Techniques to Bootstrap a Verifiable Notion of Identity

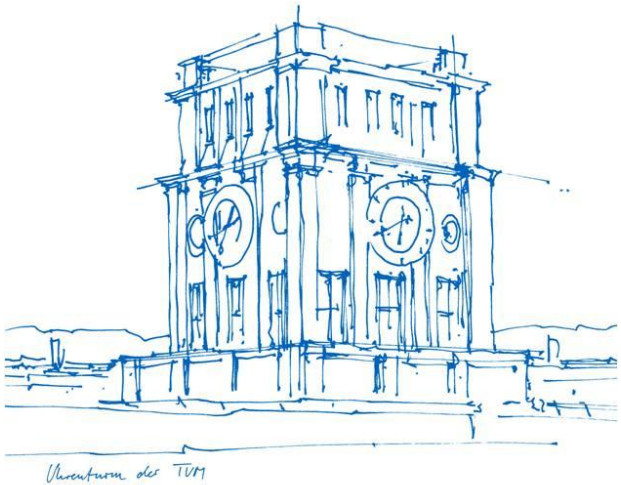
Jan Lauinger

Technical University of Munich

TUM Department of Electrical and Computer Engineering

Associate Professorship of Embedded Systems and Internet of Things

Munich, April 2023



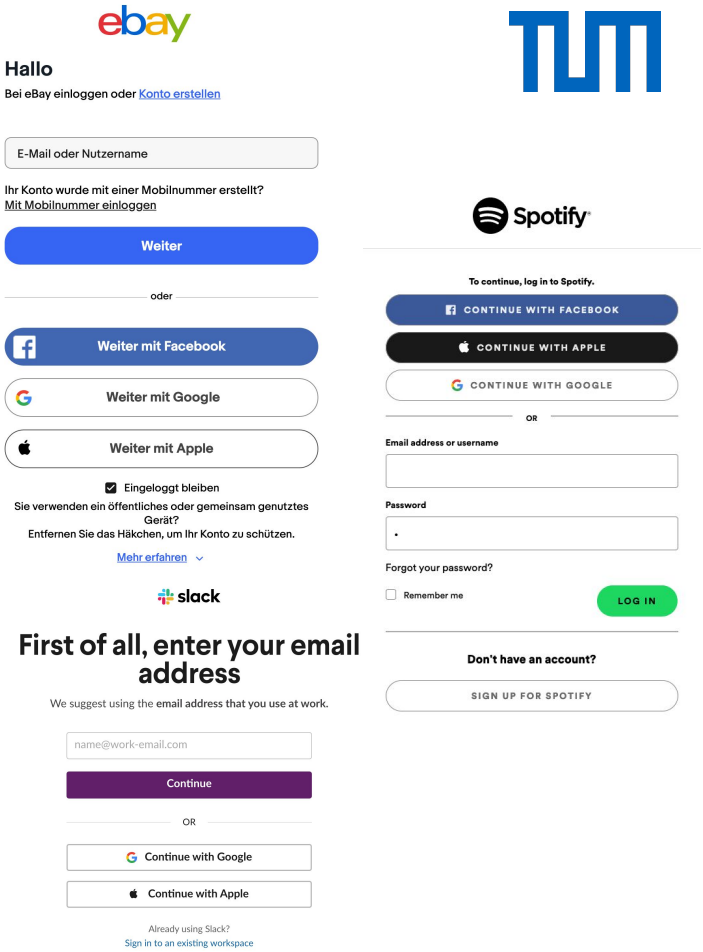
Current Situation

Who controls our digital identity today and how?

