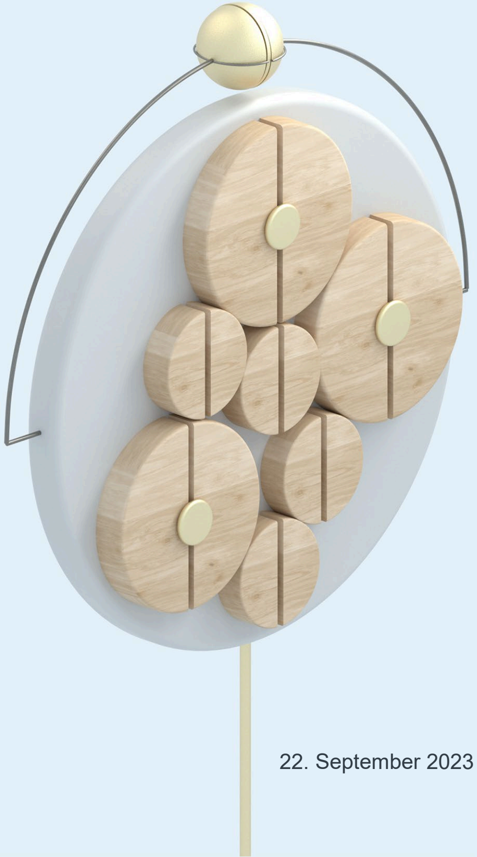
MME

Legal | Tax | Compliance

Zero-Knowledge Proofs in KYC Procedures

Overview, Use Cases and Regulation



Sebastian Hepp | Attorney at Law | sebastian.hepp@mme.ch

22. September 2023

Zero-Knowledge Proofs

Concept

- **What is Zero-Knowledge Proof?** A cryptographic process between two parties that allows one party to prove to the other party that a given statement is true without revealing the information beyond the statement.

- Introduced in 1985 by Shafi Goldwasser, Silvio Micali und Charles Rackoff

- **Types:**
  - **Interactive** ZKPs
  - **Non-interactive** ZKPs

Secret Data & Proofs

Sebastian Hepp

Zero-Knowledge Proofs

Use Cases

- **Why do we need Zero-Knowledge Proofs?**
- **Use Cases of Zero-Knowlegde Proofs on Blockchains:**
    - Verification of Transactions
    - Proof of Assets
    - Improvement of Scalability
    - Zero-Knowledge KYC (zkKYC)

Zero-Knowledge Proofs

Anti-Money Laundering Act (AMLA)

- **Scope:** Financial intermediaries and traders.

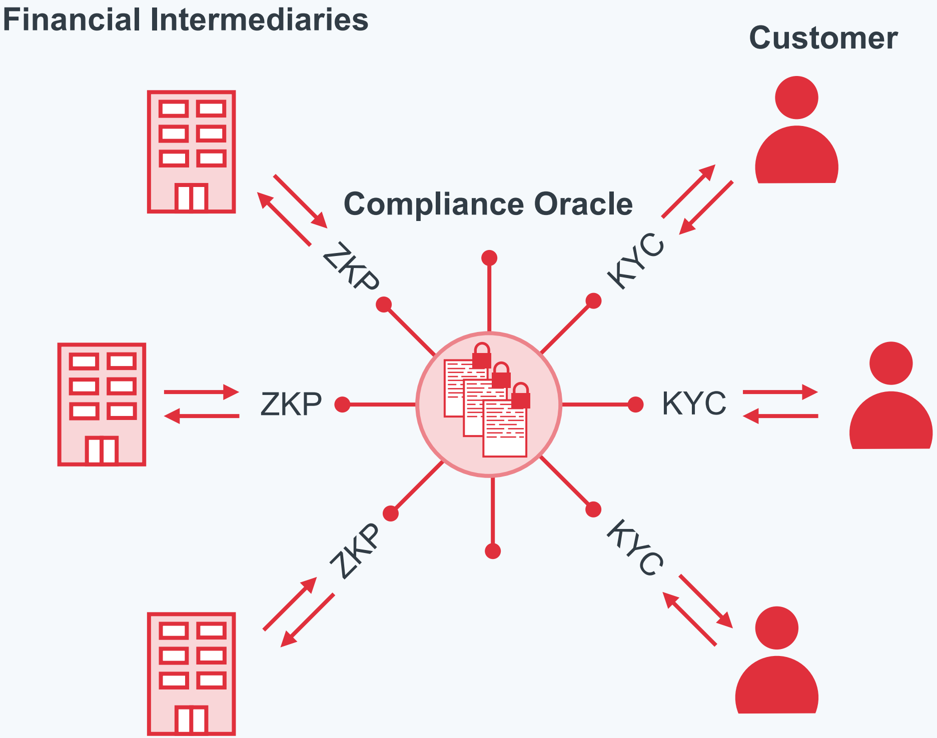
- **Obligations by law (non-exhaustive):**
  - Identification of the customers (Art. 3 AMLA)
  - Identification of the beneficial owners (Art. 4 AMLA)
  - Duty to keep the records (Art. 7 AMLA)

