

# Techniques to Bootstrap a Verifiable Notion of Identity

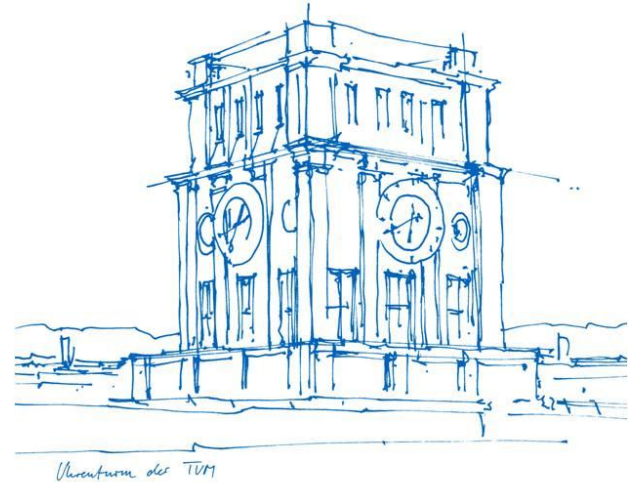
**Jan Lauinger**

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?

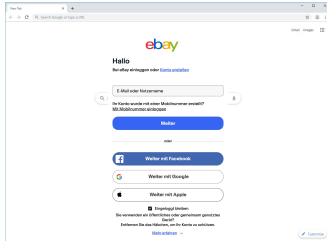
# Single Sign-on (SSO)

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

The screenshot shows the eBay login interface. At the top is the eBay logo. Below it, the text reads "Hallo" and "Bei eBay einloggen oder [Konto erstellen](#)". There is a text input field for "E-Mail oder Nutzername". Below that, a message states "Ihr Konto wurde mit einer Mobilnummer erstellt? [Mit Mobilnummer einloggen](#)". A large blue button labeled "Weiter" is present. Below this is a horizontal line with "oder" in the center. There are four buttons for social login: "Weiter mit Facebook", "Weiter mit Google", "Weiter mit Apple", and "Weiter mit Slack". A checkbox labeled "Eingeloggt bleiben" is checked. Below it, text says "Sie verwenden ein öffentliches oder gemeinsam genutztes Gerät? Entfernen Sie das Häkchen, um Ihr Konto zu schützen." with a link "Mehr erfahren". At the bottom, the Slack logo is shown, followed by the heading "First of all, enter your email address" and the subtext "We suggest using the email address that you use at work." There is a text input field with "name@work-email.com" and a purple "Continue" button. Below that is another "OR" separator and two buttons: "Continue with Google" and "Continue with Apple". At the very bottom, it says "Already using Slack? [Sign in to an existing workspace](#)".

The screenshot shows the Spotify login interface. At the top right is the TUM logo. Below it is the Spotify logo. A message says "To continue, log in to Spotify." There are three buttons for social login: "CONTINUE WITH FACEBOOK", "CONTINUE WITH APPLE", and "CONTINUE WITH GOOGLE". Below these is a horizontal line with "OR" in the center. There are two input fields: "Email address or username" and "Password". Below the password field is a link "Forgot your password?". There is a checkbox "Remember me" and a green "LOG IN" button. At the bottom, there is a link "Don't have an account?" and a button "SIGN UP FOR SPOTIFY".

# Open Authorization (OAuth 2.0) + OpenID

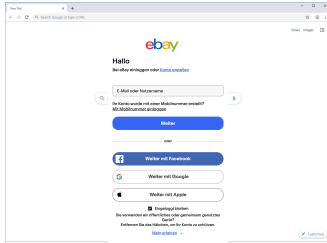


1. Login with Google



**Resource Owner**

# Open Authorization (OAuth 2.0) + OpenID



**Resource Owner**

1. Login with Google

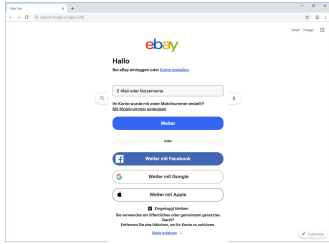


2. Redirect to Google



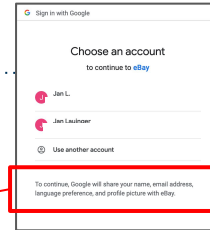
**Identity Service**

# Open Authorization (OAuth 2.0) + OpenID



**Resource Owner**

1. Login with Google



2. Redirect to Google

3. Share Login Prompt

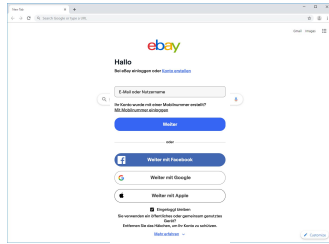


**Identity Service**



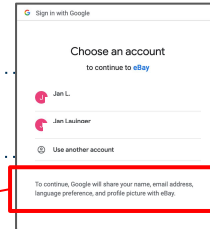
To continue, Google will share your name, email address, language preference, and profile picture with eBay.

