# Decentralized Applications

## By Amel Sellami

### July 16, 2018

**Abstract**

This paper shows how can the Blockchain be the future industry and how with it we can create a competitive application for the market to compete with big companies. We will first introduce the technology used which is Blockchain and then we will give an example of a social decentralized network project.

## 1 Introduction

The emerging field of Decentralized Application is one of a kind which could be marinated in different fields such as Artificial intelligence, games, music and even social networks. This technology uses Blockchain as its pillow of construction. Within this paper, we will first answer three major questions which are what, why and how. Then we will dive a little bit more using a technical example project a social network on the blockchain. This work is based on this tutorial for the Siraj raval course in Schoolofai.

## 2 Motivation

The world these days becomes more and more towards monopoly where only a few own the data and use them towards there benefit. That's why we find it important to change this pattern by using a new business model that gives the chance to everyone to be part of this journey. We use for this the Blockchain technology which is the backbone of the decentralized applications and thus the new business model. Our motivation with this is that we can prove we can build a decentralized social Network that can in the future compete with big companies like Facebook and Linkedin.

## 3 Decentralized Applications

### 3.1 Introduction

It's been hailed as a global revolution, and shunned as a piece of technology. But in reality, Blockchain is a fascinating piece of technology that has the power to change our world. Blockchain is as a ledger that lives on every device on which it is installed. Whenever the ledger is changed, the information is updated on each device. This networked method of tracking information has supported the rise of decentralized currencies like Bitcoin and Ethereum. [Ole]

### 3.2 Web 3.0

Web 3.0, a phrase coined by John Markoff of the New York Times in 2006, refers to a supposed third generation of Internet-based services that collectively comprise what might be called 'the intelligent Web'. For web3.0 to exist there must be a web 1.0 which is the birth of the Internet and web2.0, which is the creation of services and more likely the 'web'. So, why do we need web3.0? Actually, there are different reasons, the most important one I guess is that we can compete with big companies with Blockchain likewise Facebook, Amazon and so on. The second important reason is the data permanence it is a term that means when the data stays in the same place for a long time without removal. In the next section, we will understand more the what and the how.

## 3.3 The Blockchain

The Blockchain is an ingenious invention. The brain behind it is the pseudonym, Satoshi Nakamoto. To keep it simple the information in backbone Blockchain is distributed upon computers and not linked to a central server. AS Don and Alex Tapscott, authors Blockchain Revolution (2016) said 'The Blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.'[Blo]

The Blockchain is a Decentralized Network, as shown in the picture 1,from. A decentralized network is a network that is not controlled by any entity. Whereas a centralized network is a network that relies on a single server and a distributed network that is like a centralized network but does not only rely on a single server but multiple ones. With Blockchain, many people can write entries into a record of information and a community of users can control how the record of information is amended and updated.



Figure 1: Decentralized, Centralized and distributed Network.

The next section will answer the question How can we start building the Blockchain ?

## 3.4 Constitution of Blockchain

The Blockchain is mainly constituted of a data linked list where the values are immutable means that no one can change it. The nodes in the Blockchain are called blocks inside of them we store data in form of transactions stored in computers. For someone to change the values in the Blockchain they need to have more computing power than the majority of the network which actually no one has. This technique is called the proof of work [AP] uses proof-of-work protocol to reach consensus, which requires a node to try and solve a hard computational problem in order to validate a batch of transactions and add them as a new block to the Blockchain.

The architecture components are transactions, blocks, mining, and consensus.

## 3.5 Transactions

They are the smallest building blocks of a Blockchain system, consisted of recipient address, a sender address, and a value. A transaction changes the state of the agreed-correct Blockchain and is bundled and delivered to each node in the form of a block.

## 3.6 Blocks

Blocks are data structures whose purpose is to bundle sets of transactions and be distributed to all nodes in the network. Blocks are created by miners.

## 3.7 Mining

To put it simply, mining is the process of putting in real-world work, in the form of electricity, to create a valid block that will be accepted by the rest of the network.

## 3.8 Consensus

The concept of independent nodes checking and verifying the validity of transactions and blocks is called consensus. The consensus of a Blockchain is realized in a codified set of rules that everyone is playing by. As the network grows larger meaning that there are more miners and nodes participating in the consensus, which thus grow stronger but also, creates one of the issues in Blockchain: the scalability.

