful and further research needs to be done.

Meeting #7 - Thursday, December 1st 2016 // Lab session
Attendees: Sadir, Kristelle, Alex
We managed to get feedback on the website from our TA after which we decided on the final touches and things that need to be added/removed from the website. Also the feedback proved very helpful and we found out that we need to rethink bits of content and maybe merge 2 sections into one while clearing irrelevant general information from the About page. We also experimented a bit with the Ethereum wallet and did some mining on the test network.

Tasks Completed

- Create a hash of a document (Python, md5 algorithm)
- We're are now confident about dealing with Bitcoin technically (Testnet, transactions…)
- After some technical problems, we succeeded in creating a Truffle project for Ethereum.
- We've continued our research, and particularly focused on the different phases of the Use Case.
- We updated the website to prepare for the submission.
- We applied to the Atos IT competition

Problems

- Digitally signing a document proved unsuccessful and requires further experiments
- OP_RETURN is still under debate, and its use is controversial
- We're still indecisive between 2 technologies, Bitcoin and Ethereum

Plan for the next 2 weeks

- Continue experimenting with the 2 alternatives : Bitcoin and Ethereum
- Choose the best technology between these two
- Draw a final architecture of the back-end of our system

Individual Section

Sadir Abdul Hadi:

During the past 2 weeks, I've finally dived into the technical aspect of our project. During the first week, I've mainly researched and experimented the bitcoin technology. Hence, I was able to make transactions on the bitcoin testnet using block.io. Now, it's time to see how to inject transactions with data we want (the data being the hash Kristelle talked about). One of the proposed solutions is using OP_RETURNs, but their usage is still under debate, as they "contaminate" the blockchain with unwanted data, and I would need to research this next week, while working with Kristelle on experimenting OP_RETURNs.

In fact, many technologies similar to ours use OP_RETURNs to accomplish tasks such as "uploading" a hash of a document to the blockchain in order to later prove its existence. We need to research twisting these technologies for our purpose.

During the second week, however, and after attending a talk by ethereum co-founder Dr.Gavin Wood, my curiosity has driven me to research and experiment ethereum, using Truffle. After some technical difficulties, I've now finally created a starter project. During the second week, I also created our logo and filled the application for the Atos Competition.

Kristelle Feghali:

This week I worked on creating a hash of a document in order to upload it to the blockchain. The first part was a success, I completed the task by using Python and the md5 algorithm included in the hashlib library. However, the second part is still a work in progress since I encountered some difficulties completing transaction due to permission errors. It is also not possible to send bitcoins to a hash since it is not a valid address. A solution we found is using OP_RETURN, which I will work on during the following week. Moreover, I was in charge of the website, which I worked on during the past week: content, presentation, structure etc. My plan for the next week is to research a way to upload a hash of a document to the blockchain.

Alexandru Chiriac:

I have focused on trying to digitally sign a document and research ethereum during the past weeks, while giving a few insights and helping out with our website. Digitally signing a pdf document proved quite a challenge as there aren't many solutions out there that are easy to understand. All the forum posts I have read said that it is a difficult thing to achieve but it can be done. In depth knowledge of java and apache libraries is required to create such a program and I am still in the process of accumulating information and experimenting with the libraries. I've been tasked with researching if ethereum would be useful for our project and it proved to be quite interesting. I worked through a few tutorials about using the ethereum wallet and I have mined ether for a couple of hours, although I did not manage to get any rewards out of it, either because my laptop was too slow or because an error might have happened. As of yet, I have only mined on the test network but I am trying to find out how to mine on the real network using software that the tutorials have recommended. I have encountered a few technical difficulties with installing the software and prerequisites but I managed to find out the issue and my goal for the following week is to use my machine to mine on the real network.