# Open Authorization (OAuth 2.0) + OpenID



**Resource Owner**

1. Login with Google



5. Enter credentials



2. Redirect to Google



3. Share Login Prompt



6. Verify credentials

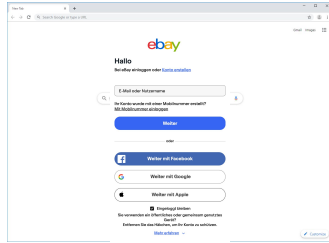


**Identity Service**



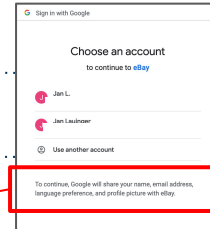
To continue, Google will share your name, email address, language preference, and profile picture with eBay.

# Open Authorization (OAuth 2.0) + OpenID



**Resource Owner**

1. Login with Google



5. Enter credentials



2. Redirect to Google



3. Share Login Prompt



6. Verify credentials



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



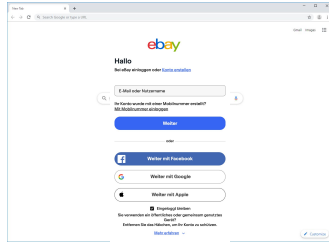
**Identity Service**



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

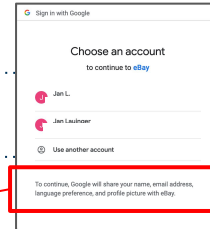


# Open Authorization (OAuth 2.0) + OpenID



**Resource Owner**

1. Login with Google



5. Enter credentials



2. Redirect to Google



3. Share Login Prompt



6. Verify credentials



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



**Identity Service**

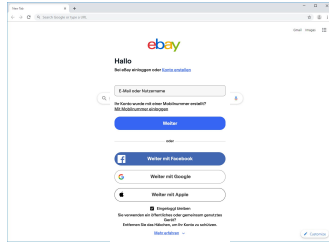


To continue, Google will share your name, email address,  
language preference, and profile picture with eBay.

8. Reload (+Token)



# Open Authorization (OAuth 2.0) + OpenID

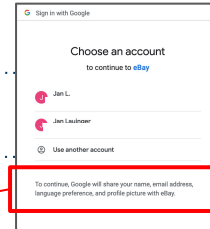


**Resource Owner**

1. Login with Google



2. Redirect to Google



3. Share Login Prompt

5. Enter credentials

6. Verify credentials

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



**Identity Service**

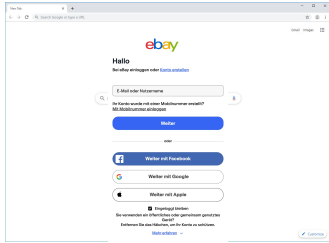
9. Authenticate with  
ID token

8. Reload (+Token)



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

# Open Authorization (OAuth 2.0) + OpenID

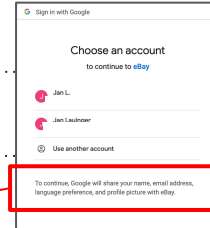


**Resource Owner**

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**

9. Authenticate with  
ID token

9. Request resource  
with access token

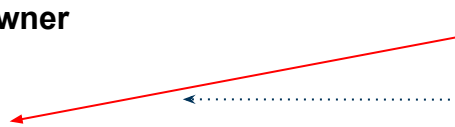


**Resource Service**

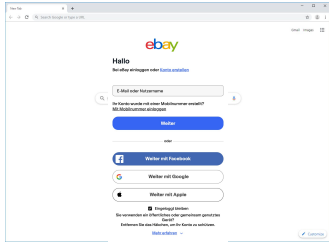
8. Reload (+Token)



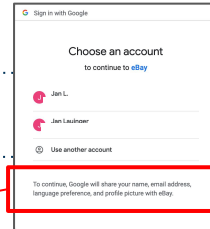
To continue, Google will share your name, email address,  
language preference, and profile picture with eBay.



