Exposé technique « Développer un contrat/programme sur Ethereum »

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 4 juillet 2016. Dernière mise à jour le 6 juillet 2016

https://www.bortzmeyer.org/pas-sage-en-seine-ethereum.html

Le 2 juillet, au festival Pas Sage en Seine / Hacker Space Festival <https://www.pseshsf.org/>, j'ai eu le plaisir de faire un exposé sur la chaîne de blocs Ethereum, plus précisement sur l'écriture de programmes (on dit parfois **contrats**) Ethereum. Cet exposé <https://www.pseshsf.org/fr/programme/2016/#event-436> s'adresse donc surtout aux programmeurs.

Voici les supports de l'exposé :

— Version adaptée à l'écran (en ligne sur https://www.bortzmeyer.org/files/pses2016-contrats-ethere pdf),
— Version adaptée à l'impression sur des arbres morts (en ligne sur https://www.bortzmeyer.org/files/pses2016-contrats-ethereum-PRINT.pdf),
— Source (en ligne sur https://www.bortzmeyer.org/files/pses2016-contrats-ethereum.tex).

Il y aussi la vidéo en ligne <http://data.passageenseine.org/2016/mp4/PSESHSF-2016%20-%20St%C3%A9phane%20Bortzmeyer%20-%20D%C3%A9velopper%20un%20contrat%20programme%20sur%20Ethereum.mp4>.

Les deux contrats présentés à Pas Sage En Seine, Soleau et FindByHash, ont été installés sur la chaîne de blocs. Sur la chaîne de tests « Morden » <http://morden.io/>, Soleau est installé en 0x165180498e843c5119d7d57b866da1392b8e8185 et FindByHash en 0x78db9a1dfe1b46c4361ac91cda111f53

Sur la « vraie » chaîne <https://ethstats.net/>, Soleau est en 0x39aa4006ee5941c0c0e41b924fdafcb2c4c et FindByHash en 0x9b6e416ea0d89a09b4ae036a774b1d31825252f8. Si vous voulez interagir avec ces contrats, voici l'ABI de Soleau :

```
[{"constant":true,"inputs":[{"name":"hash","type":"string"}],"name":"get","outputs":[{"name":"success","type":"b
```

Et celle de FindByHash :

```
[{"constant":true,"inputs":[{"name":"key","type":"string"},{"name":"index","type":"uint256"}],"name":"get","
```

Ça s'utilise comment ? Prenons l'exemple de Soleau sur la chaîne de test. Si on utilise le logiciel geth <https://github.com/ethereum/go-ethereum/wiki/geth>, avec sa console JavaScript, on déclare le contrat et on indique l'adresse :

```
soleauC = eth.contract([{"constant":true,"inputs":[{"name":"hash","type":"string"}],"name":"get","outputs":

soleau = soleauC.at("0x165180498e843c5119d7d57b866da1392b8e8185")
```

Une fois que c'est fait, on peut appeler l'ABI du contrat. Ici, on demande si un condensat est bien stocké dans la chaîne :

```
> soleau.get("98461ec184a39f0b8d89401a2756ffc84c2473a772655b425d794db6e7b68a8a")
[true, 1211232, 1467041583, "0xaf8e19438e05c68cbdafe33ff15a439ce6742972"]
> soleau.get("666")
[false, 0, 0, "0x0000000000000000000000000000000000000000"]
```

Sur la chaîne principale, le même contrat a une valeur `5e1e7a61931acb3f0e2bb80fc1d88e242d8556e6` stockée :

```
> soleau.get("5e1e7a61931acb3f0e2bb80fc1d88e242d8556e6")
[true, 1830809, 1467745954, "0xc90cd1fa9940a4d4a07a37c53bb4f423fd286945"]
```

On peut aussi ajouter des valeurs (ici, sur la chaîne de test). Comme cela change l'état de la chaîne, il faut faire une transaction, et payer, à la fois l'essence (ici, 400000 unités mais moins de 100000 seront effectivement utilisées) et le prix prévu dans le contrat :

```
> soleau.record.sendTransaction("d479b91d7a2cdd21f605c5632344228dd5f75d66", {from: eth.accounts[0], gas: 400
"0xfb6bc725e303c79c2c5426c3a0d4fce90b635521826e5bd3e94ddfa3d80c48da"
```

