Team 16: Biweekly Report 3 – Friday November 18th
Blockchain – Atos

Written by Kristelle Feghali, Sadir Abdul Hadi and Alexandru Chiriac

Overview

We believe we've done some important progress these last two weeks, and that we're finally on the right track. We decided on what we wish to work on, we did a lot of research and made a list of tasks and steps we will follow during the weeks left before the end of the term. We also discussed our idea with our client, which helped us get a clearer view about what we need to get done. In addition, the team decided to enter the Atos' Blockchain competition as long as it does not interfere with the requirements of the university course.

Meetings

Meeting #1 - November 9th 2016 // Skype meeting
Attendees: Sadir, Kristelle, Alex
During this meeting we discussed three different ideas: an application to vote electronically, an application to verify the authenticity of documents, and a platform for artists to sell their art. We decided to go with the second idea: authenticating documents via a potential web app. We felt it was more interesting and more accessible for us to build given our knowledge. We also shared our research on each of the topics in order to update each other and move forward with researching the idea we decided to work on. We decided to research our topic individually, in order to share our ideas after reading week.

Meeting #2 - November 14th 2016 // Group meeting
Attendees: Sadir, Kristelle, Alex
After having shared our individual research, we decided on the next "sprint" we are going to undertake: researching the most relevant available resources, before thinking of a way to combine them. Actually, our project consists of many parts: a Blockchain ledger at the middle, with parties accessing it from web platforms, checking or modifying its content. The crucial part is obviously the Blockchain, which we need to look up more technically, in the context

Meeting #3 - November 15th 2016 // Meeting the client
Attendees: Andy Wallace, Sadir, Kristelle
In this meeting we thought again about the usefulness of the idea with our client, and the outcome was very positive. It allows international students, for example, the possibility to send documents from their university to the desired administration in their country without having to pass through a notary public, the Foreign and Commonwealth office, as well as their respective embassy. Actually, all this chain used to exist because there was no direct way to know this paper was issued from the university, but this is going to change in the near future. We talked to Andy about our research and expressed our concerns regarding certain details of the ideas, which was very helpful since we actually brainstormed together. Even though we did not find answers to all

our questions we decided to start experimenting with APIs and learn to use the libraries we found that could help us create the app.

Meeting #4 - November 17th 2016 // Lab session
Attendees: Sadir, Alex

During this meeting we researched some resources available online, including:

- Stampd: Uploads a hash of the documents to Blockchain. Hence, a user can prove the existence of a document at a certain point of time. (Many other such tools exist)
- Stampery: A tool used for proof of ownership, proof of integrity, proof of existence and proof of receipt.
- Blocksign: It's actually a partially similar concept to what we're building. It's not specialised for notary public, wasn't functional when we experimented it, and doesn't provide an API

We also discussed our evolution with Yun Fu and our TA, who were satisfied of what we've done up until now.

MoSCoW Requirements - Summary

Must have

- A tool to register and verify the authenticity of a document on Blockchain

Should have

- A web app than can be accessed by official parties (who provide the documents), and customers

Could have

- Ability to authenticate documents from multiple parties.

Would have

- A very secure way to access the web app, which effectively verifies the identity of the user

Tasks Completed

- Researched the 3 main ideas we had from the previous meetings
- Decided on a final project idea to work on: virtual notary public
- Started experimenting/technical research
- Met with our client to elaborate on our progress

Problems

- Main technology is new and some elements are difficult to comprehend
- Not enough knowledge on programming languages that some of the APIs are written in, for some team members.

Plan for the next 2 weeks

- Learn how to use the available resources, with 3 particular points split between use: Saving/retrieving the documents on/from the blockchain, timestamping them and signing them.
- Start experimenting with the APIs
- Learn more about digital signature
- Answer the following questions:

1. How do miners check the validity of a document (digital signature)?
2. How to prove to the receiver that the document was on the blockchain (token)?
3. How to check the validity of the signature? The authenticity of the signer?

Individual Section

Kristelle Feghali:

During the past two week I did some research on using blockchain for elections. I encountered two major problems. The first one is the obvious one: how does a person vote? I thought a possible way to do that would be to create a wallet for each of the candidate and assign one bitcoin to each voter. However, this is generates a lot of other problems: how do we make sure everyone just voted once (someone could send many bitcoins each at a time), how do we make sure the candidate is not cheating, and the list goes on. The other problem was to find a way to identify the voters to make sure they are allowed to vote in this particular election. Thus, we came to the conclusion that it is best to focus our energy on another idea.
The team decided to work on authenticating documents and we all focused our research on this matter. I found some interesting libraries and APIs we could use. I am planning on experimenting with them during the next two weeks.

Sadir Abdul Hadi:

The topic I researched during reading week is the one we ended up choosing: authenticating documents via Blockchain. Hence, I researched the available resources and found various tools we can use.
The use of blockchain in this situation seems suitable. We want an element (the document) to be trusted, without passing through a central authority (the notary public).
The tools that already exist mainly deal with proving the existence of a document at a certain point of time. Hence, theoretically, adding a verified signature/stamp to this document is enough to make it verified. The issue is, obviously, not as simple as it appears. Hence, researching and experimenting the possible implementations is what I'm going to focus on. I tried to use the Stampery API during the end of the week, but still didn't manage to make it work correctly.
During next week, I am going to continue experimenting with Stampery, and to focus on the technique of saving files on the blockchain using a hash function.

Alexandru Chiriac:

From a start, I have not been able to find anything relevant that would detail more on the 'fairtrade through blockchain' subject, however, I have found some articles that hint towards the idea. One was speculating blockchain might prove useful for fair-trade, but I couldn't find anything too relevant regarding how the solution would be implemented, so this was a major problem. Another interesting article focuses on a similar idea, but this time it involved artists selling music directly to the fans (consumers). After one of the meetings with my team, we decided to drop this idea because we were lacking sufficient insight and focus on the 'e notary public' idea. I started researching competitors and tried to understand the various mechanisms they were built upon. The two main sites that have a functionality similar to our idea are stampd.io and stampery.com. For the following weeks I plan on researching the implementation of the digital signature on blockchain.