OAuth 2.0 meets verifiable credentials and blockchain-based tokens

Nikos Fotiou

https://mm.aueb.gr

https://www.sofie-iot.eu/

About this presentation

- Partially based on:

“N. Fotiou, I. Pitarras, V.A. Siris, S. Voulgaris, G.C. Polyzos, "OAuth 2.0 authorization using blockchain-based tokens," Proceedings of the NDSS 2020 Workshop on Decentralized IoT Systems and Security (DISS), San Diego, CA, USA, 2020”

- On going work in the context of H2020-SOFIE

About SOFIE*

- SOFIE enables interoperability between existing IoT platforms
  - Utilizes distributed ledger technologies
  - 3-year EU Horizon 2020 project, will end in December 2020
- SOFIE functionality will be provided through its framework**
  - “Privacy and Data Sovereignty,” and “Identity, Authentication, and Authorization” are two key components of the SOFIE framework

Aalto University School of Electrical Engineering
ASM Terni S.p.A.
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS
emotion
ROVIO
ENGINEERING
ERICSSON
guardtime
VELTION OPTIMUM
SYNELIXIS

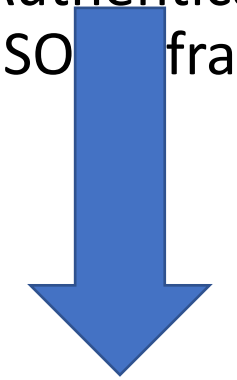
* Secure Open Federation for Internet Everywhere https://www.sofie-iot.eu/

** https://github.com/SOFIE-project/Framework

About SOFIE

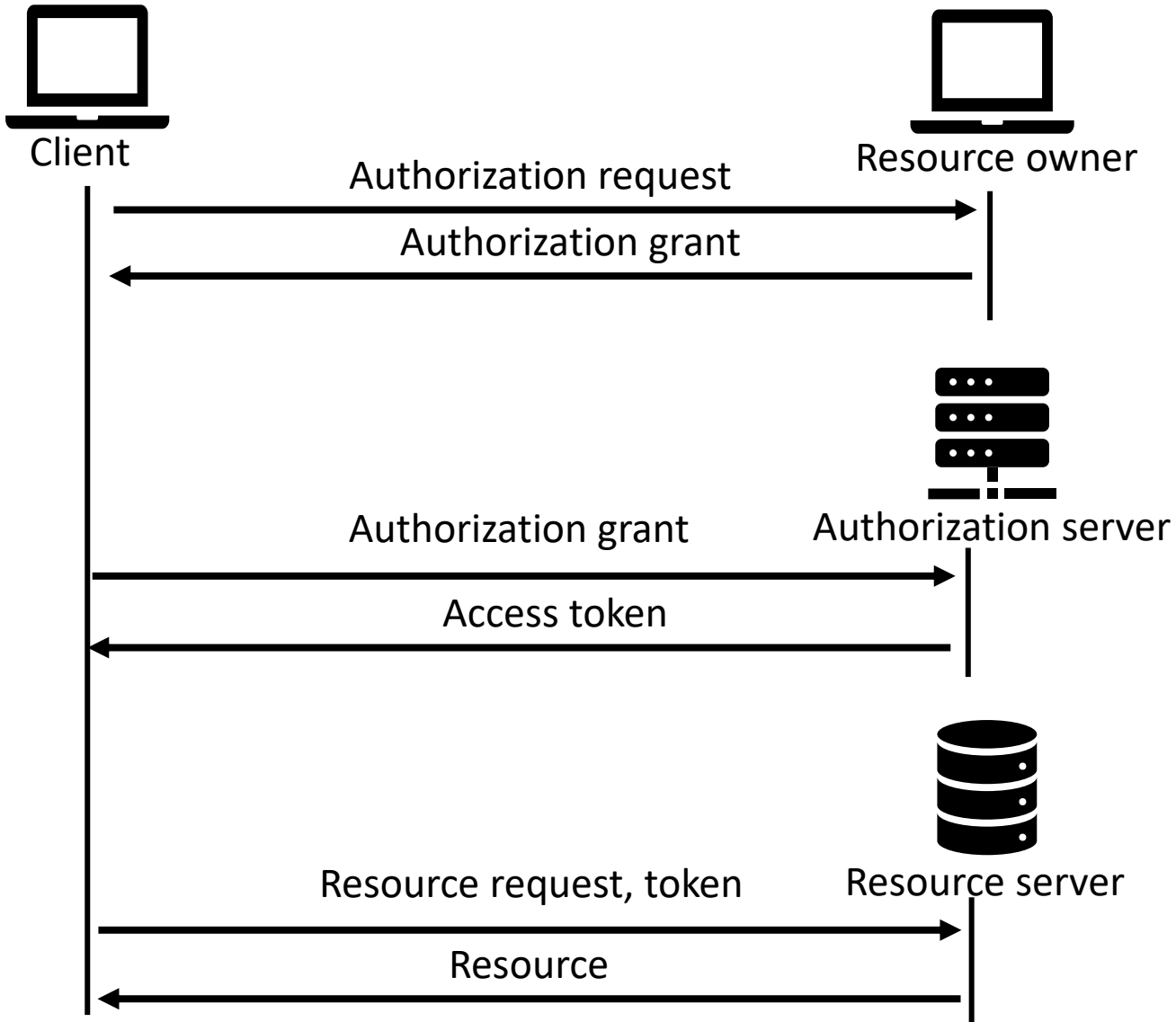
- SOFIE enables interoperability between existing IoT platforms
  - Utilizes distributed ledger technologies
  - 3-year EU Horizon 2020 project, will end in December 2020
- SOFIE functionality will be provided through its framework
  - “Privacy and Data Sovereignty,” and “Identity, Authentication, and Authorizati[illegible]” are two key components of the SO[illegible] framework

