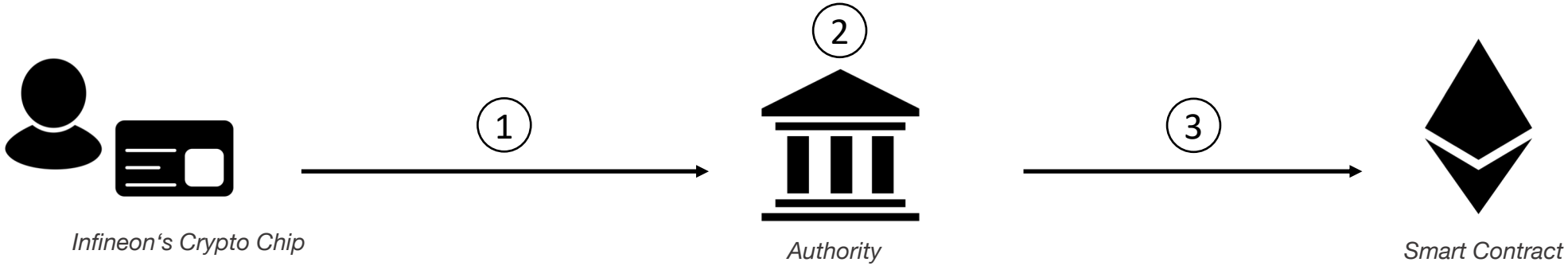
Your identification management with privacy by design

CURRENT PROBLEM

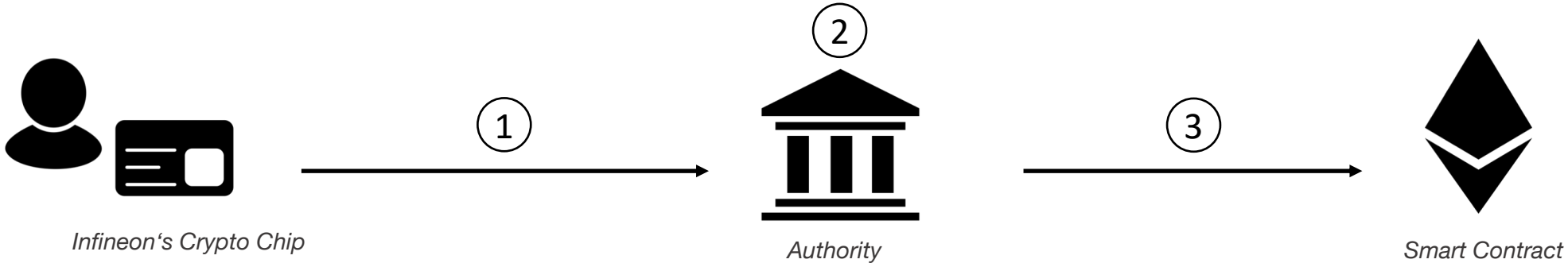
TECHNICAL OVERVIEW

User Authentication



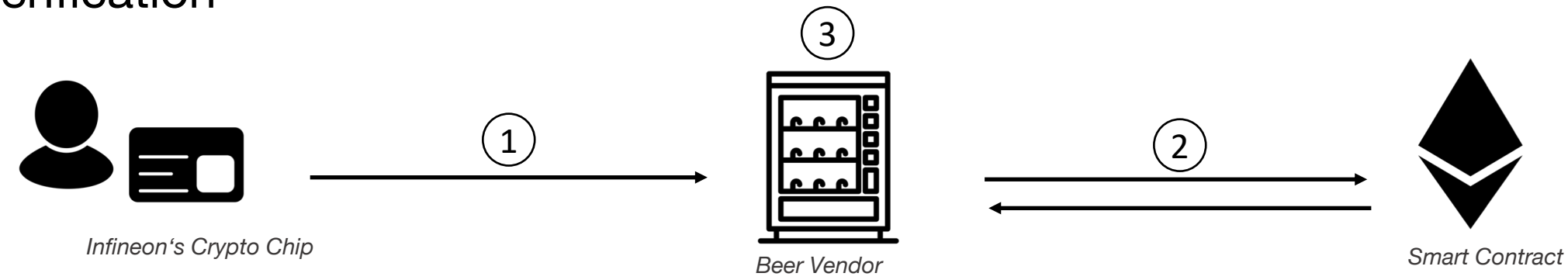
1. User identifies at a trusted authority
2. Authority generates Zero-Knowledge-Proof
   (Input = Public Key pairs from card)
3. Verification key + proof is published in IPFS
   Hashes are stored in Ethereum Smart Contract

User Authentication



1. User identifies at a trusted authority
2. Authority generates Zero-Knowledge-Proof
   (Input = Public Key pairs from card)
3. Verification key + proof is published in IPFS
   Hashes are stored in Ethereum Smart Contract

User Verification



1. User reveals public key at vending machine
2. Vending machine requests ZKP from Smart Contract / IPFS
3. Vending machine calculates proof (is person older than 18?)
   without knowing any personal data

LIVE DEMO

Q&A

….or let‘s go for a beer? ;-)