Prof. Dr. Jens-Matthias Bohli
Fakultät für Informationstechnik

Projektaufgabe 1 (bis 22.11)

Zusammenarbeit in Gruppen:

Sie können diese idealerweise in 2er Gruppen bearbeiten. 3er Gruppen bearbeiten die das 2-stufige Beispiel (siehe unten).

Aufgabe:

Ziel dieser Aufgabe ist es ein Wett-Spiel für 3 Teilnehmer als Ethereum-Contract zu realisieren und die Kosten des Spiels auszuwerten (Gas für die Funktionsaufrufe).

Regeln des Spiels

- Jeder Teilnehmer leistet einen **Einsatz**, der Gewinner bekommt den Einsatz ausbezahlt.
- Jeder Teilnehmer soll mindestens eine Zahl als seinen Spielzug übermitteln. Aus der Gesamtheit der Zahlen wird der Gewinner ermittelt.
    - Verwenden Sie ein **kryptographisches Commitment** um die Zahlen bis zum Spielende zu verbergen.
    - Jeder Spieler muss zusätzlich zu seinem Einsatz ein **Pfand** hinterlegen, das er nach dem öffnen des Commitments wieder ausbezahlt bekommt.
- Der Gewinner soll durch ein **Event** verkündet werden, damit er seinen Einsatz abholen kann.

Beispiele:

- 2er Gruppe: Jeder Teilnehmer P_0, P_1, P _2 übermittelt eine Zufallszahl z_i. Die Summe der Zahlen modulo 3 bestimmt den Gewinner.
- 3er Gruppen: Jeder Teilnehmer P_0, P_1, P 2 übermittelt zunächst eine Zahl r_i. Daraus wird die Summe mod 100 gebildet. Im 2 Schritt übermittelt jeder Spieler eine Zahl z_i. Der Teilnehmer, der am nächsten an der Summe liegt gewinnt.

Bewertungskriterien:

- Sicherheit der Implementierung
- Effizienz, Originalität, etc...