OAuth 2.0

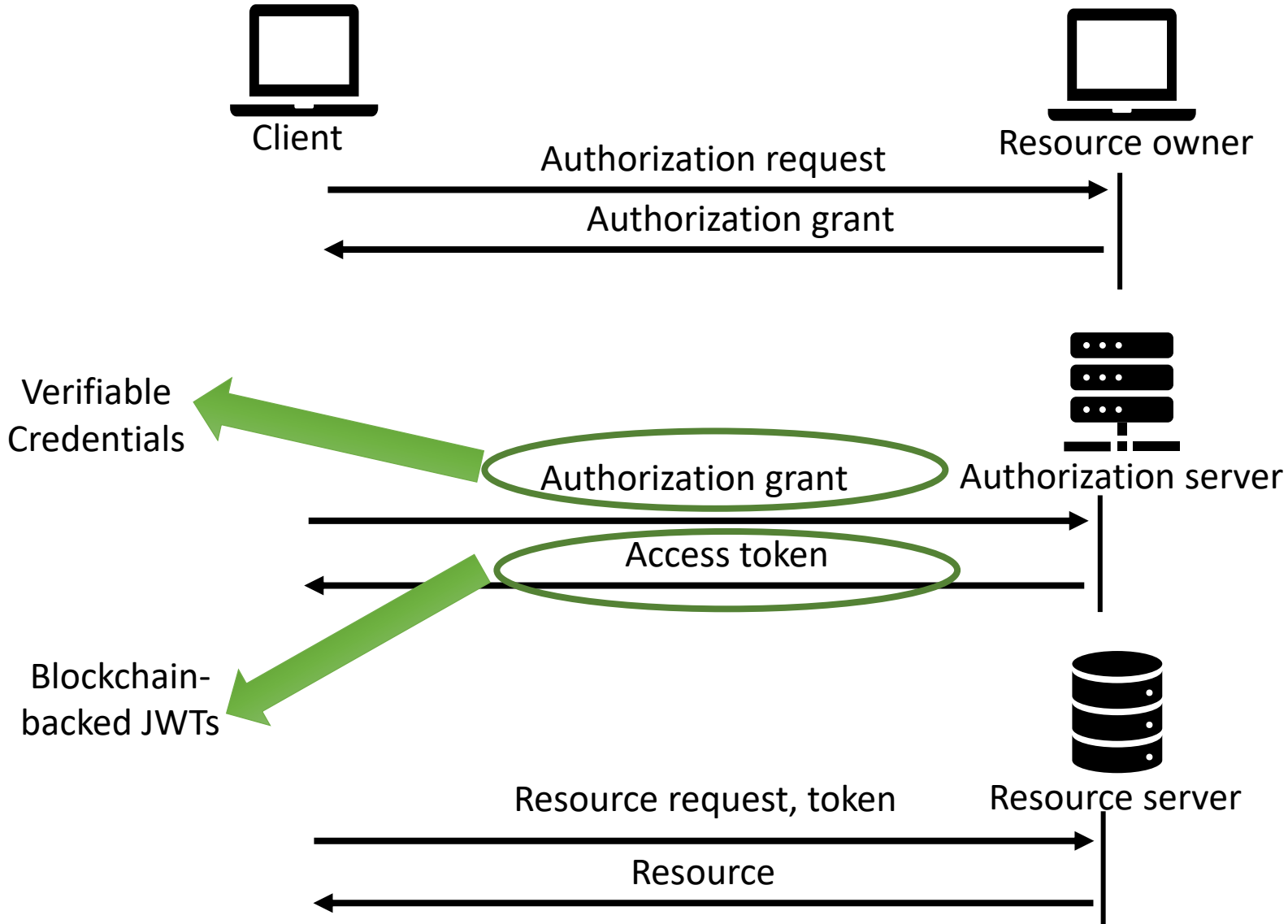


JWT

OAuth 2.0-based authorization



OAuth 2.0-based authorization



SOFIE Clients

- Resource owners do not interact with clients
- Clients may not evan have UI (e.g., IoT device)

