**Privacy in Blockchain**

* Current approaches
  + Cryptography [1] [2]
    - Conceals the identity of each user
    - Uses private/ public keys
    - Not suitable/ sufficient for our use case, as we need a link between the real households and their keys to ensure correctness
  + Zero-knowledge proofs
    - One party proves to another party that a transaction is true without revealing details about the specific transaction [3] [4]
    - Implementation by complex cryptographic methods [4]
    - allows verification of transactions without revealing identities [6]
    - suitable solution for our project
    - Basis to ZoKrates
* ZoKrates
  + toolbox using and providing zero-knowledge proof methods [6]
  + also allowing off-chaining of computational steps [7]
  + “address privacy challenges by efficiently off-chaining computations from the blockchain without impairing its desirable properties, e.g., trustlessness and immutable history” [7]
* Other approaches
  + Hawk
    - Smart contract system encrypting transactions on the blockchain [9]
    - Smart contracts can be implemented intuitively, compiler generates a cryptographic protocol [8]
    - Relies on zero-knowledge proofs [8]
    - Does not allow off-chaining 🡪 thus no performance and cost benefit

[1] https://lisk.io/academy/blockchain-basics/benefits-of-blockchain/blockchain-privacy-explained

[2] Zyskind G., Nathan O., Pentland A. (2015) Decentralizing Privacy: Using Blockchain to Protect Personal Data

[3] Rackoff C., Simon D.R. (1992) Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack. In: Feigenbaum J. (eds) Advances in Cryptology — CRYPTO ’91. CRYPTO 1991. Lecture Notes in Computer Science, vol 576. Springer, Berlin, Heidelberg

[4] https://zokrates.github.io/

[5] Eberhardt J., Tai S (2018) ZoKrates - Scalable Privacy-Preserving Off-Chain Computations

[6] <https://www.btc-echo.de/zokrates-soll-ethereum-weiter-ausbauen/>

[7] <https://www.ise.tu-berlin.de/menue/projects/zokrates/parameter/en/>

[8] Kosba A., et. al (2016) Hawk: The Blockchaain Model of Cryptography and Privacy-Preserving Smart Contracts

[9] oblivm.com/hawk/index.html