# 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.

9. Authenticate with  
ID token

9. Request resource  
with access token

8. Reload (+Token)



10. Share data

11. Show data + session cookie



**Resource Service**

# Problems

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



**Identity Service**



**Resource Service**

# 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

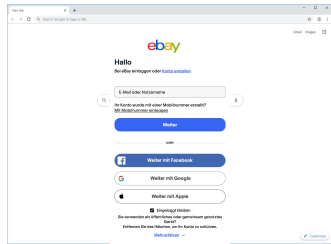


**Identity Service**



**Resource Service**

# Question: Improving Centralized Infrastructure



Resource Owner



Identity Service

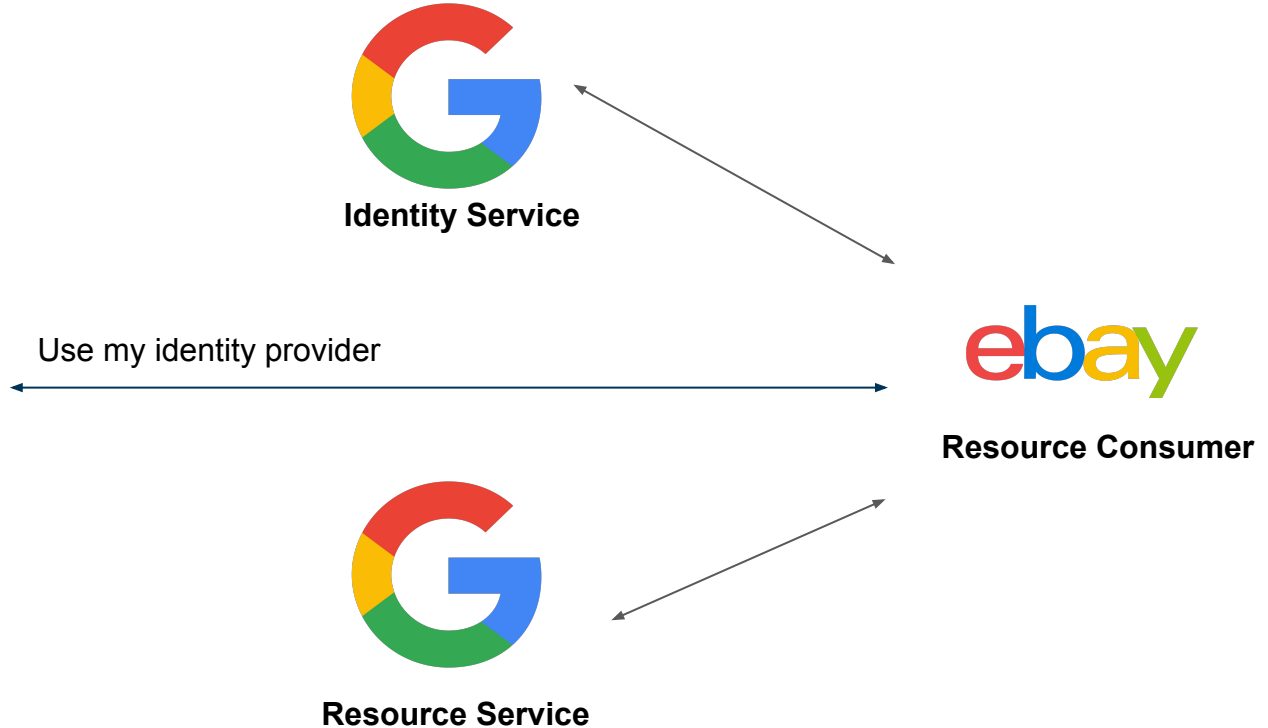