- **Are zkKYC procedures compatible with the current AML regim in Switzerland?**
  - Short answer: No

Zero-Knowledge Proofs

Compliance Oracle

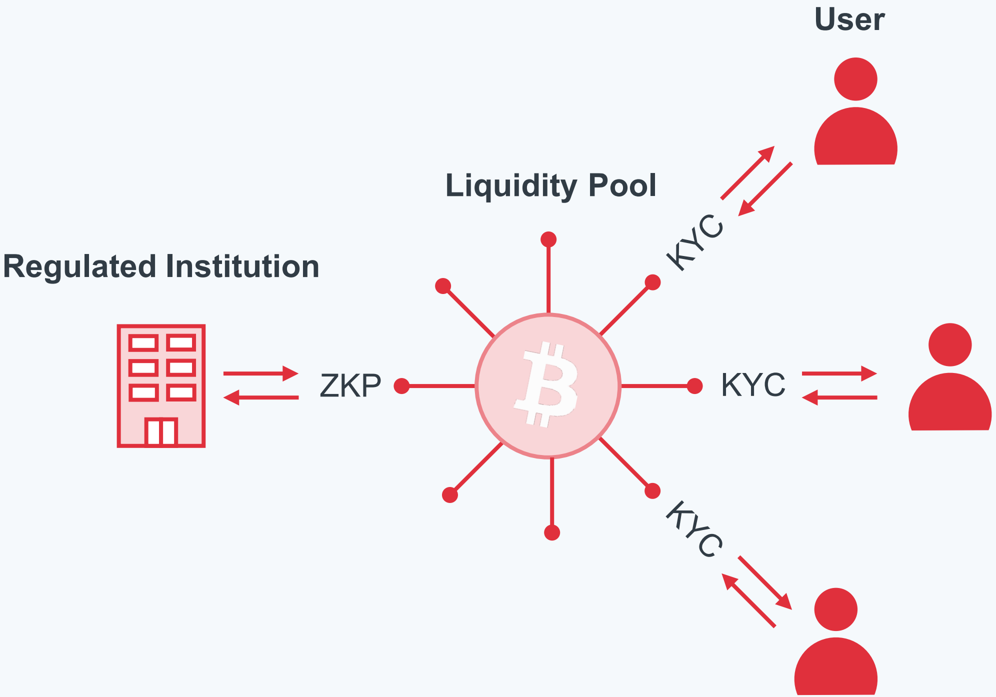
- **Functionality:**
  Onboarding new customers by a centrally trusted company (compliance oracle) which stores all the personal data. Improvement of reusability and storage of data.



Zero-Knowledge Proofs

Access to DeFi-Protocols for regulated Institutions:

- **Functionality:**
  With the ZKP technology, financial intermediaries can verify that all users of a DeFi-Protocol have been identified and wallet addresses are not contaminated, without having to know details about the individuals and/or wallet addresses.



Zero-Knowledge Proofs

Federal Act on Data Protection (FADP)

- **Scope:** Processing Personal Data.

- **Specific rights by law (not-exhaustive):**
  - Right to correct false personal data (Art. 6 FADP)
  - Right to delete personal data (Art. 6 FADP)
  - Right to access personal data (Art. 25 FADP)

- **Can Zero-Knowledge Proofs be used to solve the privacy issues in blockchain transactions?**
  - Short answer: Yes.

