From the initialization of the network to the execution of a smart contract and the selection of the necessary tools, here are the main steps for implementing a block chain application.

The block chain has passed the course of evangelization. It is no longer necessary to recall the interest represented by block chain technology. A kind of decentralized account ledger (and therefore very difficult to falsify), it allows validating transactions in near real-time without going through a trusted third party. The use cases are endless and many companies have moved from PoC (proof of concept) to concrete achievements.

The underlying technologies are available in open source, any aspiring developer can implement a small private blockchain on his workstation and run it on a network of a few machines. The opportunity to learn through practice the concepts behind such an environment, such as mining or the execution of a “smart contract”. The point on the major stages of such a project.

1. Select your platform

The Ethereum block chain network is unanimous. Due to the dynamism and responsiveness of its community but also the wealth of its documentation, the promise of the blockchain is that the objects will become fully autonomous and belong to themselves. They will be able to execute code: in exchange for money (a form of code), the door releases its access (via code) to be used during the authorized time.

Ethereum’s development environment is based on the most common languages such as C ++ (Cpp-ethereum), Haskell (ethereumH), JavaScript (EthereumJS-lib) or Python (Pyethapp). The one based on the language Go will be retained (Go-ethereum or Geth). It is the most used customer in the Ethereum world. By default, it connects to Homestead, the main network of the platform. The first step is to install Geth on his workstation (it exists for Linux, iOS, Android, macOS, and Windows).

2. Initialize the blockchain

To initialize the blockchain, simply create the first block manually. This block must contain all the characteristics of the chain. They will then be shared at all the nodes (or endings) of the network. To define this block, you have to create a file in JSON format. Several parameters must be specified: “nonce” (usually the cryptographic hash generates a random value), “timestamp” (validation time between two successive blocks), etc. Once this JSON file is filled in, it is up to the client Geth to create the folder containing the blockchain (chaindata) and to initialize it.

To ensure the propagation of the program, it will be necessary to have cryptocurrency

The goal is to replicate commands as many times as your network has nodes, the latter being set in agreement with the very first. So that they communicate within the blockchain, it is necessary for the second time to connect them to each other. In order forGeth to connect to a node in the network and coordinate the set, he must retrieve his identifier called enode on Ethereum.

To ensure the propagation of the node-to-node program on Ethereum, it will be necessary to have cryptocurrency in Gas to acquire the necessary computing power from the actors of the network.

3. Choosing the right consensus protocol

The protocol consists of asking the resolution of a mathematical problem requiring a large amount of calculation. When one of the miners manages to find the solution, it must be easily verifiable by all. The first to find the solution wins the right to write the next block. The difficulty of the problem is adjusted in real time according to the total power of the network. The blocks are thus written at regular intervals. This system makes hacking attempts difficult (becoming the first computing power is extremely expensive) and protects against spam attempts to overload the network. Since the identification of the minor-pirate is easy, falsifying the blockchain (by gathering more than 50% of the total computing power) is tantamount to destroying its hardware investment and excluding itself from the network.

Hashcash is a famous consensus by Proof of Work. Just encrypt a message via a hash function . Finding the decryption key is mathematically impossible: there is no alternative to generating keys randomly and trying them one by one to find the original message. This effort requires computational power, it is the proof of work.

4. Execute your first smart contract

Mounting a blockchain is only of interest if you can run a “smart contract”. That is a “smart contract” that self-executes from a predefined threshold that can be a date, an amount, or any duly authenticated event. In the field of public blockchains, this concept made the success of Ethereum.

The reference language for developing such applications on Ethereum is Solidity. This language is relatively simple and approaches an object-oriented programming environment with notions of class, attribute, function. In addition to Ethereum specificities, when a function is used, for example, each transaction has an issuer, associated costs. The code is also more sensitive, the slightest error has consequences.

Smart contract as a web application

Beyond knowledge in JavaScript, such a project would involve having a comprehensive understanding of the blockchain, its philosophy, and constraints. Before putting your hands in grease, it is important to first ask the question of the relevance of a DApp (or decentralized application), which is only useful for resolving a problem of trust between actors.

5. Debug and scale

The debugging of a blockchain seems to have marked the minds of those who practiced it. Unlike a program run by a computer, a block is executed on a set of nodes or network terminations. You should know that each must result in a treatment equivalent to those of others. The process makes debugging the application extremely complex.

To fix the problem, you will have to create a new one and then wait for the chain to propagate the changes. Finally, in the case of open source platforms, the code is constantly evolving.

For all these reasons, it is recommended to have your smart contract audited by an expert. A phase that would be all the more essential in the case of a contract deployed on a public blockchain for business purposes targeting customers. On this point, the case of the organization The DAO which was stolen the equivalent of 50 million dollars in Ethers because of a bug is in everyone’s minds.