Use my identity provider



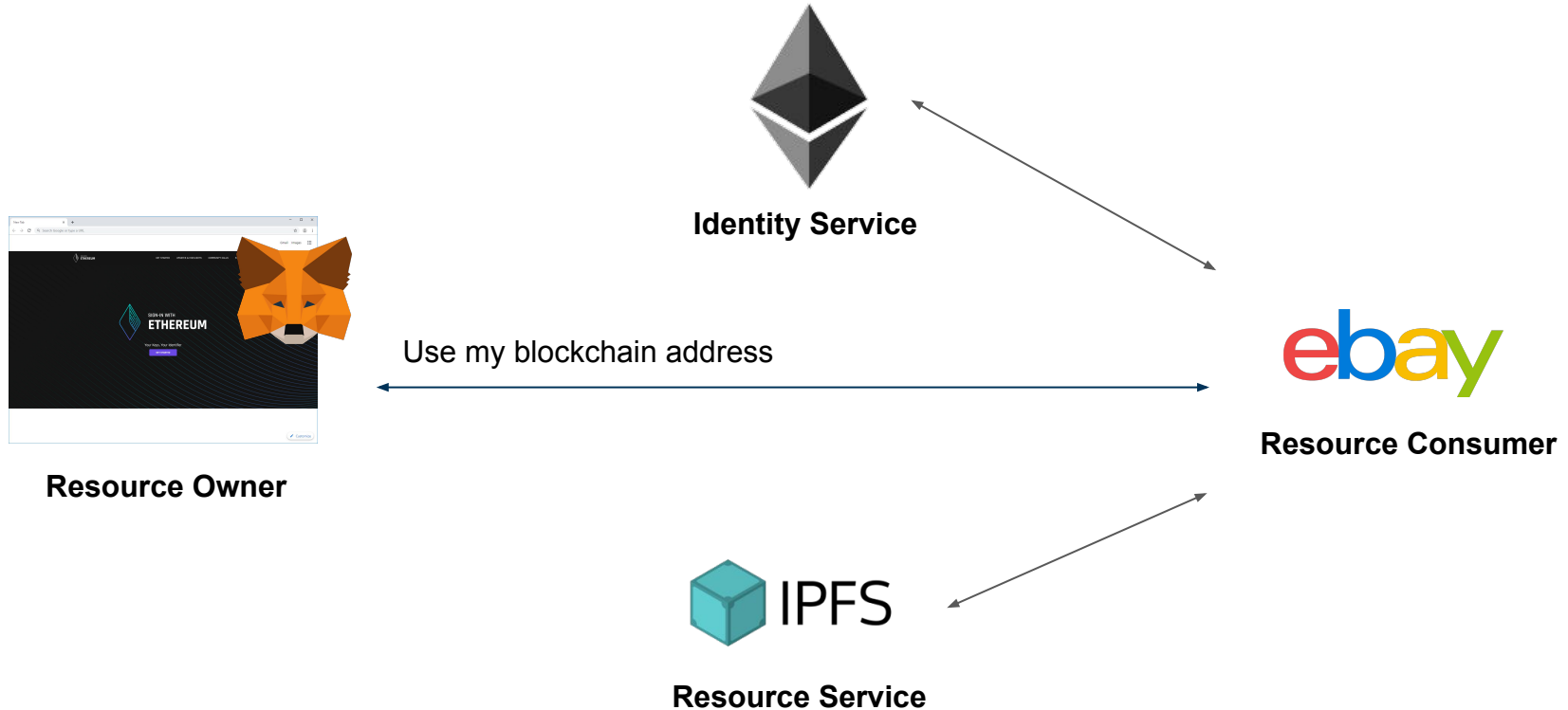
Resource Consumer



Resource Service



# Question: Using Decentralized Approaches



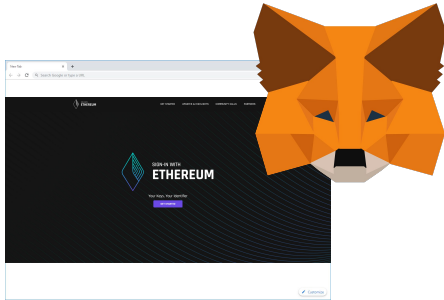


# Bootstrapping a Decentralized Identity



Which techniques are required?

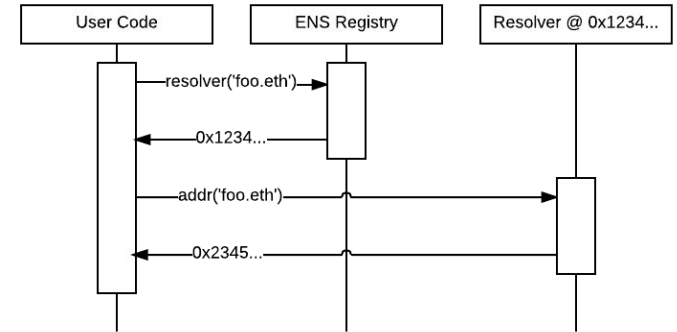
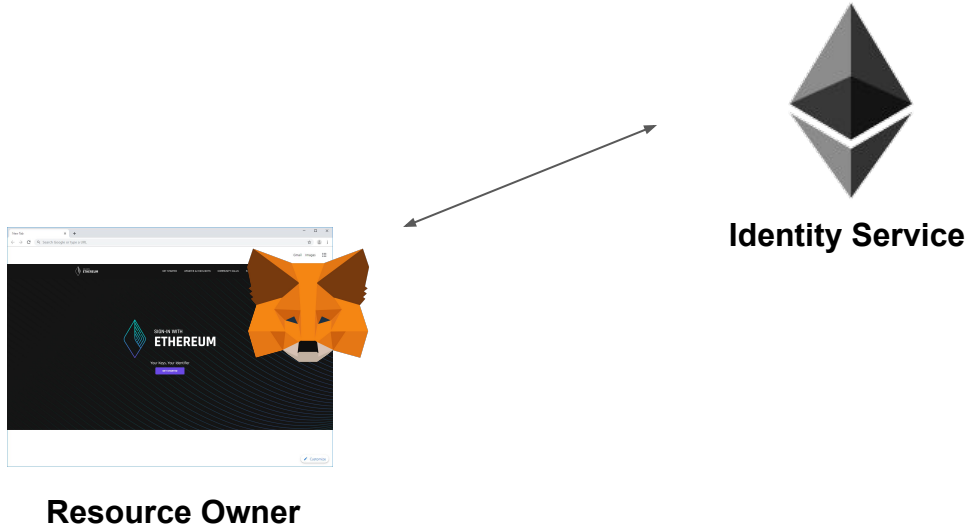
# Wallets



## Resource Owner

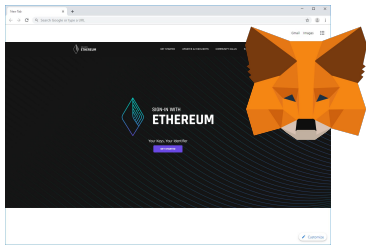
- Custodial vs non-custodial wallets

# On-chain Accounts



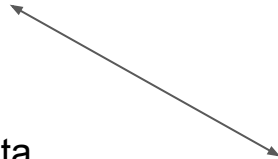
- Registry contracts & Resolver contracts
- Privacy-preserving on-chain states & policies