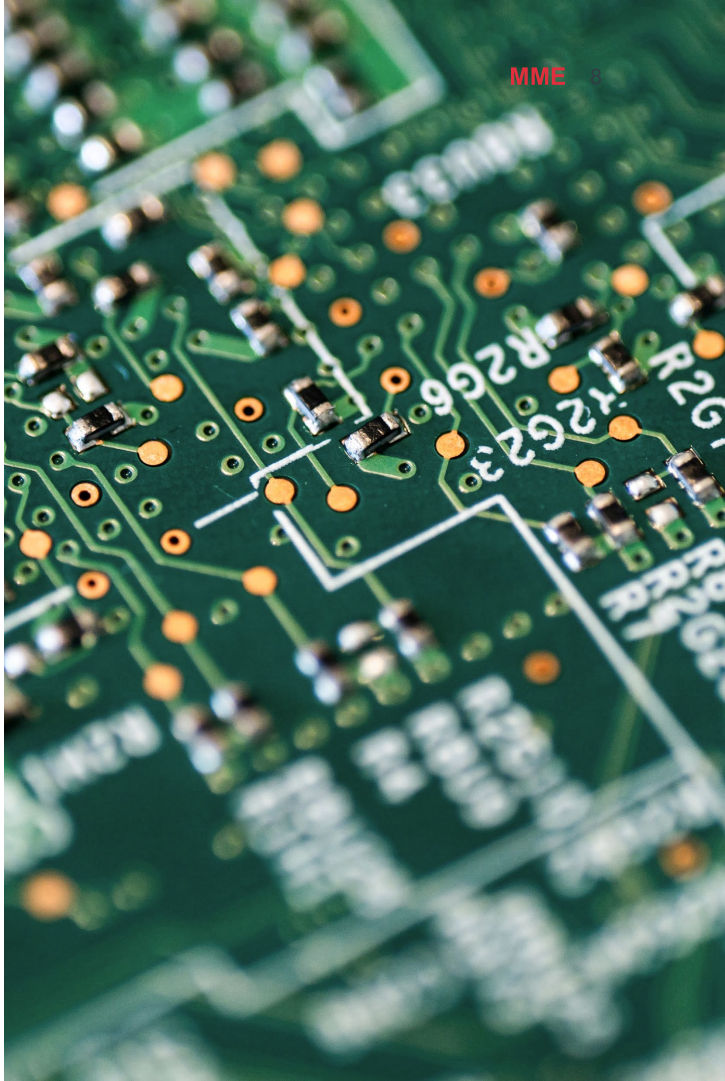
Zero-Knowledge Proofs

Sanctions Law

- **Scope:** No business with sanctioned individuals and entities.

- **Specific obligation by law:**
  - Obligation to identify customers before enter into a contract.

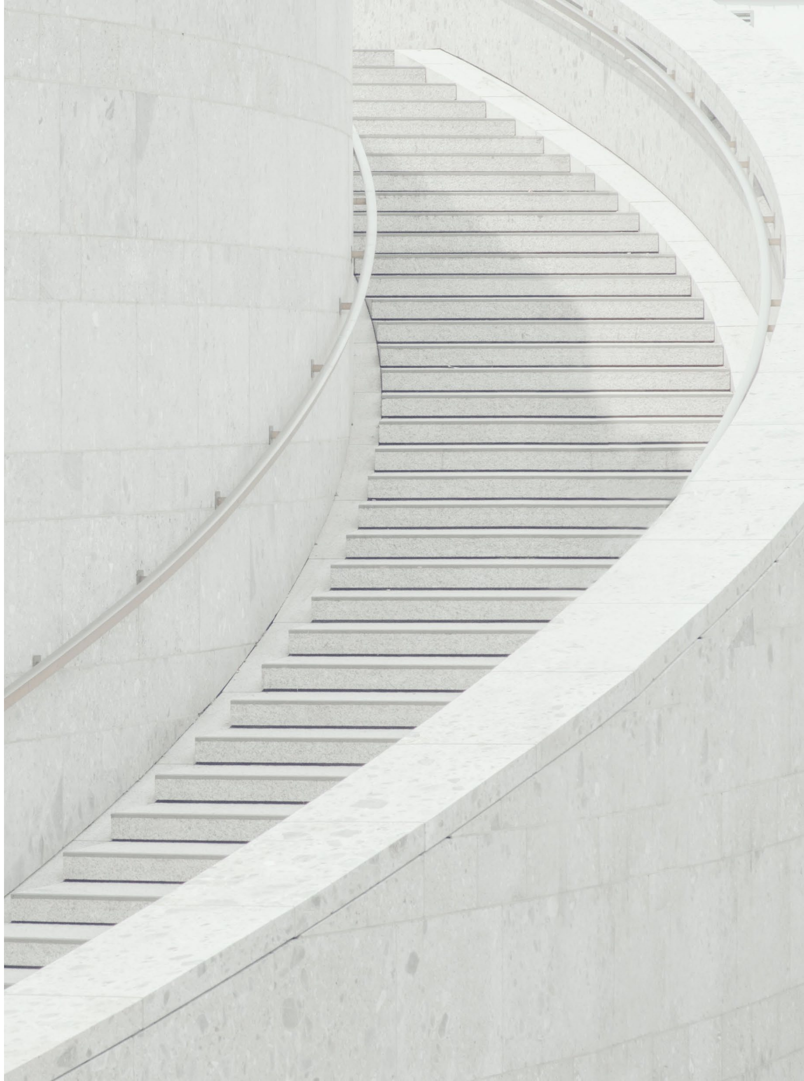
- **Zero-Knowledge Proofs as a solution to comply with sanction laws?**
  - Short answer: Yes



Sebastian Hepp

Conclusion and Outlook

- **Anti-Money Laundering Act:** Under the current Swiss AML regime the technology of ZKP is not applicable to perform KYC-checks on new customers (alternative approaches: compliance oracle and access to DeFi-protocols for regulated institutions).
- **Federal Act on Data Protection:** ZKPs are a very good solution to improve privacy in blockchain transactions.
- **Sanctions Law:** ZKP are also a very good solution to perform KYC-checks and onboard new customers in the unregulated sector (e.g. e-commerce).



Questions?

Sebastian Hepp

Attorney-at-Law

+41 44 254 99 66
sebastian.hepp@mme.ch

vCard

LinkedIn

MME

Office Zürich

MME Legal | Tax | Compliance
Zollstrasse 62
Postfach
CH-8031 Zürich

T +41 44 254 99 66
F +41 44 254 99 60

Office Zug

MME Legal | Tax | Compliance
Gubelstrasse 22
Postfach
CH-6302 Zug

T +41 41 726 99 66
F +41 41 726 99 60

office@mme.ch
www.mme.ch