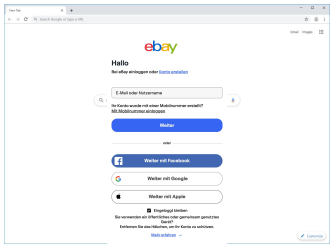
Single Sign-on (SSO)

1. Register at identity provider (IP) (e.g. Google)
2. Use IP to login at other services

- You share your credentials only with one IP
- Convenient as users only maintain one account



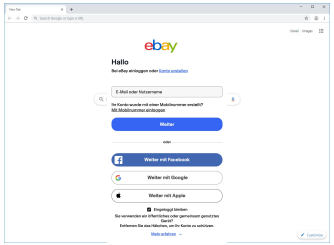
Open Authorization (OAuth 2.0) + OpenID



Resource Owner

1. Login with Google

Open Authorization (OAuth 2.0) + OpenID



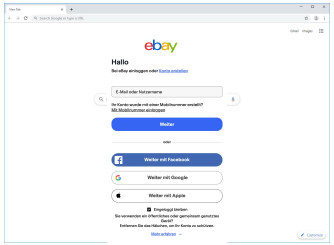
Resource Owner

1. Login with Google

2. Redirect to Google

Identity Service

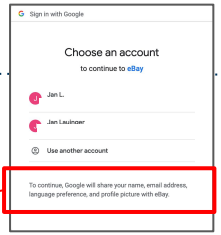
Open Authorization (OAuth 2.0) + OpenID



Resource Owner

1. Login with Google

ebay



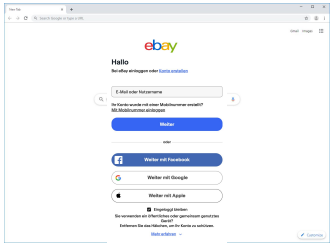
2. Redirect to Google

3. Share Login Prompt

Identity Service

To continue, Google will share your name, email address, language preference, and profile picture with eBay.

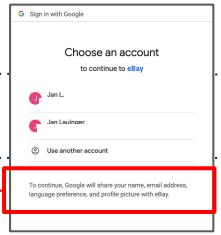
Open Authorization (OAuth 2.0) + OpenID



Resource Owner

1. Login with Google

2. Redirect to Google



3. Share Login Prompt

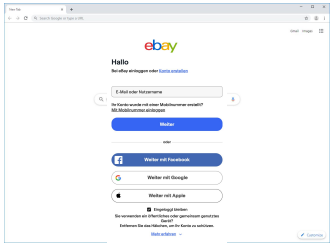
5. Enter credentials

6. Verify credentials

Identity Service

To continue, Google will share your name, email address, language preference, and profile picture with eBay.

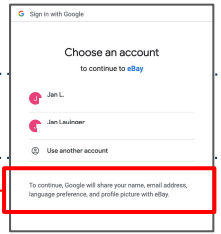
Open Authorization (OAuth 2.0) + OpenID



Resource Owner

1. Login with Google

2. Redirect to Google



3. Share Login Prompt

5. Enter credentials

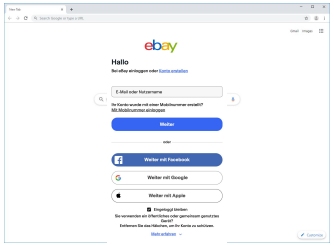
6. Verify credentials

7. Access token (OAuth), ID token/JWT (OpenID)

Identity Service

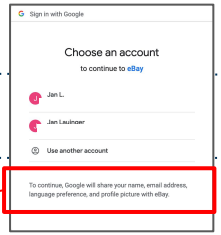
To continue, Google will share your name, email address, language preference, and profile picture with eBay.

Open Authorization (OAuth 2.0) + OpenID



Resource Owner

1. Login with Google



2. Redirect to Google

3. Share Login Prompt

5. Enter credentials

6. Verify credentials

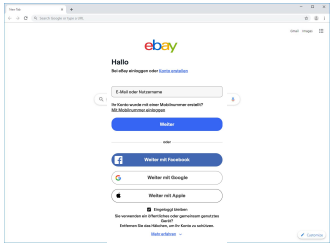
7. Access token (OAuth), ID token/JWT (OpenID)

Identity Service

To continue, Google will share your name, email address, language preference, and profile picture with eBay.