# Decentralized Storage Networks



**Resource Owner**

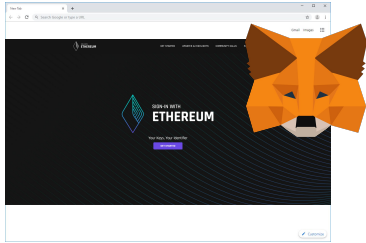
- Store encrypted data



**Resource Service**

Usenix 16: Sieve; Usenix 20: Droplet

# Decentralized Identity



Resource Owner



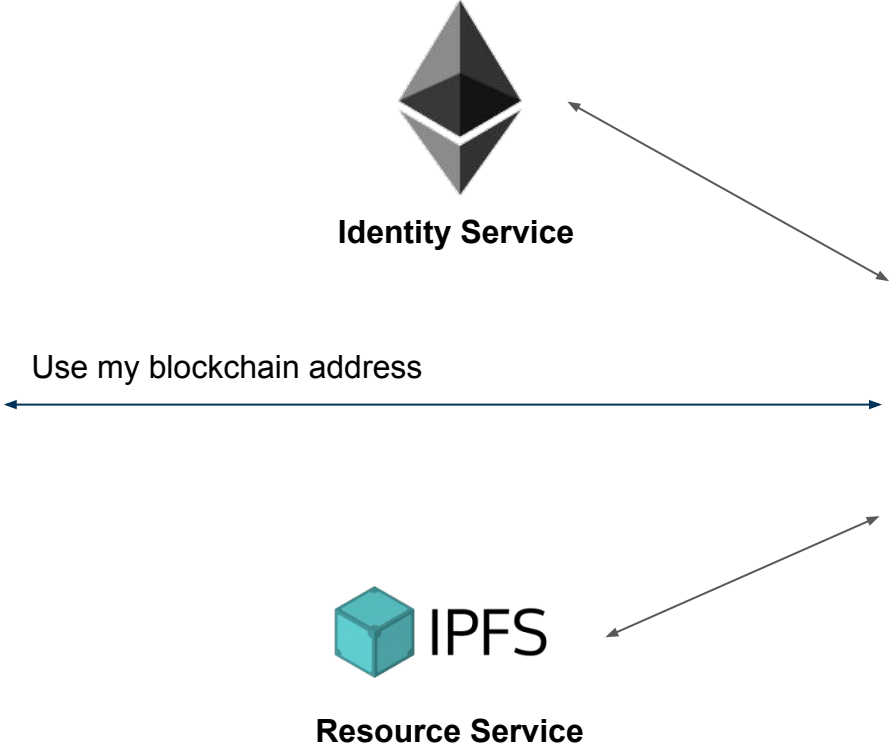
Identity Service



Resource Consumer