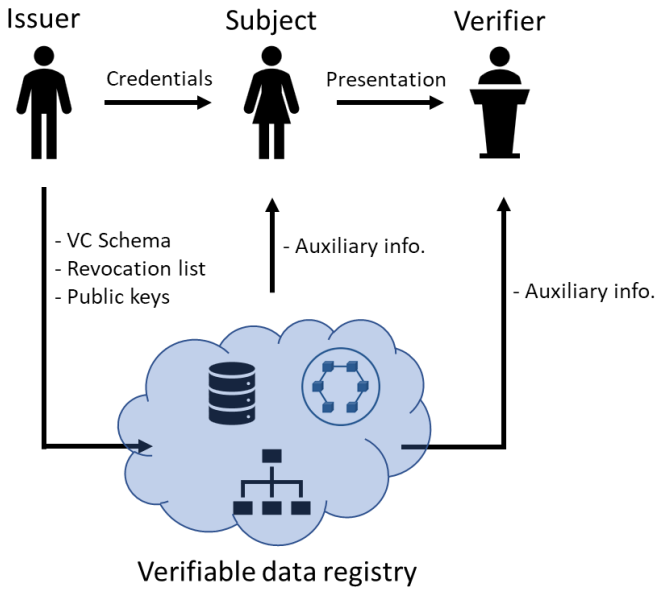
  → Client credentials are the “recommended” authorization grant for this case
- But we want to avoid long, hard to manage ACLs in the authorization server

Client Identifier	Resource Identifier
Client 1	[Resource 1, Resource 2, Resource 3]
Client 2	[Resource K, Resouce L]

→ Verifiable Credentials can solve this problem

VC in a nutshell

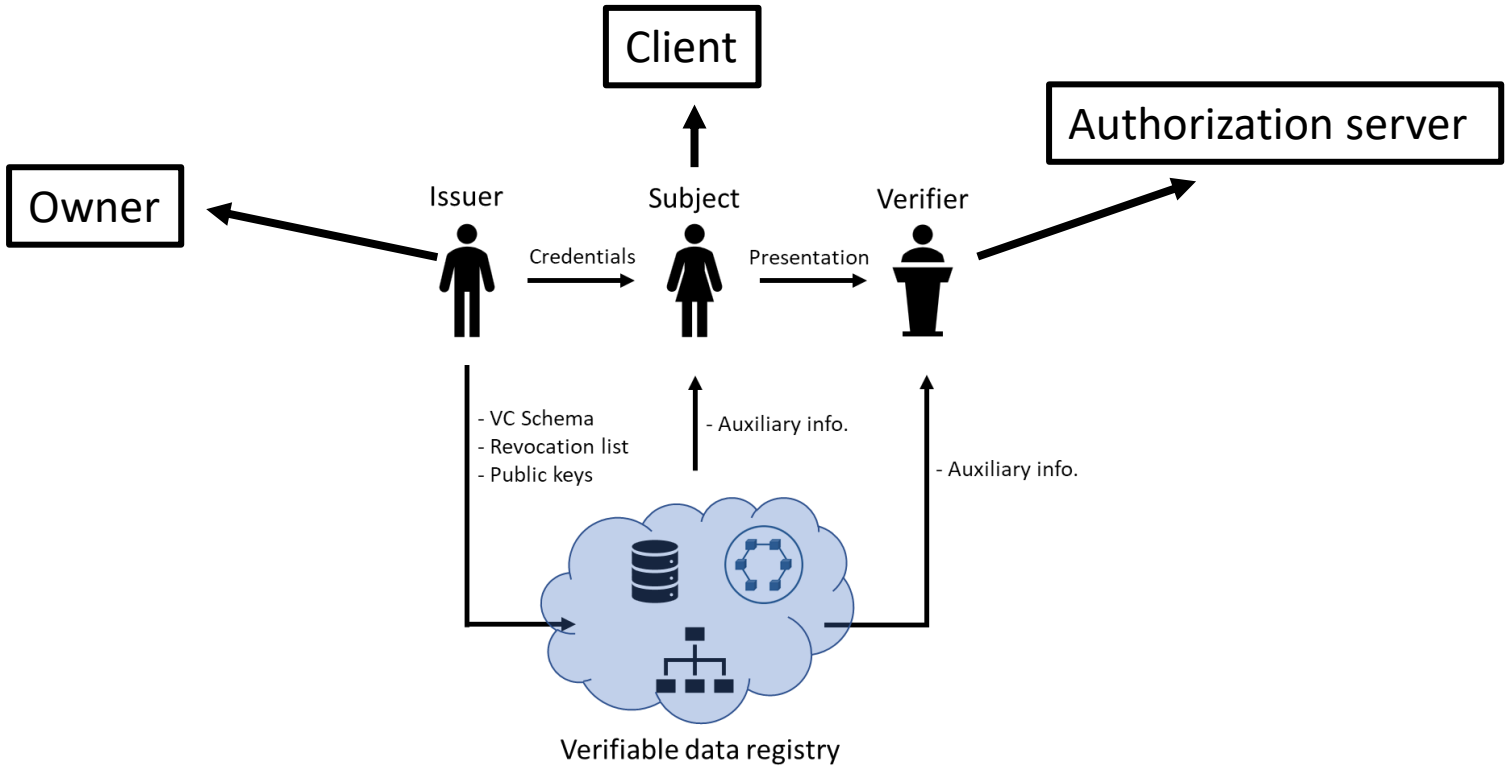
- A standard* way to express credentials on the Web