Le résultat est l'identificateur de la transaction, que vous pouvez regarder en ligne <http://testnet.etherscan.io/tx/0xfb6bc725e303c79c2c5426c3a0d4fce90b635521826e5bd3e94ddfa3d80c48da> (avec le bouton "*Convert to ASCII*", vous verrez le condensat enregistré, dans les données de la transaction). Sur la chaîne principale, un exemple de transaction de ce contrat est disponible ici <https://www.etherchain.org/tx/0xab9ea8edb42aaad2e2b7856dbc77c0039a9aa0c8858a867d31ac97a0e394b9
Pour le contrat FindByHash, si vous voulez regarder des valeurs enregistrées, il y a `cf4163b8f4c13b915e246ea7d2` sur la chaîne de tests et `3d10dcb5e503d3b8abc2fa5a72adb0a503930e0b6b8a893f17dda63b9b717dba` sur la chaîne principale :

```
> findhash.num_of("cf4163b8f4c13b915e246ea7d2792156")
2
> findhash.get("cf4163b8f4c13b915e246ea7d2792156", 0)
[true, "https://localhost/"]
> findhash.get("cf4163b8f4c13b915e246ea7d2792156", 1)
[true, "https://www.bortzmeyer.org/toto"]
```

Pour enregistrer des URL dans ce contrat, le plus simple est ce petit script shell (en ligne sur `https://www.bortzmeyer.org/files/findbyhash-url-register.sh`), qui s'utilise ainsi :

```
% findbyhash-register-url.sh http://www.bortzmeyer.org/pas-sage-en-seine-ethereum.html
...
"0x82a808828a115547b242f335783bf75a0c96d2d746ab9dff160898a8f28a5411"
3d10dcb5e503d3b8abc2fa5a72adb0a503930e0b6b8a893f17dda63b9b717dba registered for http://www.bortzmeyer.org/pas-sa
```

(Et vous pouvez voir la transaction en ligne <https://www.etherchain.org/tx/0x82a808828a115547b242f33

Si le sujet vous intéresse, j'en parlais plus longuement à la Journée du Conseil Scientifique de l'AFNIC <https://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-generales/9896/show/journee-du-conseil-scientifique-de-l-afnic-le-11-juillet-2016-1.html> le 11 juillet (avec d'autres exemples de code, rassurez-vous).

Il y avait **plein** d'autres trucs géniaux à PSESHSF, n'hésitez pas à regarder le programme <https://www.pseshsf.org/fr/programme/2016/>. Mes préférés (c'est complètement subjectif), faire son pain soi-même <https://www.pseshsf.org/fr/programme/2016/#event-461> (et avec du levain), les explications (avec démo de diffuseur d'odeurs et bonbons qui sentent bon) sur le marketing sensoriel <https://www.pseshsf.org/fr/programme/2016/#event-511>, le projet pour un camp de hackers en été en France <https://www.pseshsf.org/fr/programme/2016/#event-509>, la conférence sur l'éducation au numérique <https://www.pseshsf.org/fr/programme/2016/#event-505> (qui ne sortira sans doute pas en vidéo, l'auteur étant mineur), même si sa seconde partie, sur l'éducation au "*business*" a suscité (à juste titre), des réactions houleuses, la reprise de contrôle de l'alimentation <https://www.pseshsf.org/fr/programme/2016/#event-502>, le système d'exploitation Qubes <https://www.pseshsf.org/fr/programme/2016/#event-499> (j'avais parlé de ce système sur ce blog <https://www.bortzmeyer.org/qubes.html> mais sans le tester), la bière libre <https://www.pseshsf.org/fr/programme/2016/#event-428> (j'ai goûté ; un peu forte), l'appel aux citoyens à participer à la science <https://www.pseshsf.org/fr/programme/2016/#event-430>, la synthèse du récent virage <https://www.pseshsf.org/fr/programme/2016/#event-524> de la Quadrature du Net <https://www.laquadrature.net/>, le bilan de la loi Renseignement <https://www.pseshsf.org/fr/programme/2016/#event-521>, etc.

---

https://www.bortzmeyer.org/pas-sage-en-seine-ethereum.html