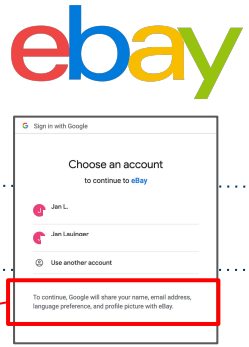
8. Reload (+Token)

Open Authorization (OAuth 2.0) + OpenID



Resource Owner

1. Login with Google



2. Redirect to Google

3. Share Login Prompt

5. Enter credentials

6. Verify credentials

Identity Service

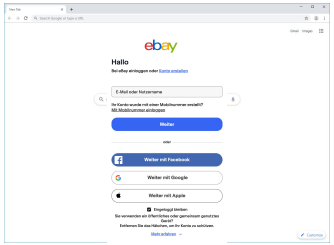
7. Access token (OAuth), ID token/JWT (OpenID)

To continue, Google will share your name, email address, language preference, and profile picture with eBay.

9. Authenticate with ID token

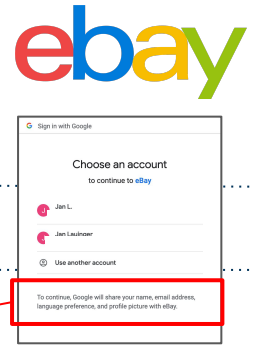
8. Reload (+Token)

Open Authorization (OAuth 2.0) + OpenID



Resource Owner

1. Login with Google



2. Redirect to Google

3. Share Login Prompt

5. Enter credentials

6. Verify credentials

Identity Service

7. Access token (OAuth), ID token/JWT (OpenID)

To continue, Google will share your name, email address, language preference, and profile picture with eBay.

9. Authenticate with ID token

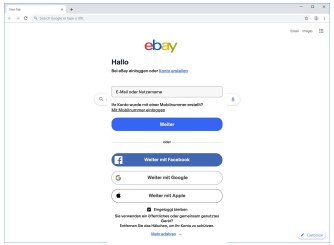
8. Reload (+Token)

ebay

9. Request resource with access token

Resource Service

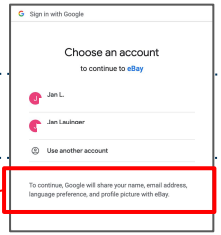
Open Authorization (OAuth 2.0) + OpenID



Resource Owner

1. Login with Google

2. Redirect to Google



3. Share Login Prompt

5. Enter credentials

6. Verify credentials

Identity Service

7. Access token (OAuth), ID token/JWT (OpenID)

To continue, Google will share your name, email address, language preference, and profile picture with eBay.

9. Authenticate with ID token

9. Request resource with access token

8. Reload (+Token)

Resource Service

11. Show data + session cookie

10. Share data

Problems

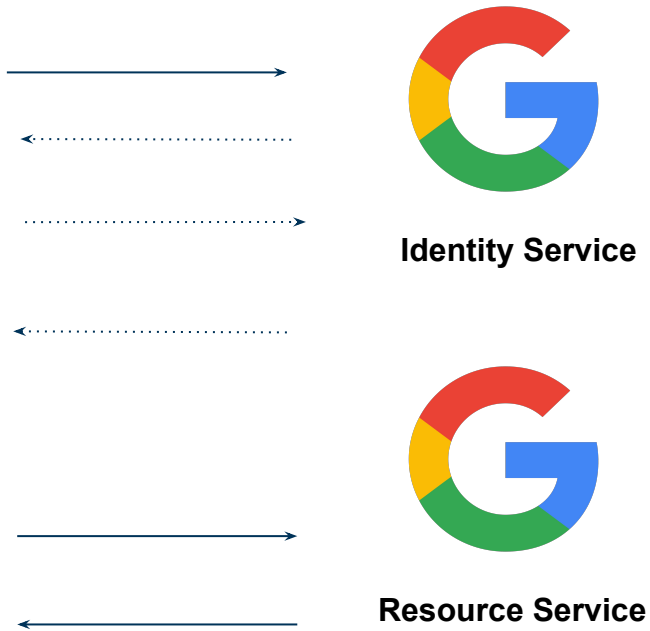
- **Control**: Fixed data policies
- **Verifiability**: Intransparent data access & data analytics
- **Security & privacy**: Data breaches & tracking

