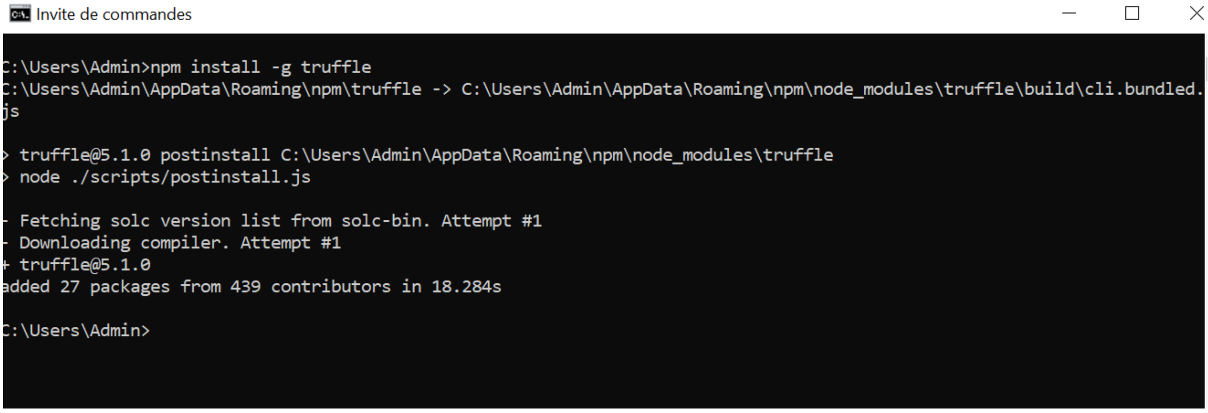
Lundi, 25 November 2019,

Monnaies Numériques

Computer Science & Engineering
9329020182
Raphael STIEFFATRE

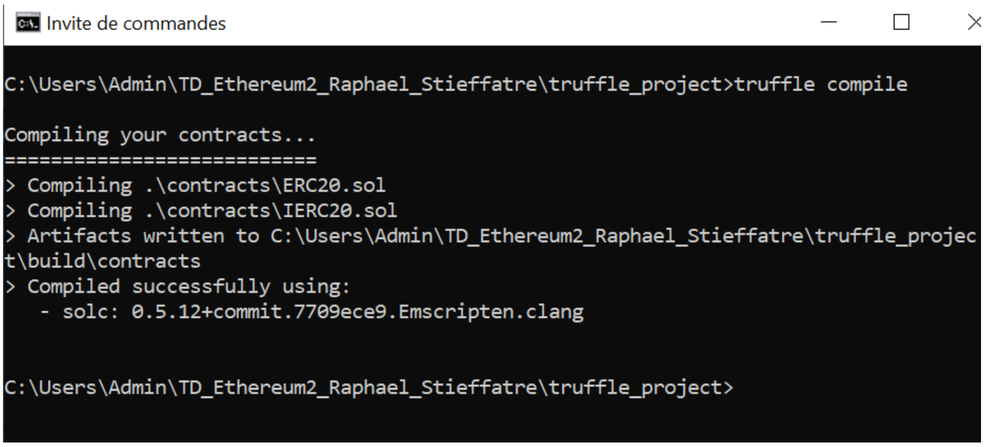
1) Installing and creating a truffle project :



```
:\Users\Admin>npm install -g truffle
:\Users\Admin\AppData\Roaming\npm\truffle -> C:\Users\Admin\AppData\Roaming\npm\node_modules\truffle\build\cli.bundled.
js

 truffle@5.1.0 postinstall C:\Users\Admin\AppData\Roaming\npm\node_modules\truffle
 node ./scripts/postinstall.js

 Fetching solc version list from solc-bin. Attempt #1
 Downloading compiler. Attempt #1
 truffle@5.1.0
added 27 packages from 439 contributors in 18.284s

:\Users\Admin>
```

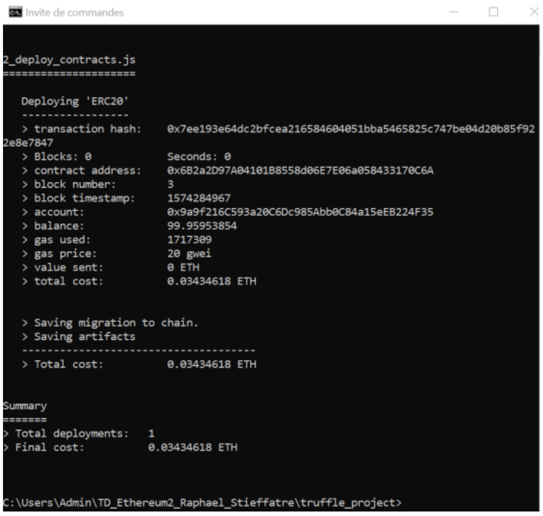
2) ERC20 token contract :