Resource Service

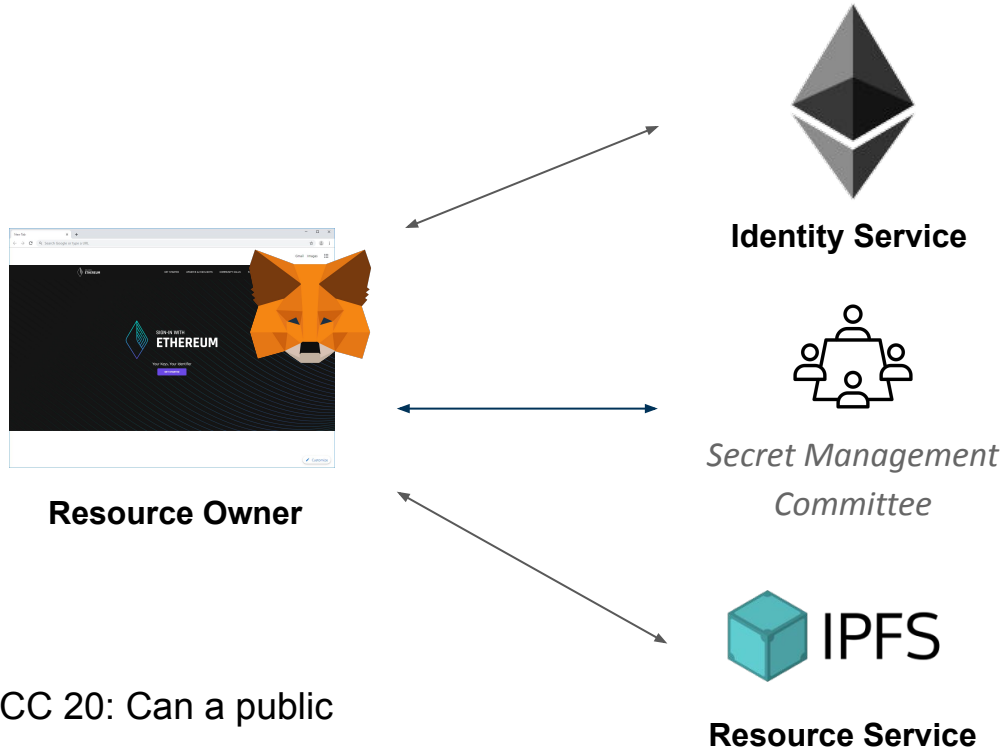


# Taking the next step



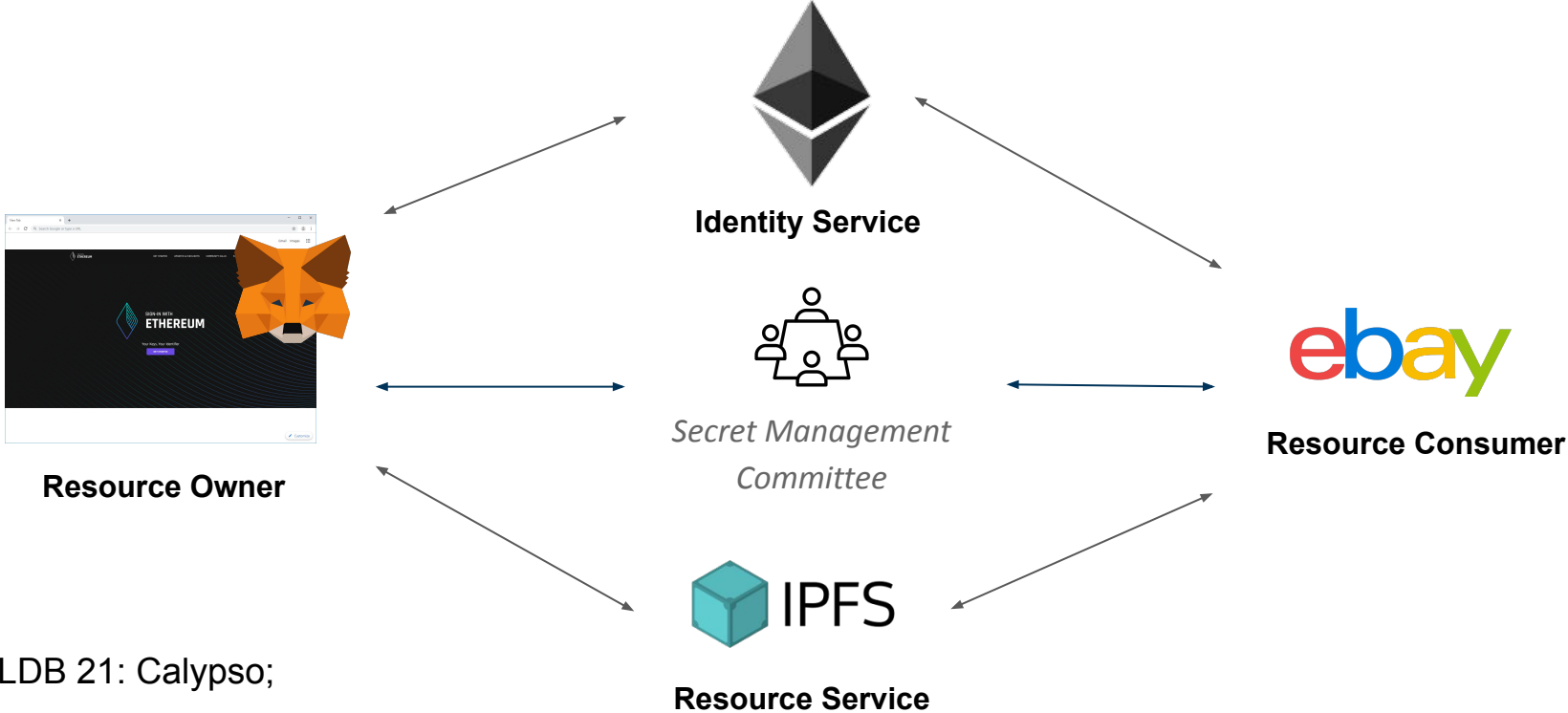
What do we need on top of decentralized identity?

# Decentralized Secret Management



TCC 20: Can a public  
blockchain keep a secret?

# Decentralized Access Control



VLDB 21: Calypso;

