Université libre de Bruxelles
INFO-F-405 - Project: Cryptocurrencies. Encore!

François Gérard

2017-2018

In the homework, we asked you to gather information on the mechanisms used in cryptocurrencies. Now, to be sure you really master this technology, you will have to prove that you can make it work in practice. However, we will simplify a bit the picture to avoid the full P2P structure of the network.
We ask you to implement a simplified cryptocurrency that will have at least the four following components:

- Master node
- Relay nodes
- Miners
- Wallets

Master node: There will be only one instance of this type of node. Instead of a fully decentralized network, a master node will handle the blockchain. Its only purpose is to store and update the blockchain and it will only be queried by relay nodes. It is the authority on the network regarding what the blockchain is, that is to say, it will add a new block only if it matches the current state of the chain it has in memory. This means that if multiple relay nodes send newly mined blocks, only the first one to arrive will be added to the chain and others will be discarded.

Relay nodes: There will exist several relay nodes (you can choose how much in practice), their purpose is to make a link between miners, wallets and the master node. Their (IP) addresses are publicly known (they can be hardcoded) and only them will exchange messages with the master node.
They should:

- Keep an updated copy of the blockchain
- Send mined blocks received from the miners to the master node
- Forward a copy of (a part of) the blockchain to the wallets
- Receive transactions requests from wallets
- Send those transactions to the miners on request

Miners: Their goal is to create valid blocks to be inserted in the blockchain. They request the transactions directly from the relay nodes. We will use a classical proof-of-work system for mining:

a block will be considered mined if its transactions are all valid and its hash starts with a given number of zeros (this number is called the difficulty). To create multiple hash values out of a fixed set of transactions, the block will contain, in addition to the transactions, a large enough nonce. Once a block is mined and added to the chain, the miner should be rewarded with coins.

Wallets: The wallets represent the users of the cryptocurrency. They offer the possibility to create new addresses with associated key pairs and to send newly signed transactions to the relay nodes. The keys will be stored encrypted on the device running the wallet and a password to decrypt them will be asked when it launches. The wallet can also explore blocks or request a full copy of the blockchain via a relay node.

On the pure cryptographic side, we want you to use the following algorithms:

- SHA256 to mine
- DSA to sign transactions
- RIPEMD160 to derive addresses from public keys
- AES-128 to encrypt private keys

You will provide a code in C++, Java or Python implementing previously described functionalities together with a readme explaining how to compile, set up the network and use wallets. There will be a defense organized in December where you will explain what you did and make a demonstration showing all the features.

Note that there are a lot of things that were not specified in this document, we only gave an high level overview of what the final product should be. Feel of course free to ask questions but we really want you to make your own decisions regarding the details of your implementation. You can make your own choices, but be ready to explain them !

The project should be sent by email to **fragerar@ulb.ac.be** in a single ZIP file with subject "INFO-F-405 Project Group XX" before 23:55:00 on Monday, 4th of December 2017