* W3C, Verifiable Credentials Data Model 1.0, https://www.w3.org/TR/vc-data-model/

VC in a nutshell

- A standard* way to express credentials on the Web



* W3C, Verifiable Credentials Data Model 1.0, https://www.w3.org/TR/vc-data-model/

VC Structure

Context
Issuer Id
Credential • Type • Subject Id • Claims
Proof

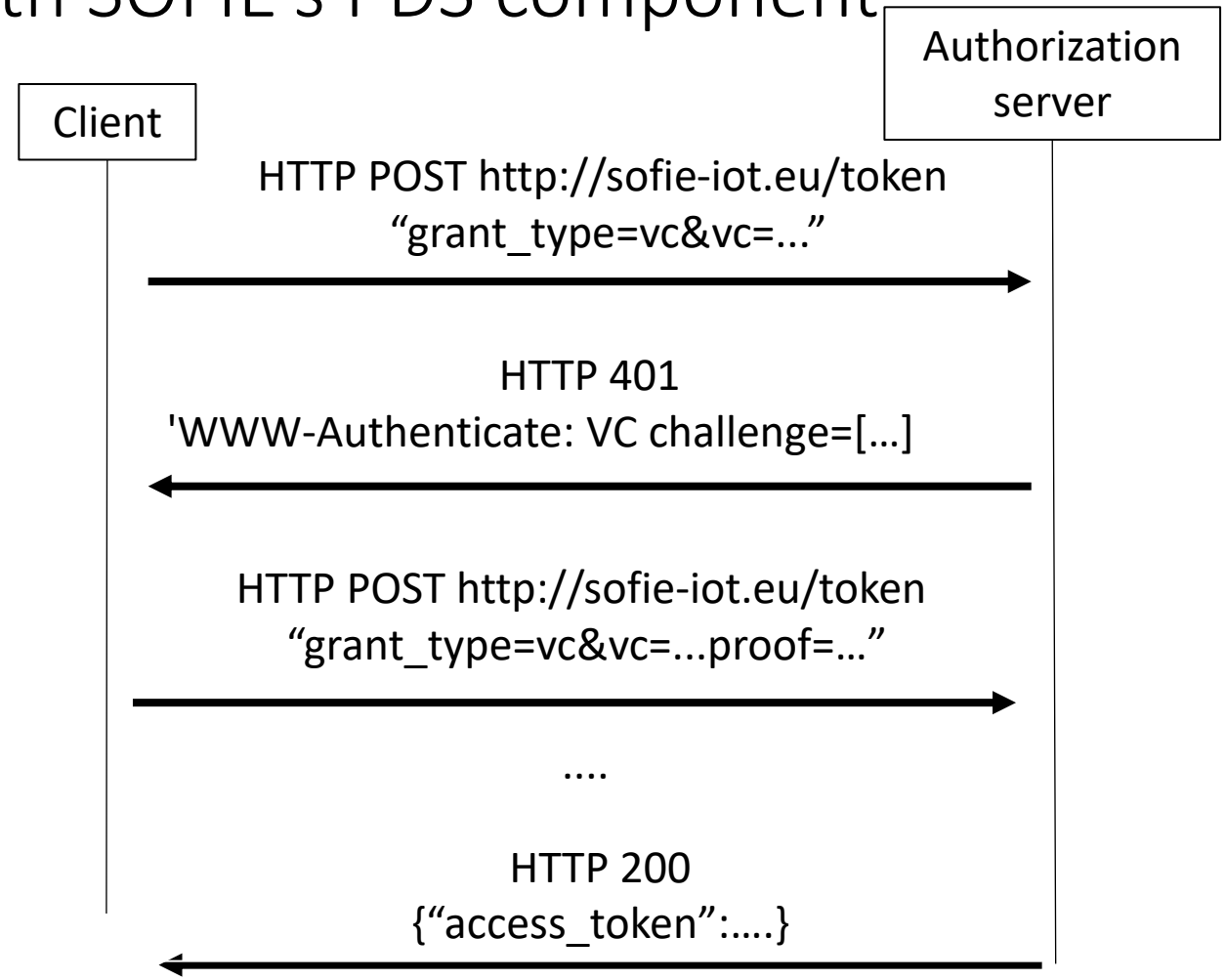
An example credential

```
sofie_credential = {
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://mm.aueb.gr/contexts/access_control/v1"
  ],
  "id": "https://www.sofie-iot.eu/credentials/examples/1",
  "type": ["VerifiableCredential"],
  "issuer": "did:nacl:E390CF3B5B93E921C45ED978737D89F61B8CAFF9DE76BFA5F63DA20386BCCA3B",
  "issuanceDate": "2010-01-01T19:23:24Z",
  "credentialSubject": {
    "id": "did:nacl:A490CF3B5B93E921C45ED978737D89F61B8CAFF9DE76BFA5F63DA20386BCCA62",
    "type": ["AllowedURLs"],
    "acl": [
      {
        "url": "http://sofie-iot.eu/device1",
        "methods": ["GET","POST"]
      },
      {
        "url": "http://sofie-iot.eu/device2",
        "methods": ["GET"]
      }
    ]
  }
}
```