## 3.9 Smart contracts

There is also another interesting thing besides storing transactions we can store code inside the Blockchain using a specific type of code 'smart contracts' written in a language named solidity. Contracts have four parts: the address, balance, code, and state. This is used in Ethereum. With this, we can create incredible applications from decentralized messengers or games with decentralized Social networks and even to decentralized search engines. The next picture 2 shows the mechanism.
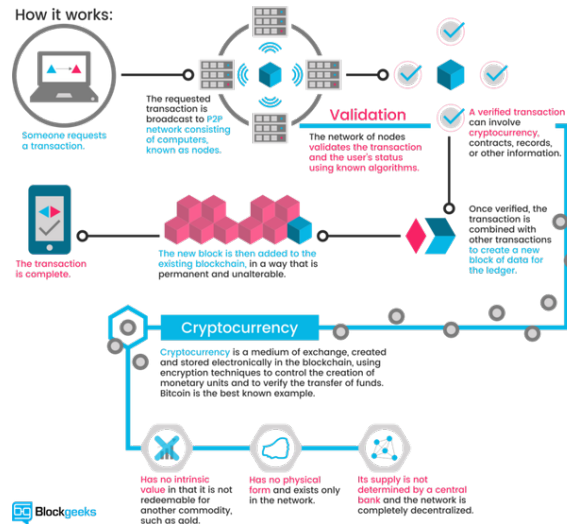


Figure 2: Blockchain Architecture .

First someone requests a transaction, then broadcast it to a P2P Network, afterward comes the validation step and once verified the transaction is added to other transactions.

After this quick introduction of Blockchain, it's important to give a model that can be somehow to future trend for Social Networks where no one can own your private data and manipulate it for that We will try to create a decentralized social network like LinkedIn.

# 4 Decentralized Social Network Project

## 4.1 Introduction

It has been a hard year for the giant of Social media world wide 'Facebook'. Apart from the scandal involving Cambridge Analytica and the fake news trope, there have been also countless lower-profile incidents that reflect badly on the image of the company.

Facebook simply has too much control over the data of its users, which, unfortunately gives it too much power to dictate terms. The decentralized infrastructure of Blockchain based social media creates a more equitable balance of power between the platform provider and its users where both parties can be satisfied. An additional problem with the Facebook system is a problem related to all centralized data stores: they're easy targets for those who wish to misuse the data. Harvesting or even misappropriating the data is far more a hard work without a central point ie in a decentralized Network.

Which lead us to develop a project that can compete with their model and have the advantage of storing the data in a place that first no can own and second no one can change.

## 4.2 Development Tools

A Smart Contract is the code that helps us communicate with the Blockchain to store data and use it. We first need Metmask which actually is a bridge that allows you to visit the distributed web of tomorrow in your browser today. It allows you to run Ethereum Decentralized Application 'dApps' right in your browser without running a full Ethereum node. We will use the Ropsten Test Net 3 ,from where the ether 'ethereum' monetary has no value. We will also use the Remix which
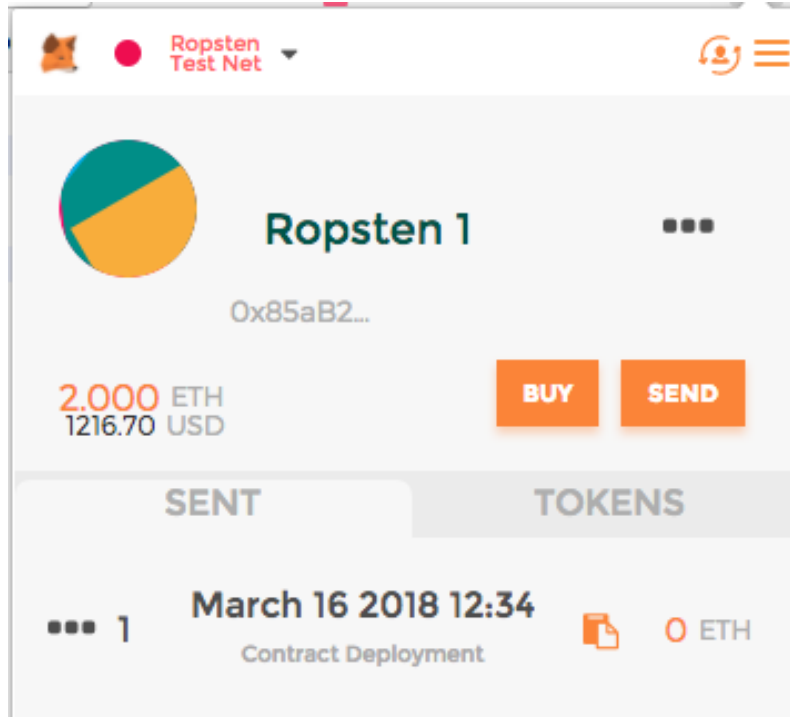
Figure 3:   .

