# Privacy in Decentralized Energy Trading

* Starting point: System until Milestone 1 (see GitHub Snapshot)
* Introduction of a Netting Entity
* Using ZoKrates for off-chaining computation
* HPU
  + Components
    - Household-Server (JS-Server)
    - Parity-Client
    - User Interface
    - Database
  + Hashes meter values and sends hashes to dUtility contract (on-chain; via Parity-Client)
  + Sends plain meter values to NED Server for netting
  + Collects Energy Transfer Receipts from the NED-Server
* Netting Entity
  + Components
    - NED-Server (JS-Server)
    - ZoKrates
  + Executes the netting algorithm
  + ZoKrates
    - Computes proof (netting correct)
    - Hashes meter values given from NED-Server (plain values as private input)
  + NED-Server
    - Sends proof to dUtility contract
    - Deploys Verification contract to Blockchain
* Ethereum Blockchain
  + Components
    - dUtility contract
    - Verification contract
    - Validator Set
  + dUtility checks that hashed values from ZoKrates match hash-value from the Households
* Trust in NED-Server?
  + Trust only that it keeps data safe (🡪 Data privacy)
  + Computation is verified by blockchain
  + No trust for correct netting needed
  + NED cannot manipulate data, or else the hashes will not be identical
* Proof is on blockchain 🡪 cannot be changed later