Liar’s Dice on a Blockchain
or Decentralised Atomic Information Disclosure using Onion Rings

Oliver Stengele
oliver.stengele@kit.edu

An arbitrary number of parties each want to disclose some information if and only if all parties disclose their information.

- Decentralised: No single party can force or abort the process to their own advantage.
- Atomic: Either all information is disclosed or none.

Onion Rings use Onion Encryption to form Cyclic Dependency Graphs out of private keys necessary to read submissions.

- Once a Ring is constructed, submissions can be published.
- As soon as the successive deconstruction of the Ring starts, submissions are no longer accepted.

• Construction and deconstruction of Onion Rings must be conducted on a public, persistent, tamper-evident, and non-repudiative channel. ➤ Blockchain
• Proper participation must be incentivised, unwanted behaviour must be discouraged. ➤ Game Theory
• Collusion between Ring members and Sybil attacks must be mitigated.

• Ring size (n) and number of encryption layers (k) determine:
  - Number of honest parties required to ensure disclosure. At least \( k \cdot \left\lceil \frac{n}{k} \right\rceil \cdot (k - 1) + \max(\lceil n \% k \rceil - 1; 0) + 1 \).
  - Number of malicious parties that can be tolerated. At least \( k - 1 \), at most \( n - k - \left\lfloor \frac{n-k}{k} \right\rfloor \).
• Depending on how honest and malicious parties are arranged in the Ring.
  … unless Onion Rings are constructed recursively.