ERC20 : implementation of OpenZepelin

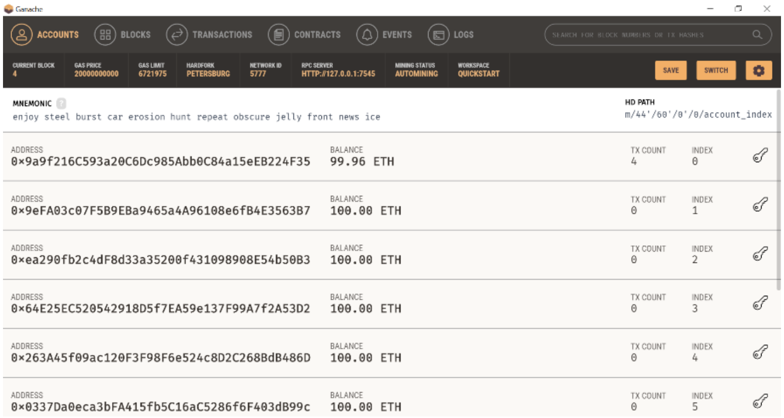


```
C:\Users\Admin\TD_Ethereum2_Raphael_Stieffatre\truffle_project>truffle compile

Compiling your contracts...
===========================
> Compiling .\contracts\ERC20.sol
> Compiling .\contracts\IERC20.sol
> Artifacts written to C:\Users\Admin\TD_Ethereum2_Raphael_Stieffatre\truffle_projec
t\build\contracts
> Compiled successfully using:
   - solc: 0.5.12+commit.7709ece9.Emscripten.clang


C:\Users\Admin\TD_Ethereum2_Raphael_Stieffatre\truffle_project>
```

3) Migration to Ganache :



```
2_deploy_contracts.js
=====================

   Deploying 'ERC20'
   -----------------
   > transaction hash:    0x7ee193e64dc2bfcea216584604051bba5465825c747be04d20b85f92
2e8e7847
   > Blocks: 0            Seconds: 0
   > contract address:    0x6B2a2D97A04101B8558d06E7E06a058433170C6A
   > block number:        3
   > block timestamp:     1574284967
   > account:             0x9a9f216C593a20C6Dc985Abb0C84a15eEB224F35
   > balance:             99.95953854
   > gas used:            1717309
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.03434618 ETH


   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:          0.03434618 ETH


Summary
=======
> Total deployments:   1
> Final cost:          0.03434618 ETH


C:\Users\Admin\TD_Ethereum2_Raphael_Stieffatre\truffle_project>
```



CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
4	20000000000	6721975	PETERSBURG	5777	HTTP://127.0.0.1:7545	AUTOMINING	QUICKSTART

MNEMONIC
enjoy steel burst car erosion hunt repeat obscure jelly front news ice

HD PATH
m/44'/60'/0'/0/account_index

ADDRESS	BALANCE	TX COUNT	INDEX
0×9a9f216C593a20C6Dc985Abb0C84a15eEB224F35	99.96 ETH	4	0
0×9eFA03c07F5B9EBa9465a4A96108e6fB4E3563B7	100.00 ETH	0	1
0×ea290fb2c4dF8d33a35200f431098908E54b50B3	100.00 ETH	0	2
0×64E25EC520542918D5f7EA59e137F99A7f2A53D2	100.00 ETH	0	3
0×263A45f09ac120F3F98F6e524c8D2C268BdB486D	100.00 ETH	0	4
0×0337Da0eca3bFA415fb5C16aC5286f6F403dB99c	100.00 ETH	0	5

4) Whitelisting : use of the modifier onlyWhitelisted of Openzeppelin WhitelistedRole contract :

```
function transferFrom(address from, address to, uint256 value)
  onlyWhitelisted
  public
  returns (bool)
{
  require(value <= _balances[from]);
  require(value <= _allowed[from][msg.sender]);
  require(to != address(0));

  _balances[from] = _balances[from].sub(value);
  _balances[to] = _balances[to].add(value);
  _allowed[from][msg.sender] = _allowed[from][msg.sender].sub(value);
  emit Transfer(from, to, value);
  return true;
}
```

```
function transfer(address to, uint256 value)
onlyWhitelisted
public
returns (bool)
{
  require(value <= _balances[msg.sender]);
  require(to != address(0));

  _balances[msg.sender] = _balances[msg.sender].sub(value);
  _balances[to] = _balances[to].add(value);
  emit Transfer(msg.sender, to, value);
  return true;
}
```