An example credential

```
sofie_credential = {
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://mm.aueb.gr/contexts/access_control/v1"
  ],
  "id": "https://www.sofie-iot.eu/credentials/examples/1",
  "type": ["VerifiableCredential"],
  "issuer": "did:nacl:E390CF3B5B93E921C45ED978737D89F61B8CAFF9DE76BFA5F63DA20386BCCA3B",
  "issuanceDate": "2010-01-01T19:23:24Z",
  "credentialSubject": {
    "id": "did:nacl:A490CF3B5B93E921C45ED978737D89F61B8CAFF9DE76BFA5F63DA20386BCCA62",
    "type": ["AllowedURLs"],
    "acl": [
      {
        "url": "http://sofie-iot.eu/device1",
        "methods": ["GET","POST"]
      },
      {
        "url": "http://sofie-iot.eu/device2",
        "methods": ["GET"]
      }
    ]
  }
}
```

Interacting with SOFIE's PDS component



PDS configuration

```
filters = [
    ["$.@context[*]", "https://mm.aueb.gr/contexts/access_control/v1"],
    ["$.issuer", ["did:nacl:…","another issuer", "or this issuer"]],
    ["$.credentialSubject.acl[?@.url='http://sofie-iot.eu/device1'].methods[*]","GET"]
  ]
```

The use of JWT in SOFIE

- JWT is a standard mean for tranfering claims, used in may authorization systems
- Usually they are used as Bearer tokens
- We leverage blockchain to provide
  - Proof-of-possession
  - Revocation
  - Delagation

The Ethereum blockchain

- Decentrilized “smart contract” executed by untrusted nodes
- Smart contract code and state are public
- Smart contract execution is deterministic
- State modification are permantly recorded in the blockchain
- Users identified by a public key. The hash of the public key is used as the “address” of the user. The private key is used for singing “transactions”

