IOTWeek

Dublin —— June 20-23, 2022

I3-MARKET
Wallets, Secure Auditing, Blockchain Network

Juan HERNÁNDEZ SERRANO
Rafael GENÉS DURÁN
Fernando ROMÁN GARCÍA

GLOBAL VISION:
IoT TODAY AND BEYOND

IOTForum

Why blockchain (distributed ledger)?

- Cryptocurrency?
- Reliable, distributed infrastructure for managing identities
  - The path for Self-Sovereign Identity
- Reliable ledger/notarisation
  - Auditable accounting system
    - E.g. access to sensitive data, explicit-user consents
  - Non-repudiation protocol for data exchanges
    - Fair billing even with fiat money

Self-Sovereign Identities:
- Decentralized Identifiers
- Verifiable Credentials
- Selective Disclosure

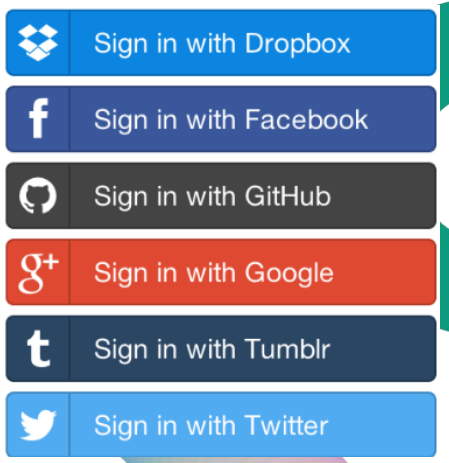
blockchain

Auditable Accounting

The problem with online identities

- People have many online personas at many organizations

- Federated auth. (OAuth2, OIDC) partially solves the problem
  - IdPs manage user identities
    - censorship
    - surveillance → bad for privacy!



- However, most of the online personas are bounded to users' identifiers not controlled by themselves:
  - Email accounts
  - Telephone numbers

SSI: give control back to users

- Users have a stable identifier created and managed by themselves.
  - This identifier can be resolved/used to retrieve user identity data

Method | Method-Specific Identifier

`did:ethr:0xb9c5714089478a327f09197987f16f9e5d936e8a`

  - A smart contract can be used to manage how to resolve the DID to a DID document
- manage (verifiable) claims about their identity which are issued against a managed DID

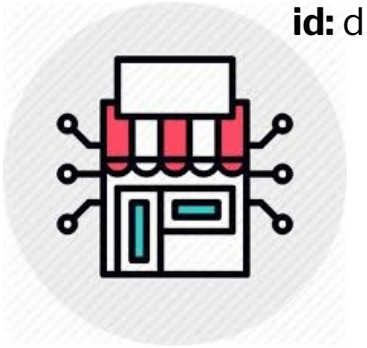
Issuer: did:ethr:0xk7bhac37c498d8e2386....
Subject: did:ethr:0xf3beacff02a498d93f79a....
Role: Car-data seller

- manage what information to share at every interaction (selective disclosure)

Self-Sovereign Identity

IOTWeek
Dublin — June 20-23, 2022

Credential Issuer



id: did:ethr:0xf7b34fe37c...

Claim Holder

Issuer: did:ethr:0xf7b34fe37c...
Subject: did:ethr:0xf3beacff02....
Role: i3-MARKET consumer
Name: Mario
Surname: Rossi
Country: Italy
Age: 58
Proof: 0x7662f1ea3250b...

WALLET

did1: did:ethr:0xf3beacff02....
privKey1: 0x75eae41782e0...
verifiableCredentials1:

did2: did:ethr:0x1976efb34....
privKey2: 0x9841f975ee7c...
verifiableCredentials2:

SSI Selective Disclosure

Claim Holder

Data Provider
(Claim Verifier)

Distributed Ledger
DID-Resolver's
Smart Contract

SDR: I3-market consumer?

Get pubKey1 from
0xf3beacff02a4....

Verify vp
with pubKey1

Get issuer's pubKey
from 0xf7b34fe37c...

Verify vc with
issuer's pubKey

Verifiable Presentation

did:ethr: 0xf3beacff02a4....