is actually a Decentralized Application where we can develop smart contracts and can deploy them on the Blockchain and interact with them. The picture below 4

To deploy the project we need also to request virtual faucet from this site 'https://faucet.metamask.io/'.

We use also the contract ABI and the contract address that can be extracted from the remix.org after deploying the smart contracts in the Ropsten Test Net within the project.

## 4.3   Development of the smart contract

The logic in this is the fellow: We first need to initialize the variables. We create a smart contract named Linked where we create a user. The user variables are the name, the occupation, and the bio. To interact with each other they need messages. To write a message, stored in the database with variables its content, the writer and the time stamp of the message. Each time an action takes place the accounts and messages are stored in the database. There is also the part where people follow and neglect a person. To sum up, we have users who send each other messages for people they follow and neglect those who don't want to accept. That's mostly the philosophy behind the smart contract development.

Now we have a contract that can be used afterward in the development of the decentralized application.

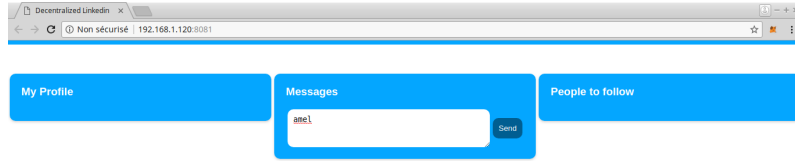In the end this is how the project will look like in the picture 4

Figure 4:  The Final project.

## 4.4    Architecture and Development

The next picture 5 Will demonstrate a simplified architecture of the Project.  As we can notice
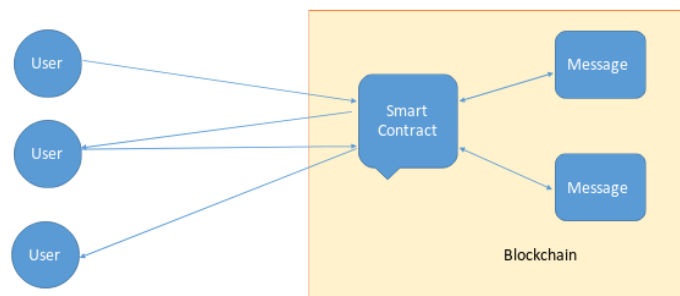


Figure 5:  The Simplified Architecture.

that the message and the smart contract reside in the Blockchain which actually is no more than computers stacked together in the virtual cloud likewise the Torrent Architecture. The interaction between the different users is done by the smart contract, when someone wants to send a message to a follower, the smart contract creates a new message and send it towards the targeted user.

We first need the metmask to test the smart contract developed in the Ropsten test net. Then develop the part where The accounts and messages are stored on a database, each time an action is taken and The server saves on the database who you're following in ethereum, the server side-like code. Morover, we need to connect the smart contracts to the web application. web3.js. is for the use of decentralized Smart Contract on your web application.

To put it in a simple way A decentralized application is just a web application where the server database logic is stored on the Blockchain. To get the information from Blockchain, we need first to get the current user address then if the function is getting its data correctly from the smart contract the variables values can be accessed.

## 5    Conclusion

Within this report, we have introduced generally The Blockchain technology, its importance in the future and how we can create a revolutionary business model network that can solve the today problems as of the data ownership and censorship. We have developed a basic Social Media Network using solidity and other languages that are not cited here because they are not relevant to our work. The Blockchain could be the answer to many questions but what if it can be combined

with Artificial Intelligence this could lead to great inventions.

# References

[AP]  Parth Shah Vinit Adkar Amitai Porat, Avneesh Pratap. Blockchain Consensus: An analysis of proof-of-work and its applications. pages 2–6.

[Blo]  BlockGeek. What is blockchain technology? a step-by-step guide for beginners, month = july, year = 2018, url = https://blockgeeks.com/guides/what-is-blockchain-technology/.

[Ole]  Steve Olenski. What the blockchain revolution means for cmos.