ERC-721

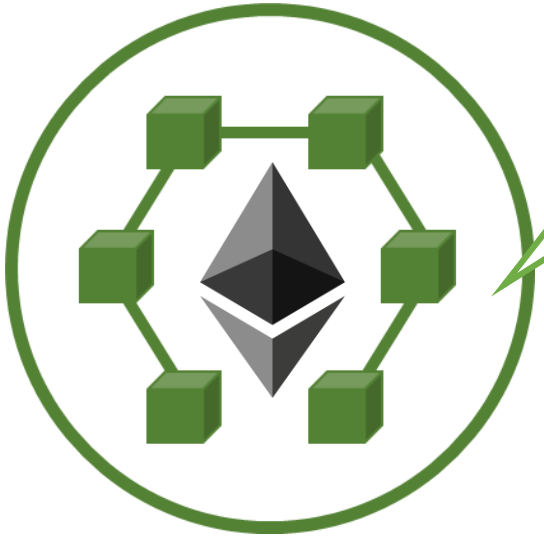
ERC-721 tokens

- Token Id
- Owner Id
- Metadata

ERC-721

ERC-721 tokens

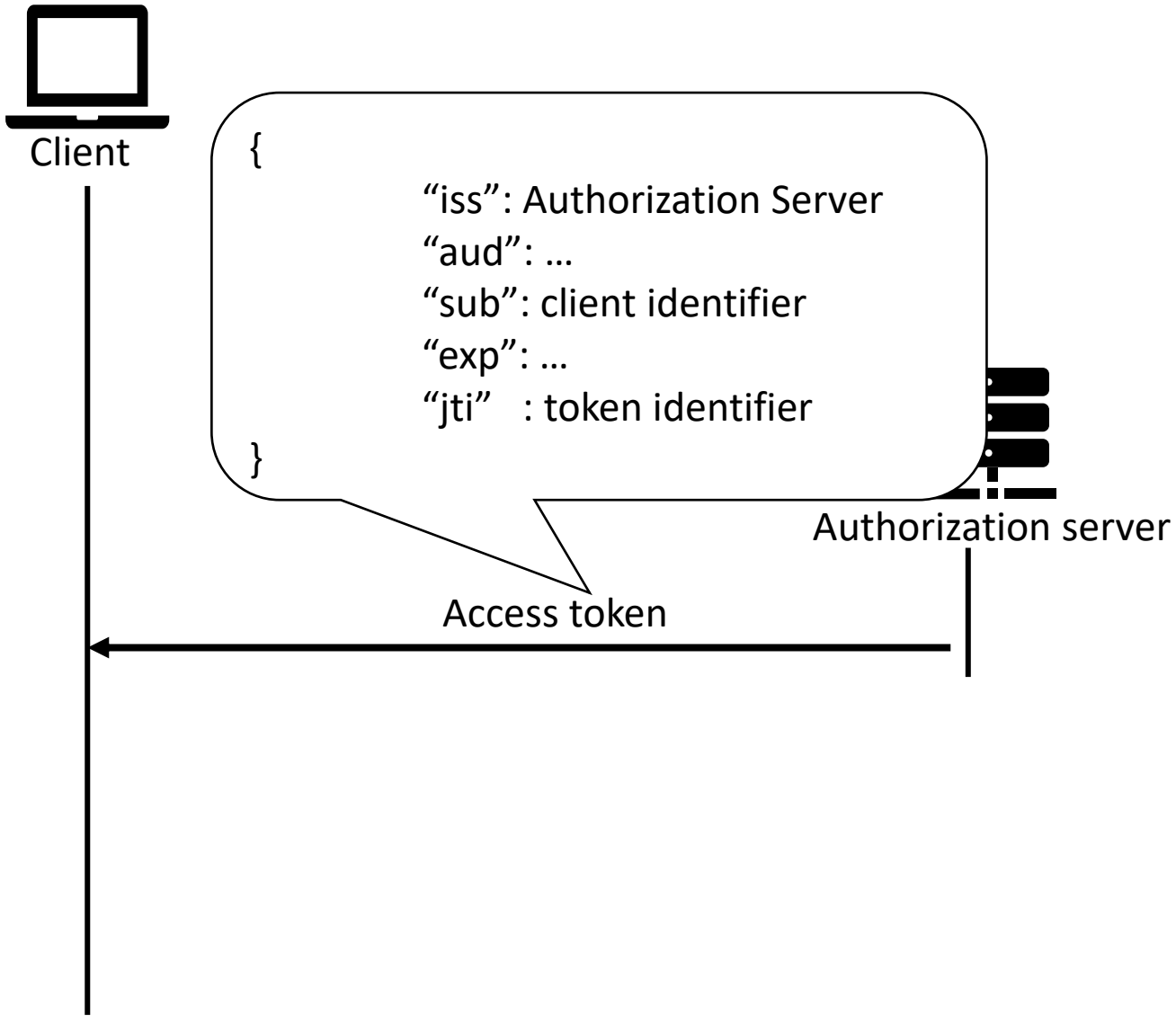
- Token Id
- Owner Id
- Metadata



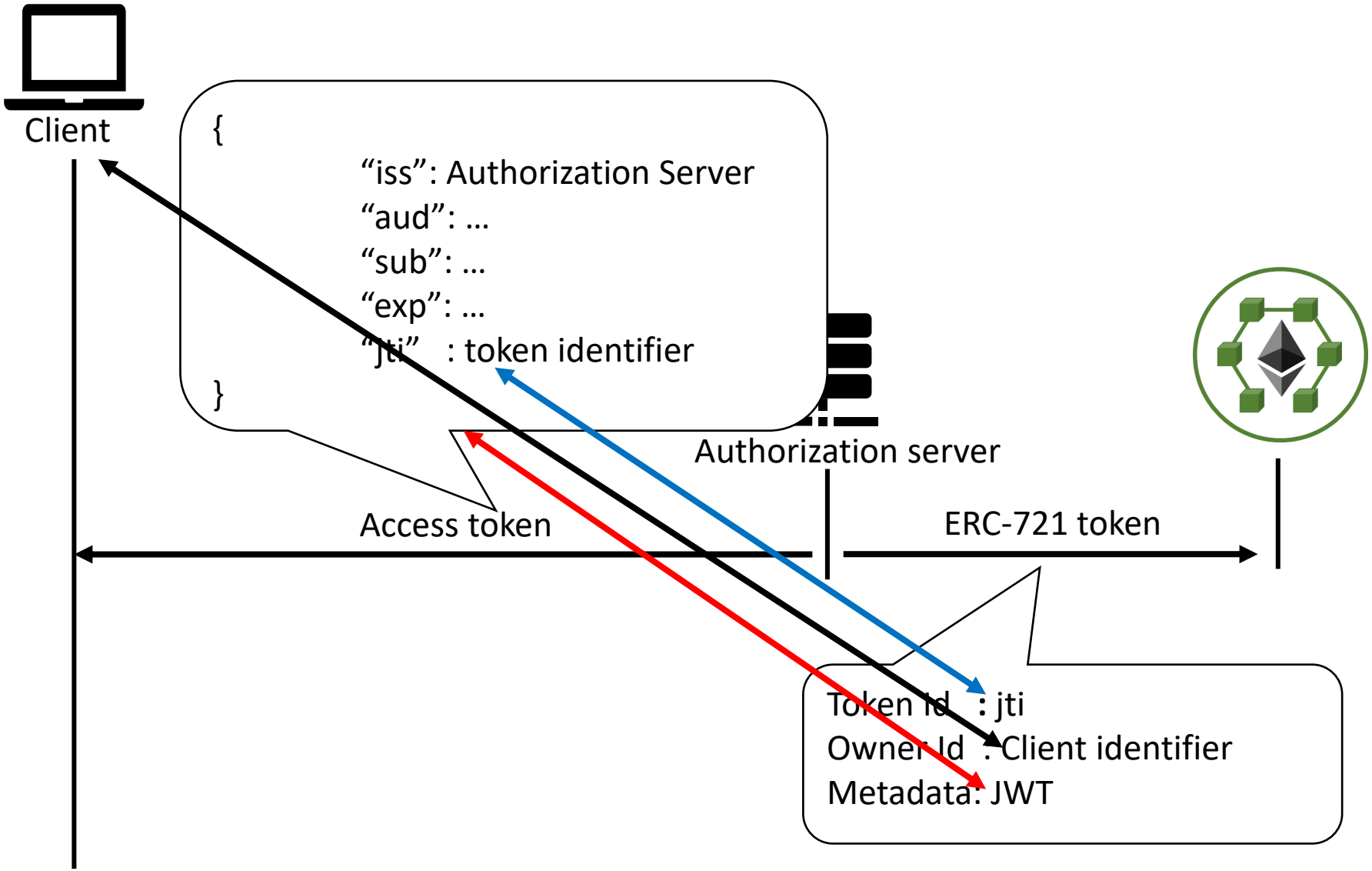
ERC-721 token management contract

