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

Oliver Stengele
Karlsruhe Institute of Technology
oliver.stengele@kit.edu

We define the atomic information disclosure problem which tasks an arbitrary number of parties to release an individually held piece of information iff all of the parties release their information. This is similar to the “common hand” variant of Liar’s Dice\(^1\) where the previously private dice rolls of each player have to become public in order to determine the outcome of each round. This problem also arises in open ballot voting where partial results are undesirable and timing-based advantages and disadvantages should be eliminated.

To achieve the desired atomicity, the privilege of disclosure must be delegated, otherwise parties could refuse to participate after learning the information of some or all other parties. In order to avoid a single point of failure and to separate the privilege of disclosure from read access, a decentralised approach is imperative.

We present the concept of Onion Rings which uses asymmetric encryption to construct multilayered lockboxes containing the private keys necessary for disclosure in a circular manner. Using an Onion Ring, a large number of participants can delegate the privilege of disclosure to a comparatively small group in such a way that the members of the ring cannot peek into the encrypted submissions whose disclosure they oversee, unless they collude. While threshold encryption schemes can be used to construct a similar procedure, they tend to be difficult to deploy on current blockchains or prohibitively expensive to execute.

The circular structure gives rise to a quasi-threshold property where only a subset of involved parties need to agree on the release of their keys in order to cause the disclosure of all submissions. While it is unavoidable that any party in the ring holding the last private key necessary for disclosure can peek before releasing their key, the circular construction ensures that this advantageous position is held by at least two parties of which only one needs to cooperate in order to finalise the procedure.

Both the number of participants and the number of lockbox layers are adjustable parameters that immediately affect the security of the scheme with regard to both ensuring disclosure and preventing unwanted outcomes.

Lastly, it should be noted that game theory and economic incentive schemes seem to be well suited to facilitate the proper execution of this scheme and to discourage unwanted behaviour. A blockchain can serve as both the enforcement and rewarding mechanism as well as a public, persistent, tamper-evident, and non-repudiative communication channel.

\(^1\) [https://en.wikipedia.org/wiki/Liar%27s_dice#Common_hand](https://en.wikipedia.org/wiki/Liar%27s_dice#Common_hand)