Problems

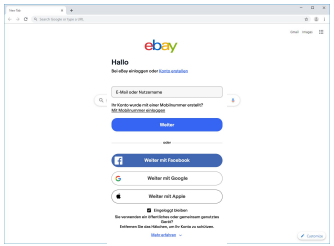
- **Control**: Fixed data policies
- **Verifiability**: Intransparent data access & data analytics
- **Security & privacy**: Data breaches & tracking

What we want instead:

- Control of identifiers, control of data policies
- Transparent access logs
- Verifiable policy-compliant computation
- No data breaches
- Provision of verifiable data



Question: Improving Centralized Infrastructure



Resource Owner

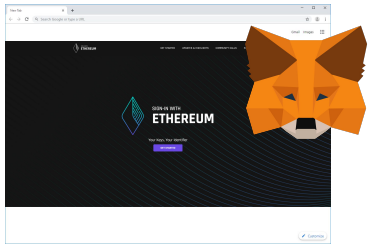
Identity Service

Use my identity provider

Resource Consumer

Resource Service

Question: Using Decentralized Approaches



Resource Owner

Identity Service

Use my blockchain address

Resource Consumer

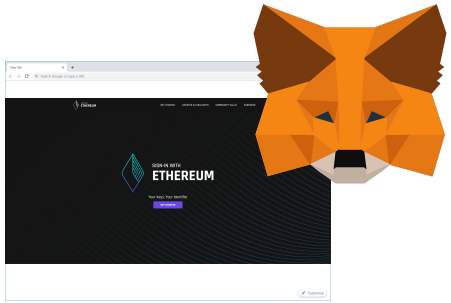
IPFS

Resource Service

Bootstrapping a Decentralized Identity

Which techniques are required?

Wallets

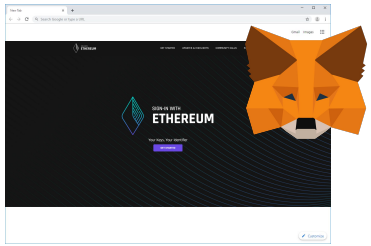


Resource Owner

- Custodial vs non-custodial wallets

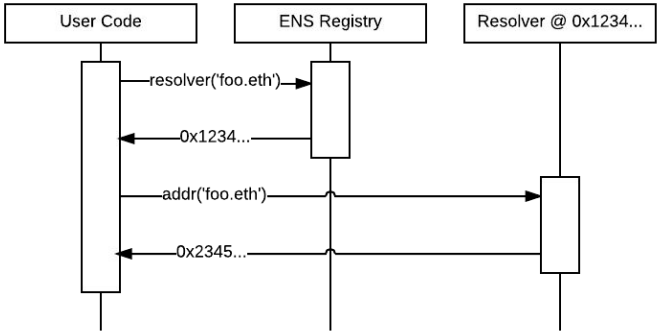
Usenix 23: MFKDF for Fast, Flexible, Secure, & Practical Key Management

On-chain Accounts



Resource Owner

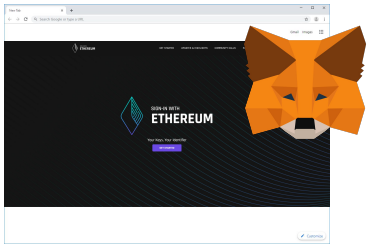
Identity Service



- Registry contracts & Resolver contracts
- Privacy-preserving on-chain states & policies

