Blockchain, GDPR & cryptography

zkSNARKs for scaling and privacy.

Alexandre Poltorak

Blockchain, Sustainable Development and Privacy
26-27 November 2019 – Berlin, Germany

The problem with GDPR and blockchains : Bitcoin & Privacy

Bitcoin is pseudo-anonymous. Bitcoin chooses and still maintains a pseudo and not fully anonymous system to be absolutely sure to maintain sound monetary policy (<21Mio bitcoins and predictable issuance rate). So auditability is an integral part of the Bitcoin design.

The tradeoff is between privacy and on the other side immutability, transparency & public verifiability.

Potential solutions for GDPR compliance

- RollUp : optimistic (staking), SNARKs (crypto)
- ZKP is an old field (80ies), but it only find practical application with blockchain technology
- ZkSNARKs - outsourcing the verification process
- Soundness / privacy (zk) - proprieties of zkSNARKs
- Non-reusable proofs
- Secure enclaves VS code obfuscation

zkSNARKs for scaling and privacy.

zkSNARKs - Zero-Knowledge Succinct Non-Interactive Argument of Knowledge

ZKPs allows for greater privacy on public blockchains by enabling nodes, or network participants, to verify the existence and validity of transactions, and therefore maintain distributed consensus, without actually being able to see or make public any of the transaction details, guaranteeing privacy.

“With zero-knowledge proofs, organizations can transact on the same network as their competition in complete privacy and without giving up the security of the public Ethereum blockchain." - EY

zkSNARKs provides the ability to verify the correctness of computations without having to execute them.

https://z.cash/ is a privacy-protecting, digital currency. It was the first to widely spread ZKP and zkSNARKs technology.

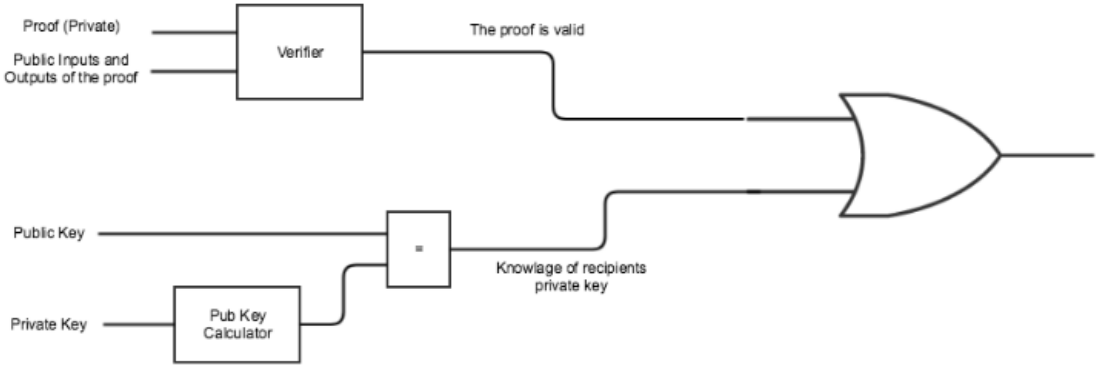
Coda Protocol

Coda is a scalability solutions using recursive zkSNARKs or recursive proof-composition. Coda swaps the traditional blockchain for a tiny cryptographic proof, enabling a cryptocurrency as accessible as any other app or website.

20 kB

Non-reusable proofs

This mechanism is implemented with a specific circuit that gives validity of the proof to the original recipient but invalidates the proof if this identity would try to forward it, because the proof is only valid if the sender does not know the private key of the validator. Since the initial recipient knows his own private key, this proof is not valid to be forwarded.



Other solutions based on zkSNARKs

- Off-chain scaling using zkSNARKs (sidechains)
- Iden3 – claims-based identity management
- zk-DAI
- Circom

https://zeroknowledge.fm Episodes 100