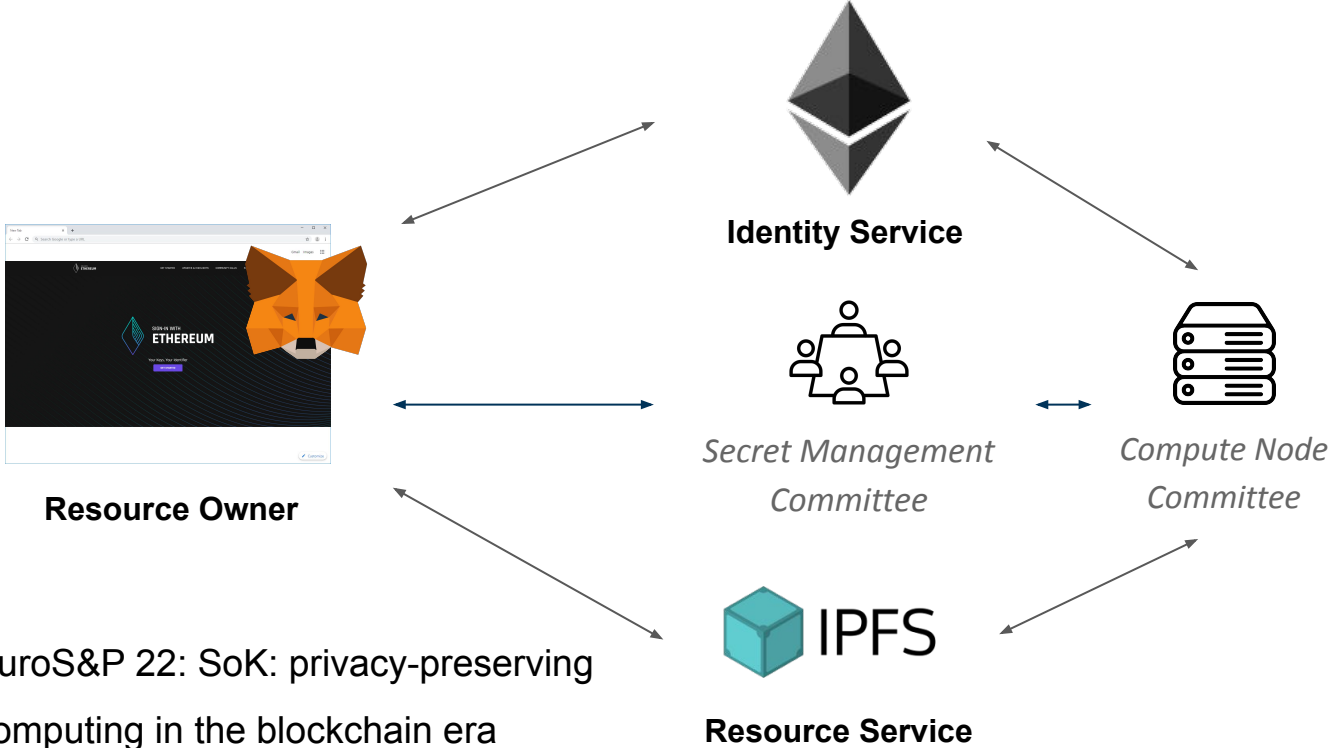


# Going Beyond



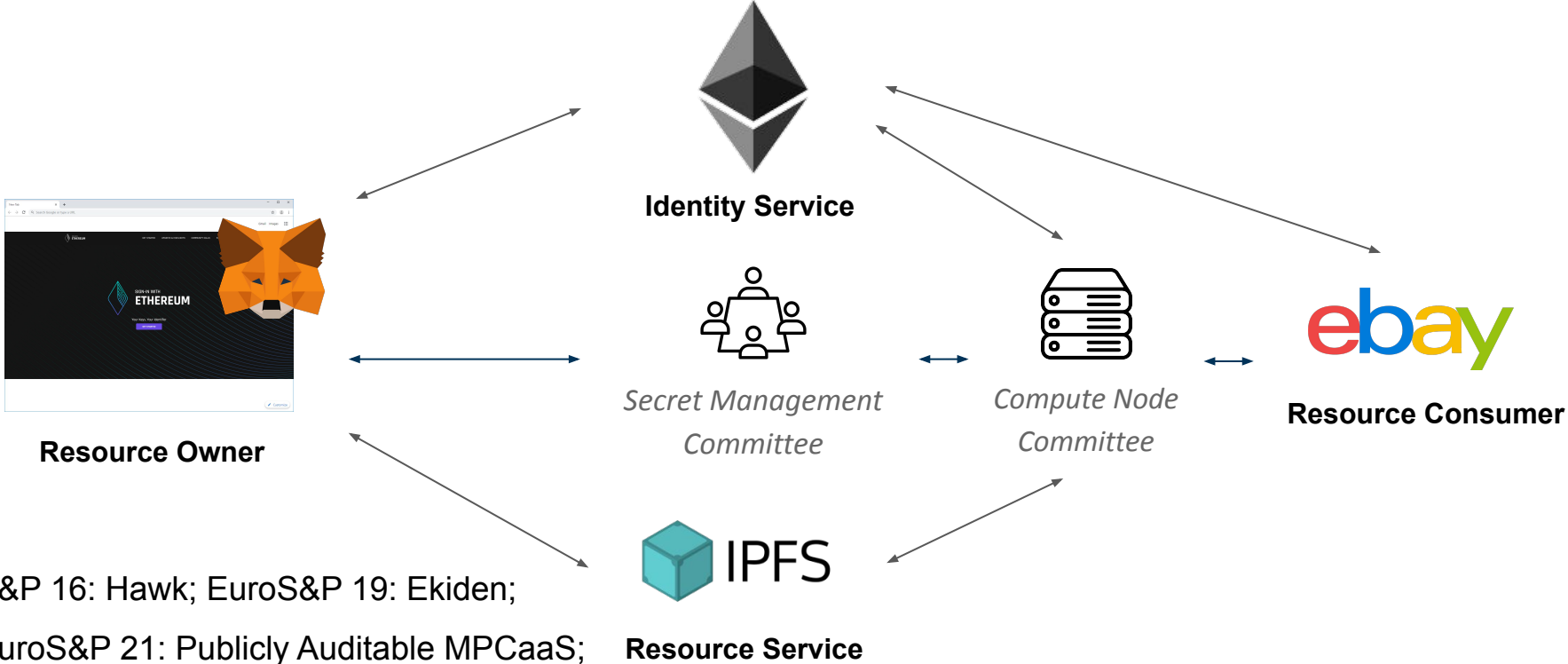
Can we achieve something even better, e.g. full data sovereignty?

