TO ATTACK, OR NOT TO ATTACK...

… that is the question.

Group Project by Jeremias Lenzi & Ramazan Maliqi

Smart Contracts and Decentralized Blockchain Applications

University of Basel, Prof. Dr. Fabian Schär, 10. December 2019

SITUATION

A big jackpot is sitting around on the blockchain

We're somewhat poor students and want to get it!

COOL!

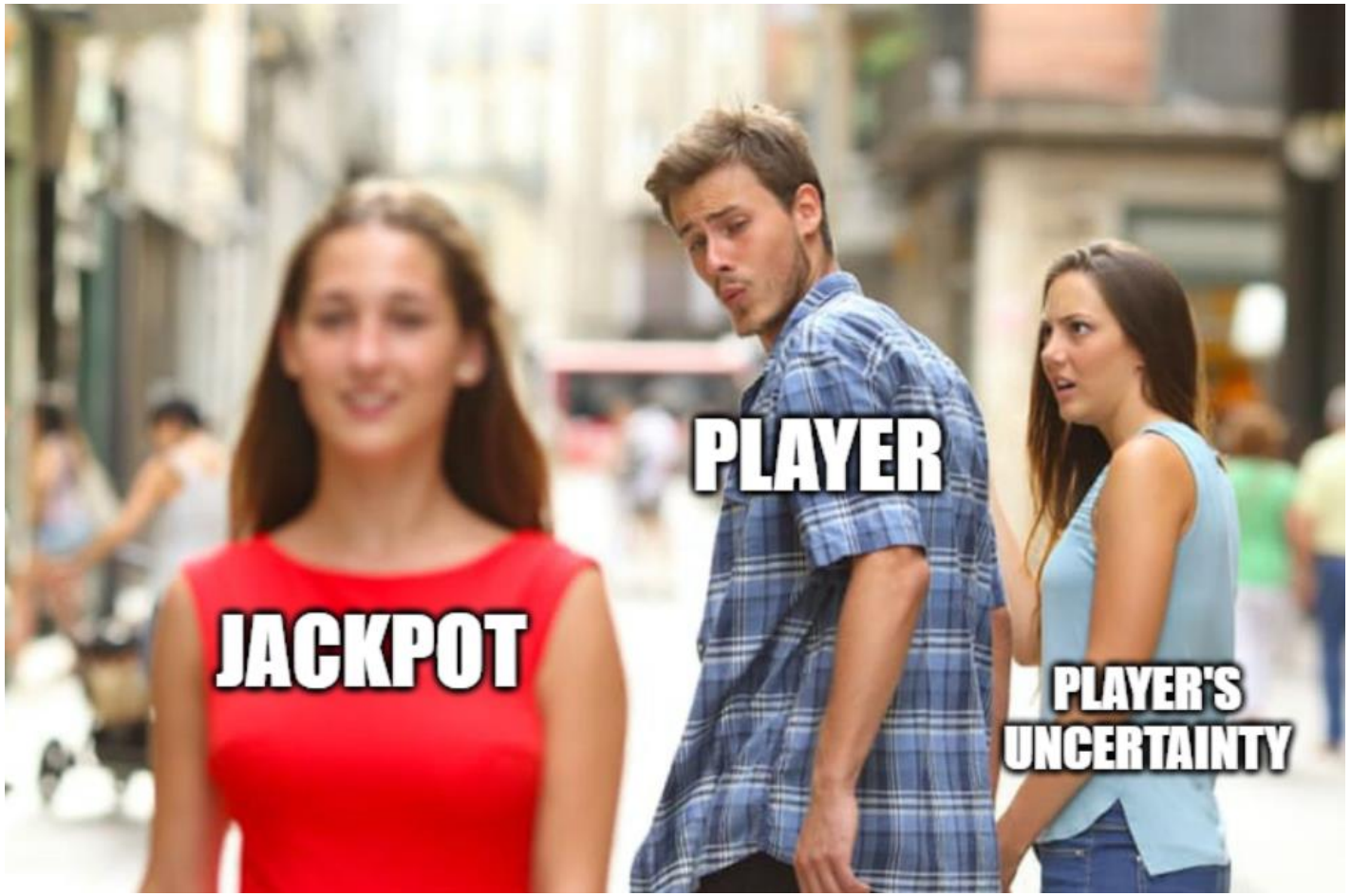
Coordination among attackers needed to succeed

There is COSTS associated with the attack. Poor students!

We do not know how many attackers are sufficient

NOT COOL!

SITUATION SUMMARISED



SOME THEORY FIRST: COMMIT-REVEAL

1. Step

Keccak256-hash → Commit = Hash gets stored → Commit is linked to player

31password

3 = player's bet in ETH (has to be an uint between 1 and 9)

1 = player's decision to attack (0 if no attack planned)

password = player's personal password (e.g. wewillwin)

2. Step

Plain text («31password») → Reveal = do they really match → Player's decision is public

https://emn178.github.io/online-tools/keccak_256.html

HOW DOES IT WORK ON THE BLOCKCHAIN?

Let’s gamble on Rinkeby testnet!

AREAS OF CONCERN

- Dynamic cost of attack along the number of Ether in the jackpot to disincentivize multiple attacks from a single person from different accounts
- Who provides the initial jackpot? Would such a contract be used in the wild?
- …

THANK YOU