Preprint 23: Zero-Knowledge Address Abstraction

Decentralized Storage Networks



Resource Owner

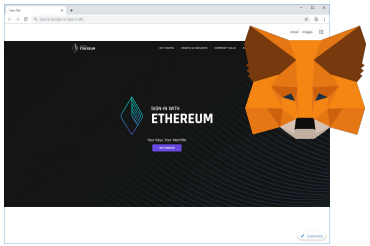
- Store encrypted data

IPFS

Resource Service

Usenix 16: Sieve; Usenix 20: Droplet

Decentralized Identity



Resource Owner

Identity Service

Use my blockchain address

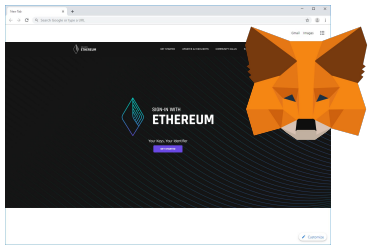
Resource Consumer

Resource Service

Taking the next step

What do we need on top of decentralized identity?

Decentralized Secret Management



Resource Owner

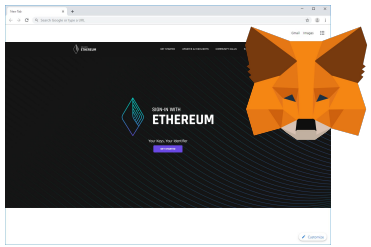
Identity Service

Secret Management Committee

Resource Service

TCC 20: Can a public blockchain keep a secret?