Issuer: did:ethr: :0xf7b34fe37c...
Subject: did:ethr:0xf3beacff02....
Role: i3-MARKET consumer

Signed with
privKey1

WALLET

did1: did:ethr: 0xf3beacff02....
privKey1: 0x75eae41782e0...
verifiableCredentials1:

did2: did:ethr: 0x1976efb34....
privKey2: 0x9841f975ee7c...
verifiableCredentials2:

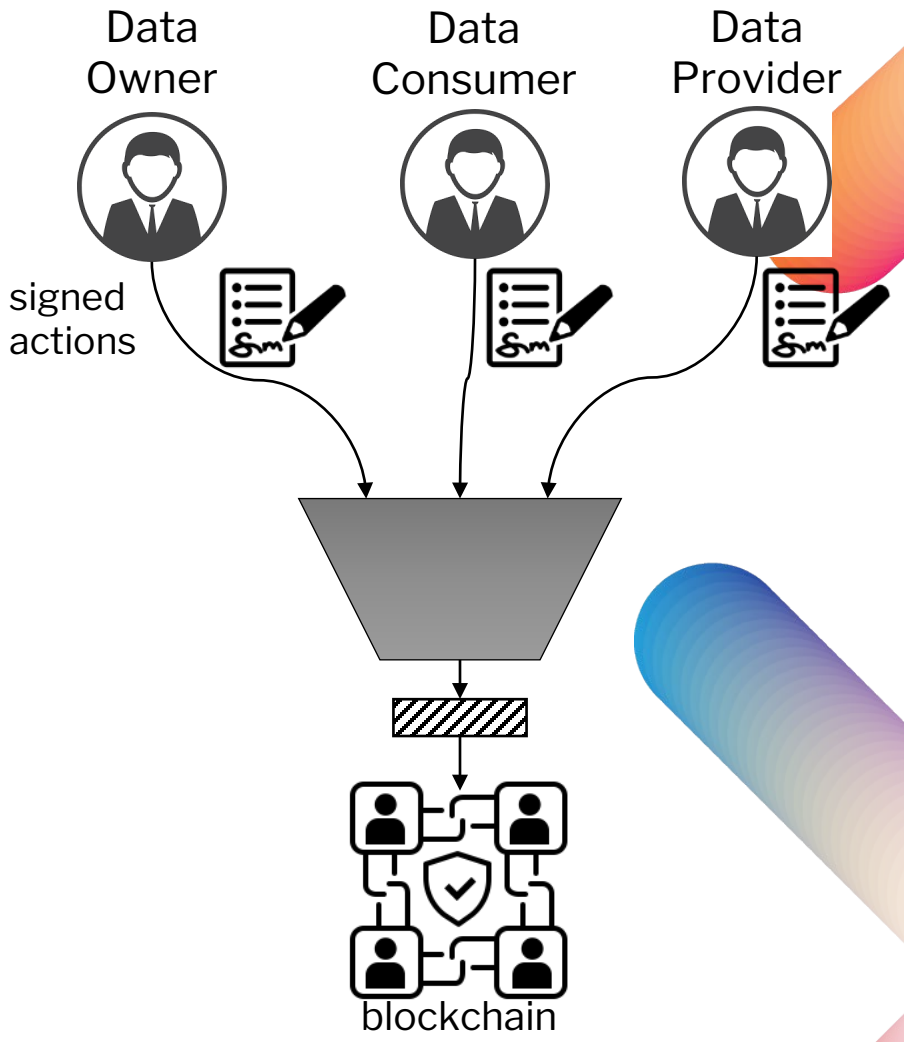
i3-MARKET Wallet

- I3-MARKET Wallet is a desktop application that can be securely paired with any other desktop app or SPA
- Working functionalities:
  - Create/manage multiple wallet instances using multiple DLTs (including i3-MARKET BESU)
  - Create/manage identities (DIDs)
  - Securely store verifiable credentials
  - Selectively disclose verifiable credentials
  - Integration with i3-MARKET OIDC flow.
  - Secure pairing protocol
- On-going work:
  - Integration with IDEMIA HW Wallet.
  - Secure cloud backup (Cloud Secure Vault)

More info: https://github.com/i3-Market-V2-Public-Repository/SP3-SCGBSSW-I3mWalletMonorepo