- ownerOf()
- transferFrom()
- approve()
- getApproved()
- tokenURI()

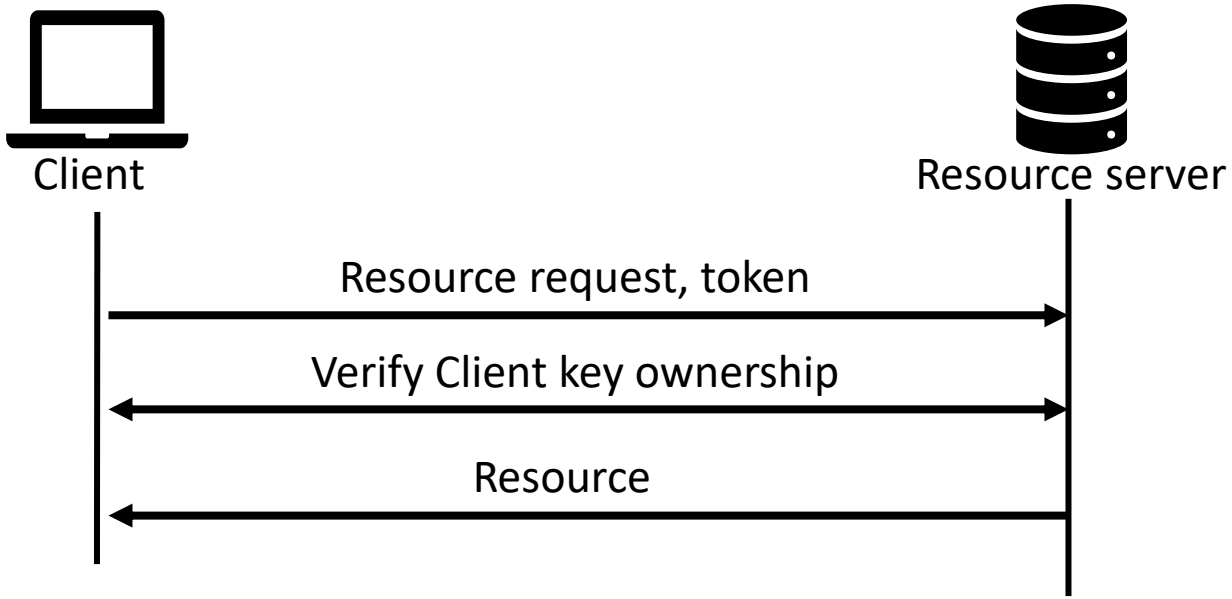
JWT


Client
{
“iss”: Authorization Server
“aud”: …
“sub”: client identifier
“exp”: …
“jti” : token identifier
}
Authorization server
Access token