Decentralized Access Control



Resource Owner

Identity Service

Secret Management Committee

Resource Consumer

IPFS

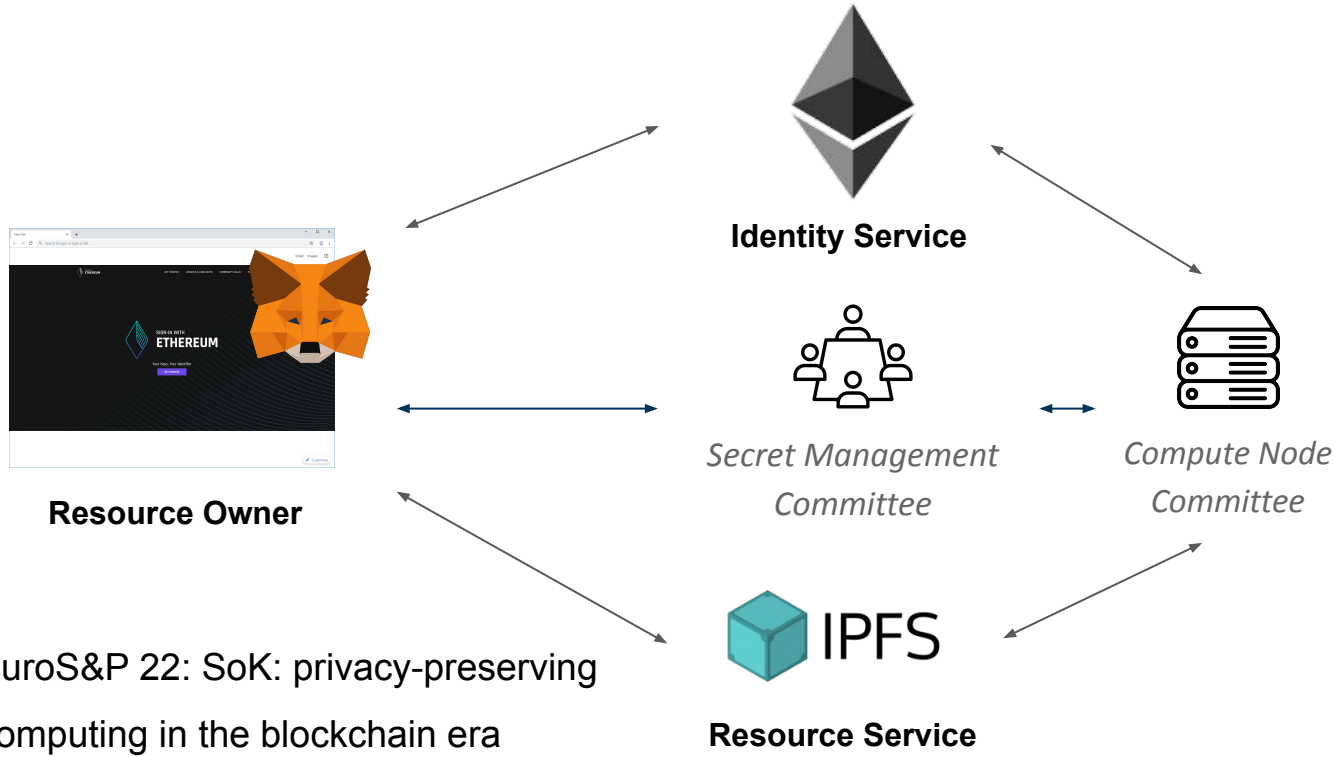
Resource Service

VLDB 21: Calypso;

Going Beyond

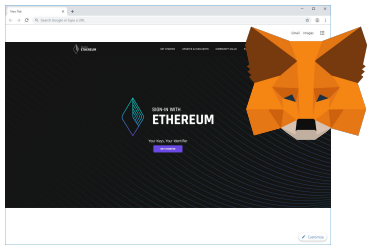
Can we achieve something even better, e.g. full data sovereignty?

Decentralized Secure Computation



EuroS&P 22: SoK: privacy-preserving computing in the blockchain era

Decentralized Policy-compliant Computation



Resource Owner

Identity Service

Secret Management Committee

Compute Node Committee

Resource Consumer

IPFS

Resource Service

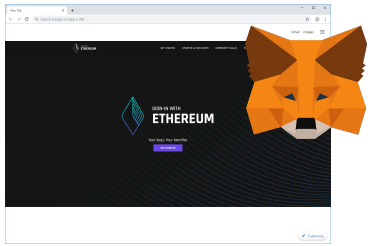
S&P 16: Hawk; EuroS&P 19: Ekiden;

EuroS&P 21: Publicly Auditable MPCaaS;

So far so good

- Control of identifiers, control of data policies
- Transparent access logs
- Verifiable policy-compliant computation
- No data breaches
- Provision of verifiable data

Something is missing



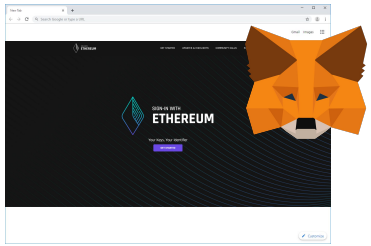
Resource Owner

Is the data we provide authentic and trustworthy?

IPFS

Resource Service

Ebay Seller KYC



Resource Owner

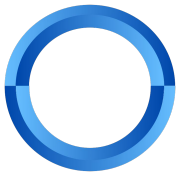
Please share your proof of address & age.