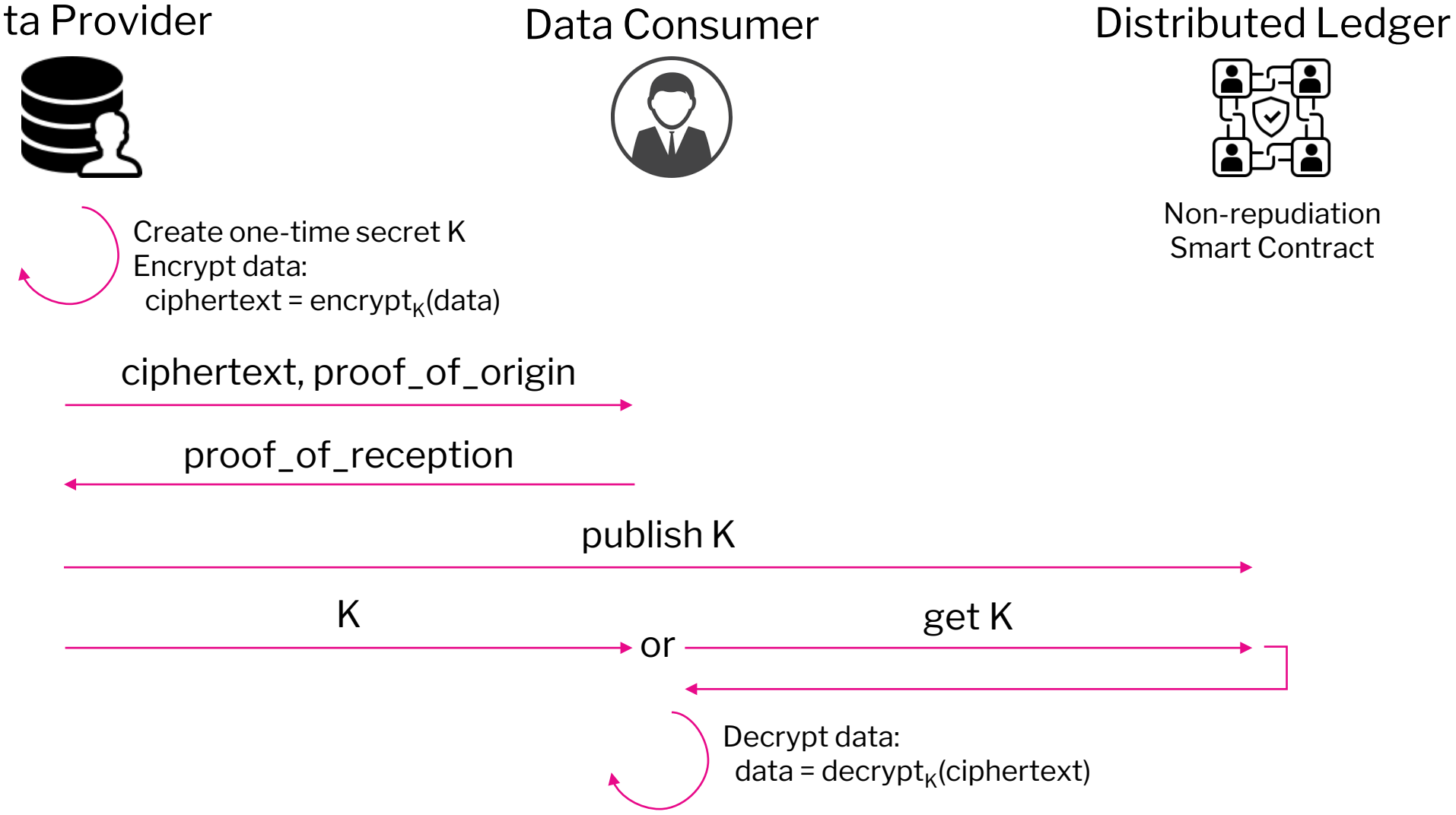
Auditable Accounting

- Accounting of selected operations:
  - Access, modification, deletion of sensitive data
  - Payment data
  - Contractual agreements
- Reliable, privacy-guaranteed proofs of data exchange will support any future claim regarding a data trade
- Proofs cannot be repudiated by the involved stake holders
- Backed up by a public blockchain the accounting cannot can not be faked or tampered



More info: https://github.com/i3-Market-V2-Public-Repository/SP3-SCGBSSW-AA-AuditableAccounting

Non-repudiation protocol



More info: https://github.com/i3-Market-V2-Public-Repository/SP3-SCGBSSW-CR-Documentation

IOTWeek

Dublin — June 20-23, 2022

Thank you!

Find more:

https://www.i3-market.eu/

https://github.com/i3-Market-V2-Public-Repository

iotweek.org