PIXI

A privacy centered adaptation of Montreal's BIXI system

TABLE OF CONTENTS

01. BIXI's LIMITATIONS

- Handle very sensitive data (geolocation, trip history)
- Not **Minimized**: Collects various lookup identifiers
- Account based system: No data **Separation**
- Widely used => impacts many people

➡ Crucial to improve the system

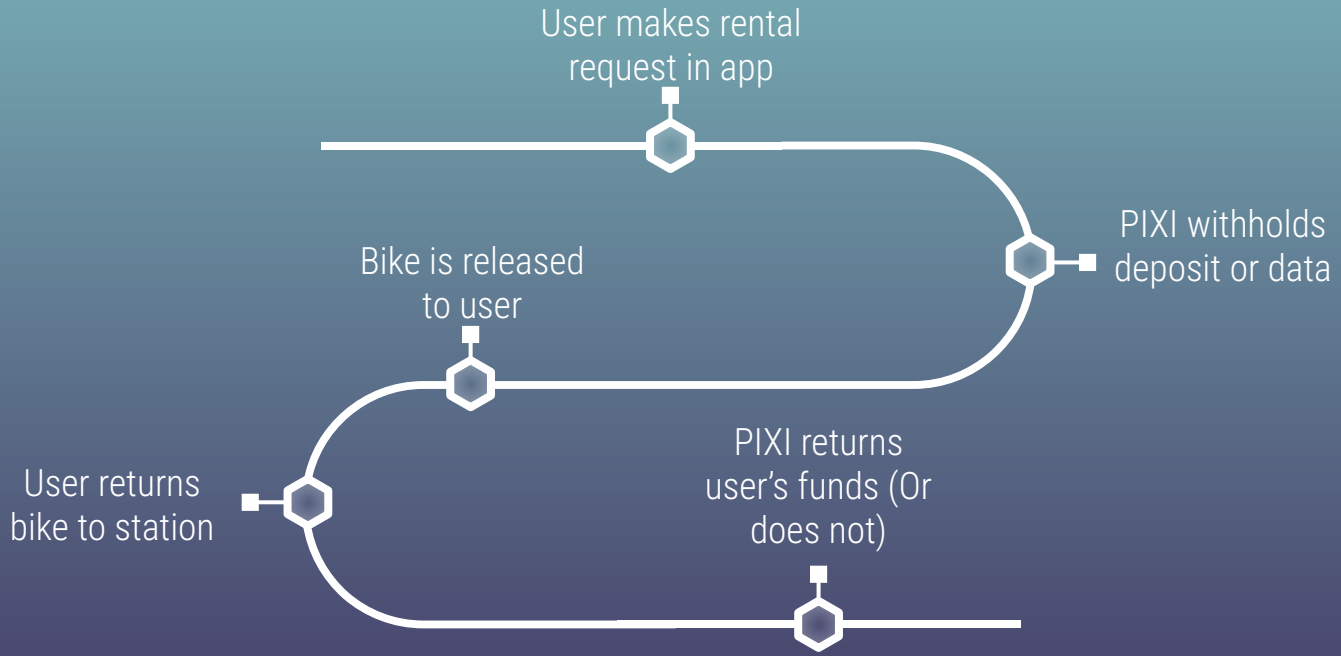
PIXI's REQUIREMENTS

- Anonymous users
- Unlinkability
- Bike theft is sufficiently discouraged => PIXI needs a collateral:
  - Deposit reimbursed when bike is returned.
  - Encrypted identifiers decryptable by PIXI iff contract is broken => Revocable privacy
- Service is user friendly

02

OVERVIEW OF PIXI

USER PIPELINE



KEY COMPONENTS

- Smart contract => Untamperable decentralized contract between user and PIXI
- Web app => Where users rent bikes.
- Metamask & Ether => Handle anonymous payments
- TEE & Asymmetric encryption => Enables revocable privacy

03

Technical presentations of third parties/systems used

I. ETHEREUM AND SMART CONTRACTS

- Ethereum is a public blockchain stored on a decentralized network of nodes across the globe that each hold a copy of the full chain.
  - Unmodifiable: The content of each block is hashed into all the subsequent ones
  - Transparent: All transactions are publicly accessible => anyone can verify the data, but also track wallet IDs making transactions

- Smart Contracts: self executing digital agreements deployed on a block of the ethereum blockchain.
  - Can be invoked by anyone at anytime with proper arguments
  - Cannot be tampered with once deployed

II. METAMASK

- MetaMask is a popular cryptocurrency wallet and gateway to blockchain-based applications
- No personal identifiers given by user during process-
- Private wallet key stored locally
- Open source
- Very user friendly => Accessible to non introduced users

III. Off-Chain Trusted Execution Environment (TEE)

- Known as enclave
- Cannot be altered externally (not even OS)
- Can store sensitive data (private key)
- Does not provide the transparency of the blockchain

04

DESIGN DECISIONS

The unlinkable payment problem

Goal: Anonymous and Unlinkable payment method.

Problem: Digicash ran out of cash => No perfect working solution.

