Hausaufgabe zum Solidity-Workshop

Michael Fröwis

28. Mai 2020

Die Abgabe der Übungen ist fällig am 04.06.2020 im OLAT. Jede Aufgabe spezifiziert die Dateien, die bei der Abgabe erwartet werden. Die Fragen müssen jeweils in aufgabeX.txt oder aufgabeX.pdf beantwortet werden.

Viel Spaß bei der Bearbeitung!

Remix IDE/Debugger:	`https://remix.ethereum.org/`
Solidity-Dokumentation:	`https://solidity.readthedocs.io/`

1 Schere, Stein, Papier auf der Blockchain

(Lesen Sie die Aufgabe komplett, denn in den Unteraufgaben verstecken sich Hinweise für die erste Aufgabe.)

a. Schreiben Sie einen Smart Contract in Solidity, mit dem zwei Personen Schere, Stein, Papier (SSP) spielen können. Es soll außer der Blockchain keine dritte Partei einbezogen werden und kein Spieler darf zu irgendeinem Zeitpunkt mogeln können.

b. Beschreiben Sie kurz das Problem von geheimen Werten auf der Ethereum-Blockchain. Wie sieht die Lösung für unseren SSP-Smart Contract aus?
Tipp: Erinnern Sie sich an den kryptographischen Münzwurf.

c. Sie können folgende Solidity-Funktion verwenden, um ein *Commitment* zu erzeugen. Was ist bei der Verwendung dieser Funktion umbedingt zu beachten?

```
// use via call only...
function generateCommit(uint v, uint rand) public pure
returns (bytes32) {
    return keccak256(abi.encodePacked(v, rand));
}
```

Abgabe: `rock_paper_scissors.sol`, `aufgabe1.txt` oder `aufgabe1.pdf`
Links: `https://de.wikipedia.org/wiki/Schere,_Stein,_Papier`

2 “I accidentally killed it”

Lesen Sie diesen Fehlerbericht auf GitHub:
`https://github.com/openethereum/openethereum/issues/6995`.

Beantworten Sie folgende Fragen:

a. Beschreiben Sie mit eigenen Worten, was genau passiert ist.

b. Welche Ursache hatte der Bug?

c. Welche Auswirkungen hatte der Bug?

d. Wieso wurde ein Teil des *Wallets* als externe Bibliothek realisiert?

e. Wie viel Geld ist in etwa verloren gegangen?

Abgabe: `aufgabe2.txt` oder `aufgabe2.pdf`