# Decentralized Secure Computation



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

# Decentralized Policy-compliant Computation



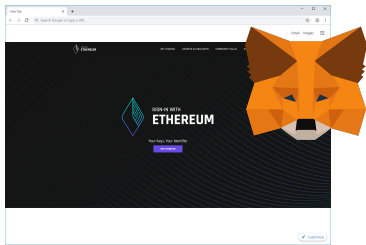
S&P 16: Hawk; EuroS&P 19: Ekiden;  
EuroS&P 21: Publicly Auditable MPCaaS;

# So far so good



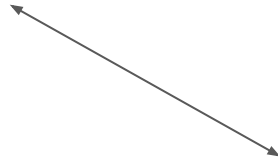
- Control of identifiers, control of data policies
- Transparent access logs
- Verifiable policy-compliant computation
- No data breaches
- Provision of verifiable data

# Something is missing



**Resource Owner**

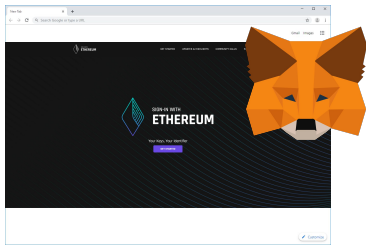
Is the data we provide authentic and trustworthy?



**Resource Service**



# Ebay Seller KYC



**Resource Owner**

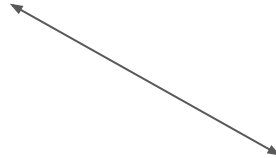
Please share your proof of address & age.



**Resource Consumer**



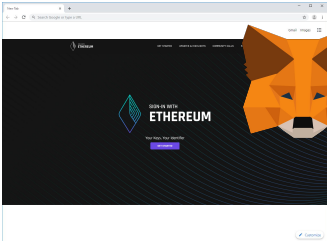
**Resource Service**



# Data Provenance Oracles



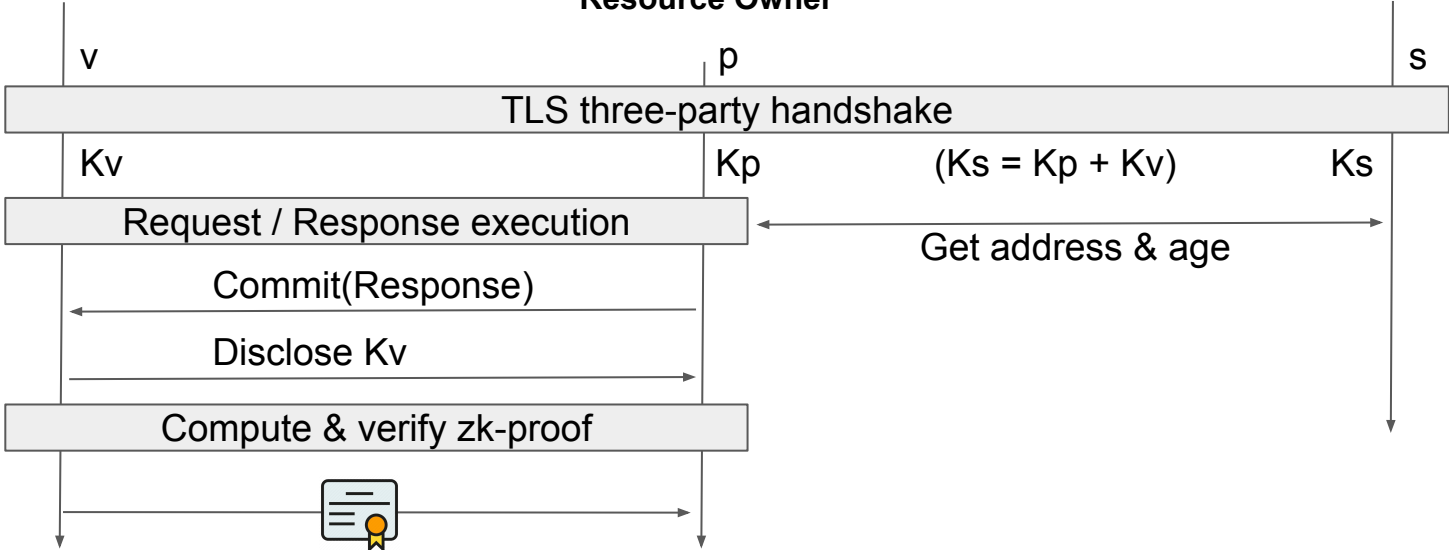
Oracle Verifier



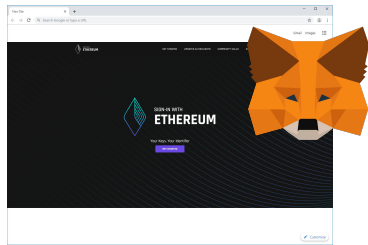
Resource Owner



Trusted Data Provider



# Ebay Seller KYC



Resource Owner

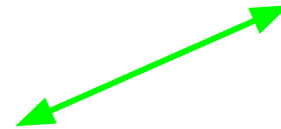
- Address verified.  
• Provision of verifiable data



Resource Consumer



Resource Service





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

This year @EuroS&P 23: SoK Data Sovereignty

Github repository: [web3knowledge](https://github.com/web3knowledge)

Upcoming work on TLS oracles...

Contact: [jens.ernstberger@tum.de](mailto:jens.ernstberger@tum.de), [jan.lauinger@tum.de](mailto:jan.lauinger@tum.de)

Thank you for listening



Questions?