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

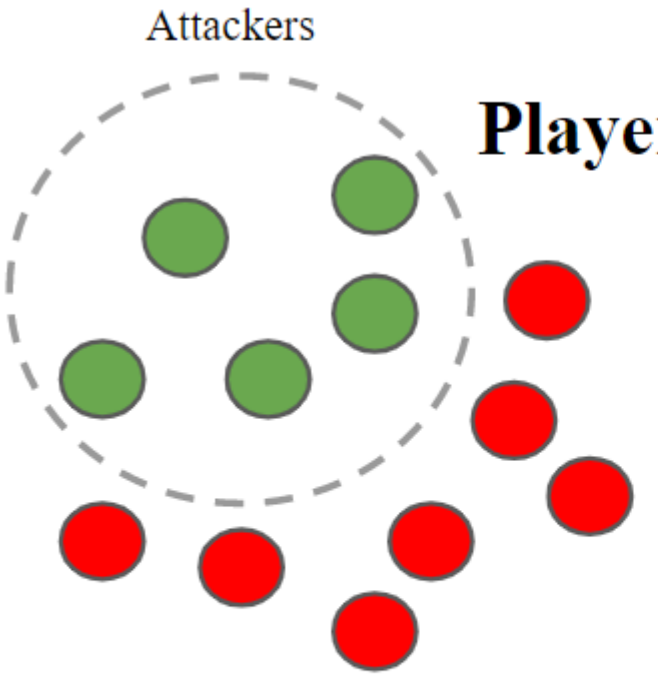
There is COSTS associated with the attack. Poor students!

We do not know how many attackers are sufficient

NOT COOL!

SITUATION SUMMARISED

INTUITION OF THE GAME



- Attackers win proportional to their bet over total attackers' bets
- Defenders always get refund
- Defenders make "false bets" to deceive other players
- There is a cost on attacking
- Players that try to misbehave loses their bets
- Players are incentivized to attack, increasingly through the rounds

Resistance = 90% ⇒ Attack Failed ⇒ Jackpot increases !!!

Resistance = 20% ⇒ Attack Succeeded ⇒ Winners take price

A BIT OF THEORY: COMMIT-REVEAL

1. Step

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

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 intended)

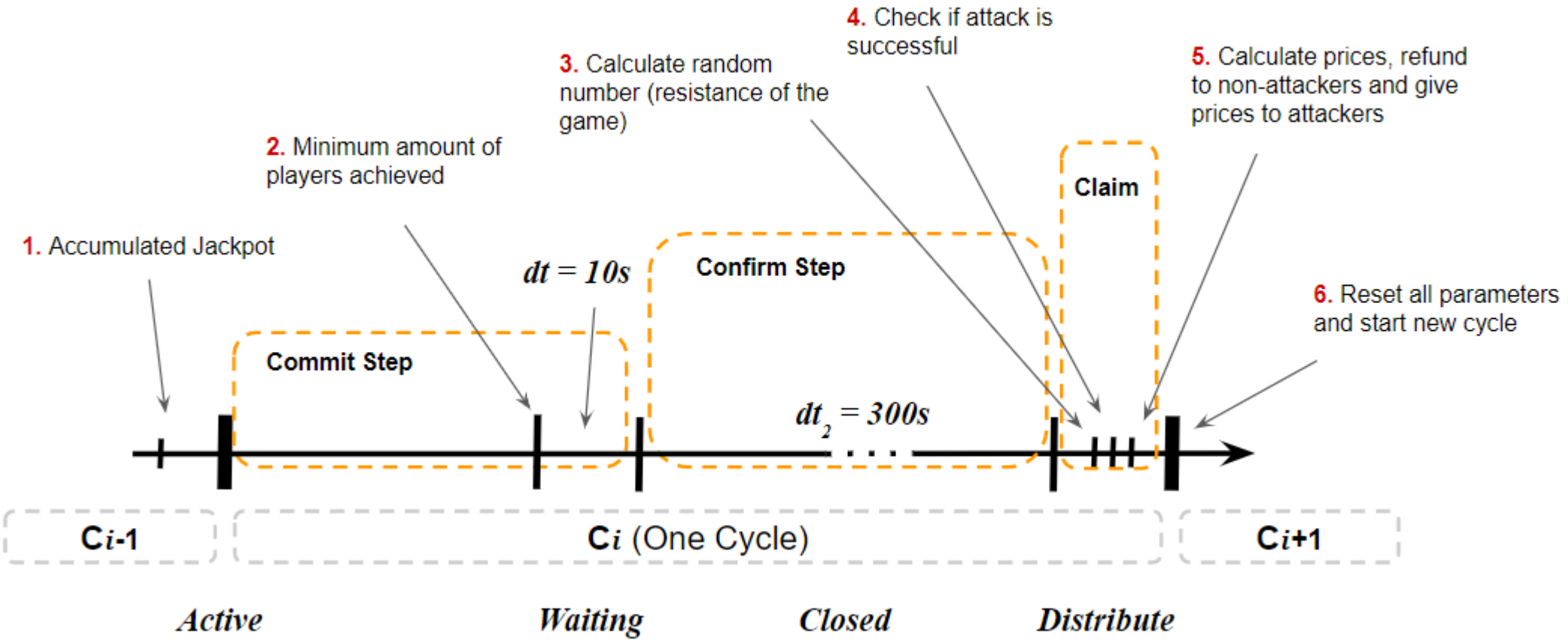
password = player's personal password (e.g. wewillwin)

2. Step

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

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

TIMELINE OF THE GAME



HOW DOES IT WORK ON THE BLOCKCHAIN?

Let’s gamble on Rinkeby testnet!

THANK YOU