Resource Consumer

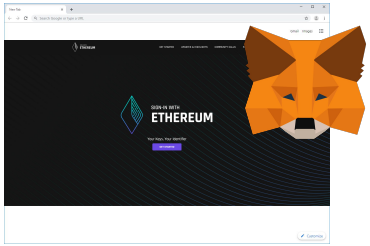
IPFS

Resource Service

Data Provenance Oracles

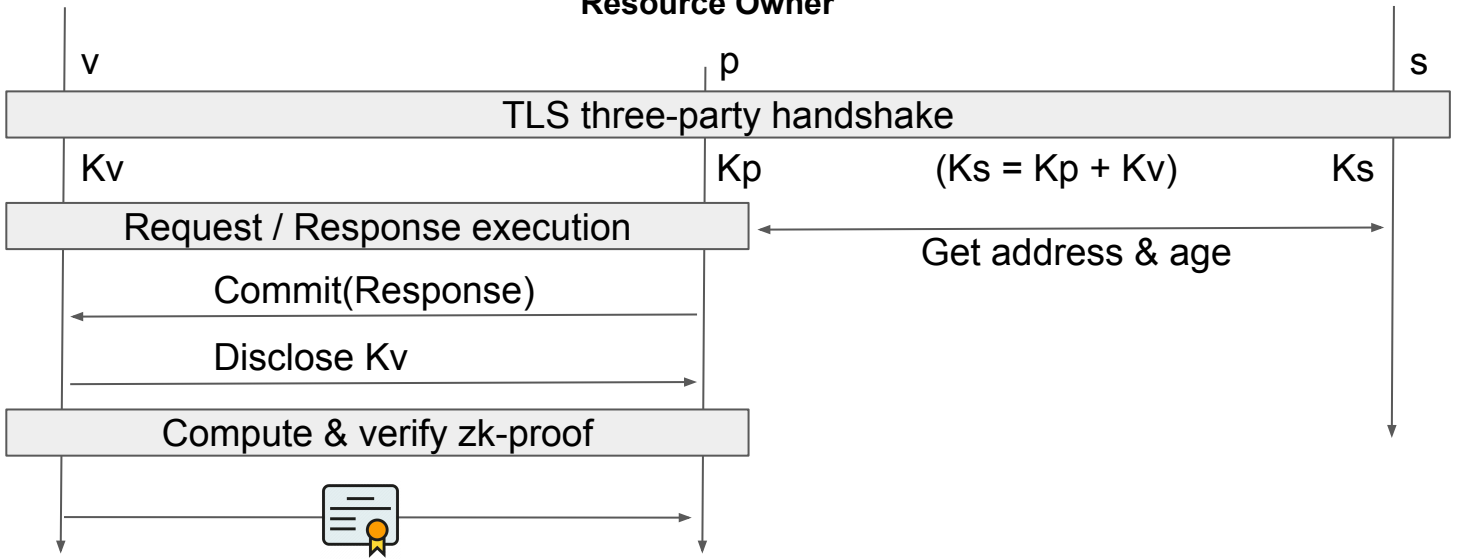


Oracle Verifier

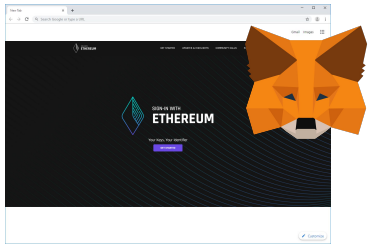


Resource Owner

Trusted Data Provider



Ebay Seller KYC

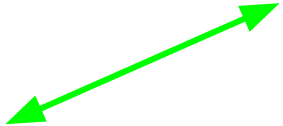


Resource Owner

Address verified.

- Provision of verifiable data

Resource Service



ebay

Resource Consumer

Data Provenance Oracles

- Software based vs hardware based oracles, privacy-preserving oracles
- Server attested data vs verifier-based data attestation
- On-chain vs external oracles

TLSNotary; CCS 16: Town Crier; NDSS 18: TLS-N; CCS 20: DECO; S&P 21: Candid

If you are interested, please contact & monitor us

SoK: Data Sovereignty

Jens Ernstberger [†‡‡], Jan Lauinger [†], Fatima Elsheimy [‡], Liyi Zhou [§‡‡],
Sebastian Steinhorst [†], Ran Canetti [¶], Andrew Miller [‖], Arthur Gervais [**‡‡], Dawn Song [††‡‡]
[†]*Technical University of Munich, Germany*
[‡]*Yale University, United States*
[§]*Imperial College London, United Kingdom*
[¶]*Boston University, United States*
[‖]*University of Illinois at Urbana-Champaign, United States*
[**]*University College London, United Kingdom*
[††]*University of California, Berkeley, United States*
[‡‡]*Berkeley Center for Responsible, Decentralized Intelligence (RDI)*

This year @EuroS&P 23: SoK Data Sovereignty

Github repository: web3knowledge

Upcoming work on TLS oracles…

Contact: jens.ernstberger@tum.de, jan.lauinger@tum.de

Thank you for listening

Questions?