# Proposte applicative per ZKP

Nicolò Zarulli

Aprile 2022

**Le Proposte**

1. **Studio, utilizzo e/o replicazione di librerie di implementazione per modelli Zero Knowledge Proof**

   - **zkSNARKs**

     [1] Zokrates: toolbox per la creazione di zkSNARKS su Ethereum. E' disponibile un tutorial, fornito dai creatori, che permette di studiare la libreria per arrivare alla creazione di circuiti zero-knowledge-proofs testabili su Ethereum tramite l'IDE Remix.
     -> https://github.com/Zokrates/ZoKrates
     -> https://zokrates.github.io/gettingstarted.html
     -> https://zokrates.github.io/examples/rng_tutorial.html
     -> ZKP Application Demo (usa Zokrates, Truffle e Docker) https://medium.com/hackernoon/zero-knowledge-proof-application-demo-2a457cfc73c1

     [2] Gnark: libreria per la creazione di zkSNARKs (principalmente circuiti aritmetici) scritta in Go. Sono disponibili vari esempi introdotti dal creatore.
     -> https://github.com/ConsenSys/gnark

     [3] jSNARK: libreria scritta in Java, si basa su libsnark e puo' integrare circuiti prodotti dal compiler Pinocchio.
     -> https://github.com/akosba/jsnark

     [4] RollupNC: utilizzo delle librerie Circum e SnarkJS per la creazione di RollupNC (il RollUp è alla base di quesi tutte le implementazioni di protocolli zkp sulle blockchain: aggrega più transazioni in una singola transazione onchain).
     -> Tutorial: https://github.com/therealyingtong/roll_up_circom_tutorial
     -> RollupNC: https://github.com/rollupnc/RollupNC

   - **PayPub**
     PayPub è un interessante libreria-zk costruita su C++. Vuole implementare la possibilità di effettuare pagamenti affidabili ( quindi a *zero knowledge*) per la pubblicazione di informazioni sulla blockchain Bitcoin.
     -> https://github.com/unsystem/paypub

- **Zero Knowledge Range Proofs**

  [1] ING Group ZKRP framework: Il Gruppo Bancario ING ha portato avanti lo sviluppo di un framework completamente incentrato sui Zero Knowledge Range Proofs. La loro repository Open Source mette a disposizione un interessante implementazione del modello zkp *Bulletproofs*, interamente scritta in Go.
  - > https://github.com/ing-bank/zkrp
  Una versione archiviata del progetto mette a disposizione un branch interamente dedicato all'implementazione di Bulletproofs in Java.
  - > https://github.com/ing-bank/zkproofs/tree/bulletproofs

2. **Studio, utilizzo di applicativi che implementano ZKP**

- **zkSync**
  zkSync e' una piattaforma che ha l'obiettivo di implementare la validazione delle transazioni sullo strato L1 di Etheruem interamente a Zero Knowledge. Essendo un progetto Open Source, la completezza del codice e' disponibile su GitHub. La piattaforma offre dei test token per effettuare degli esperimenti. Possibili sviluppi applicativi:

  [1]Smart Contracts in Zinc o Solidity
  -> https://zksync.io/

  [2]Test delle prestazioni della piattaforma
  -> https://wallet.zksync.io/

  [3]Testnet con documentazione
  -> https://v2-docs.zksync.io/dev/guide/front-end-integration.html

- **zkPoD**
  zkPoD è una libreria open source che mette a disposizione un sistema decentralizzato per effettuare uno scambio di dati mirato al concetto di "Payment on Delivery". Il framework utilizza come *third party* la blockchain per assicurare che i nodi in comunicazione siano onesti tra loro. Questa libreria mette a disposizione un ottima documentazione per la sua sperimentazione.
  - > https://github.com/sec-bit/zkPoD-node

3. **Sviluppo di un applicativo nell'ambito ZKP**

- **Sviluppo di una DApp (L2 Ethereum) che implementi un framework zkp**
  Sviluppare un'applicazione decentralizzata che comunichi direttamente con il L1 di Ethereum e che veda l'implementazione di un protocollo ZKP. Una prima fase potrebbe vedere lo sviluppo di un framework per la creazione di Zero Knowledge Proofs (visto che si parla di Ethereum, sarebbe importante dare uno sguardo ai Range Proofs come Bulletproofs, oppure zkSNARKs), mentre una seconda fase potrebbe vedere l'implementazione di questo framework atteaverso una DApp su Ethereum.
  - > https://www.moesif.com/blog/blockchain/ethereum/Tutorial-for-building-Ethereum-Dapp-wi

- **Sviluppo di una libreria Python che implementi un protocollo ZKP per lo scambio di informazioni tra due Peer**
  Questa proposta si scosta dal mondo delle Blockchain e vede uno sviluppo più approfondito ed avanzato della mia piccola Libreria *pyZKP* che vede l'implementazione di un *Interactive ZKP* basato sull'aritmetica modulare.