With Ether/Metamask:
+ Fully anonymous
+ Can be unlinkable if user changes wallet each time
- Wallet address + balance made public
- Some latency in transactions

With regular Bank procedure:
- Each user is clearly identified
- Payments are always linkable
+ Transaction details and account balance remain private
+ Very fast transactions

The revocable privacy Problem

1. Users can't revoke access to personal data	2. Only PIXI can see data	3. Data accessible only if Bike is stolen
Copy of personal Data is sent through the smart contract.	All data entering smart contract is encrypted with PIXI's public key	Personal data is encrypted with TEE public key. Sent to TEE for decryption iff contract broken

Assumptions: Data is Verified, PIXI is not running the TEE

05

Rental Procedure

UNDER THE HOOD

INFORM
The web app receives bike availability data from smart contract

RENT
The user selects a bike to request rental

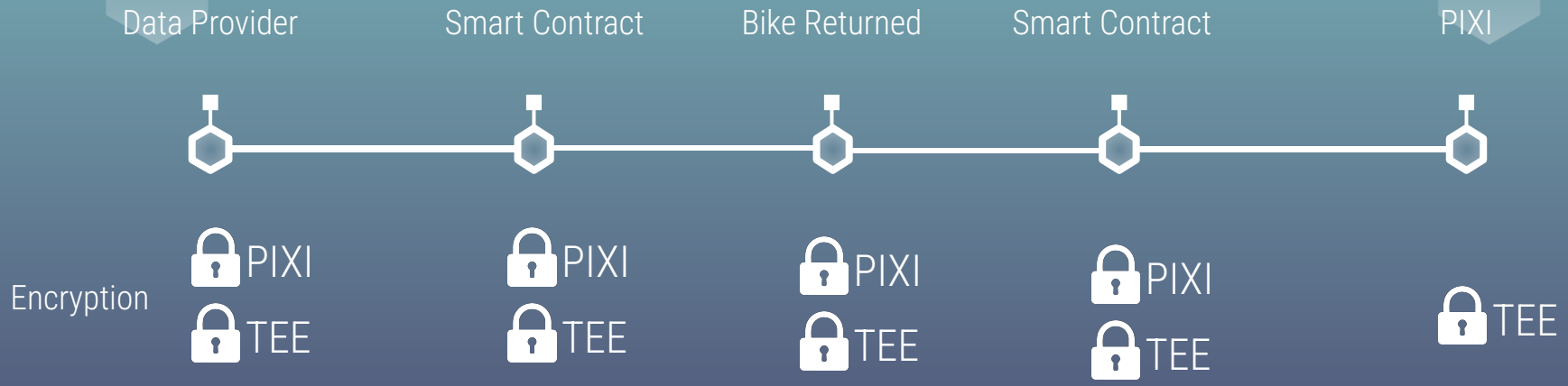
CONNECT
The JavaScript web app connects the user to the contract

CALL
The web app calls a function of the contract

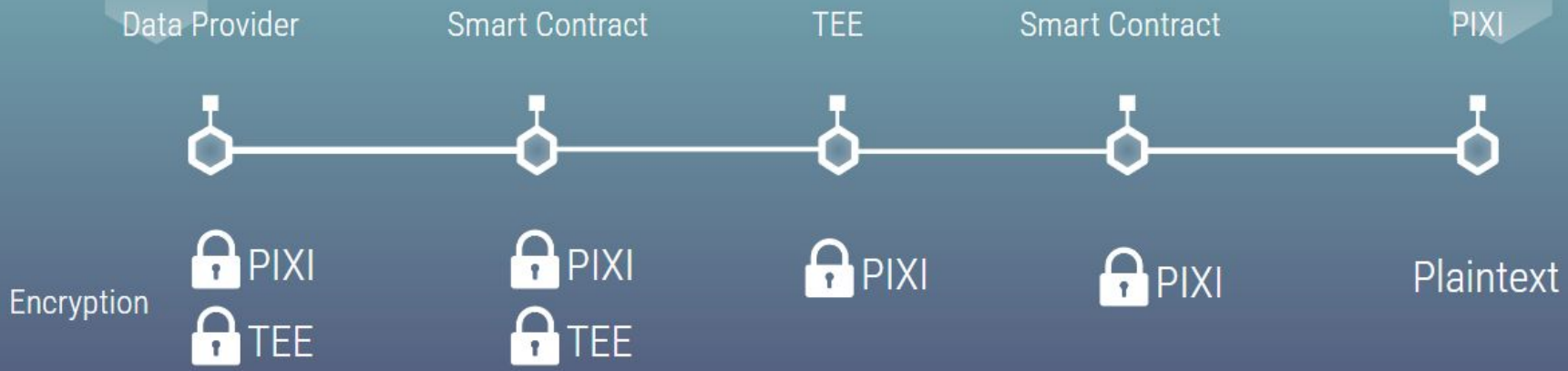
EXECUTE
The smart contract executes its predefined code

FINALIZE
The contract completes the transaction based on the user's actions

PERSONAL DATA FLOW I



PERSONAL DATA FLOW II



SUMMARY

What PIXI **stores**	What PIXI **could** see	What PIXI will **never** see
A bike was rented at station X at time T and returned at station Y at time T’	Wallet address corresponding to each trip (linkability).	Personal identifiers other than your wallet address (unless you steal a bike)

LIMITATIONS

- Slower response time
- Gas fees => more expensive
- Less user friendly experience (cryptocurrency)
- Validator problem

06

LIVE DEMO TIME!!