JWT + ERC-721

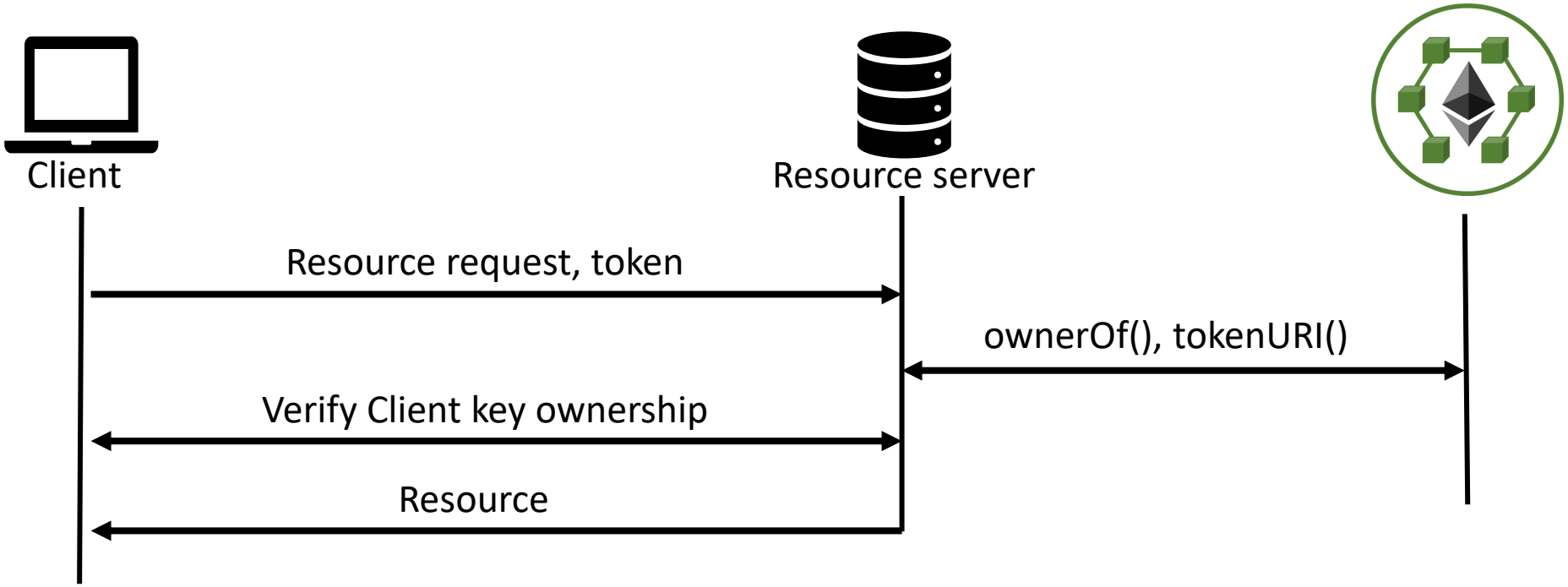

Client
{
"iss": Authorization Server
"aud": …
"sub": …
"exp": …
"jti" : token identifier
}
Authorization server
Access token
ERC-721 token
Token Id : jti
Owner Id : Client identifier
Metadata: JWT

Accessing legacy resource servers

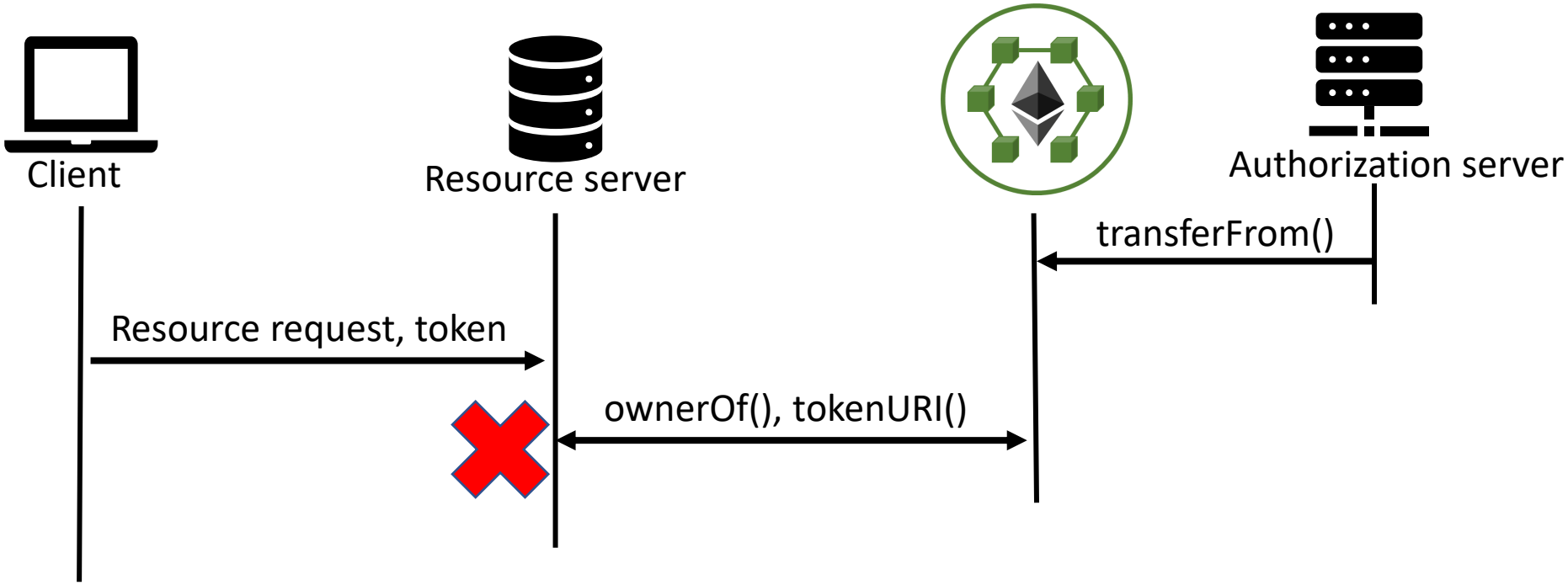


- It facilitates logging and auditing services

Accessing resource servers with BC read access

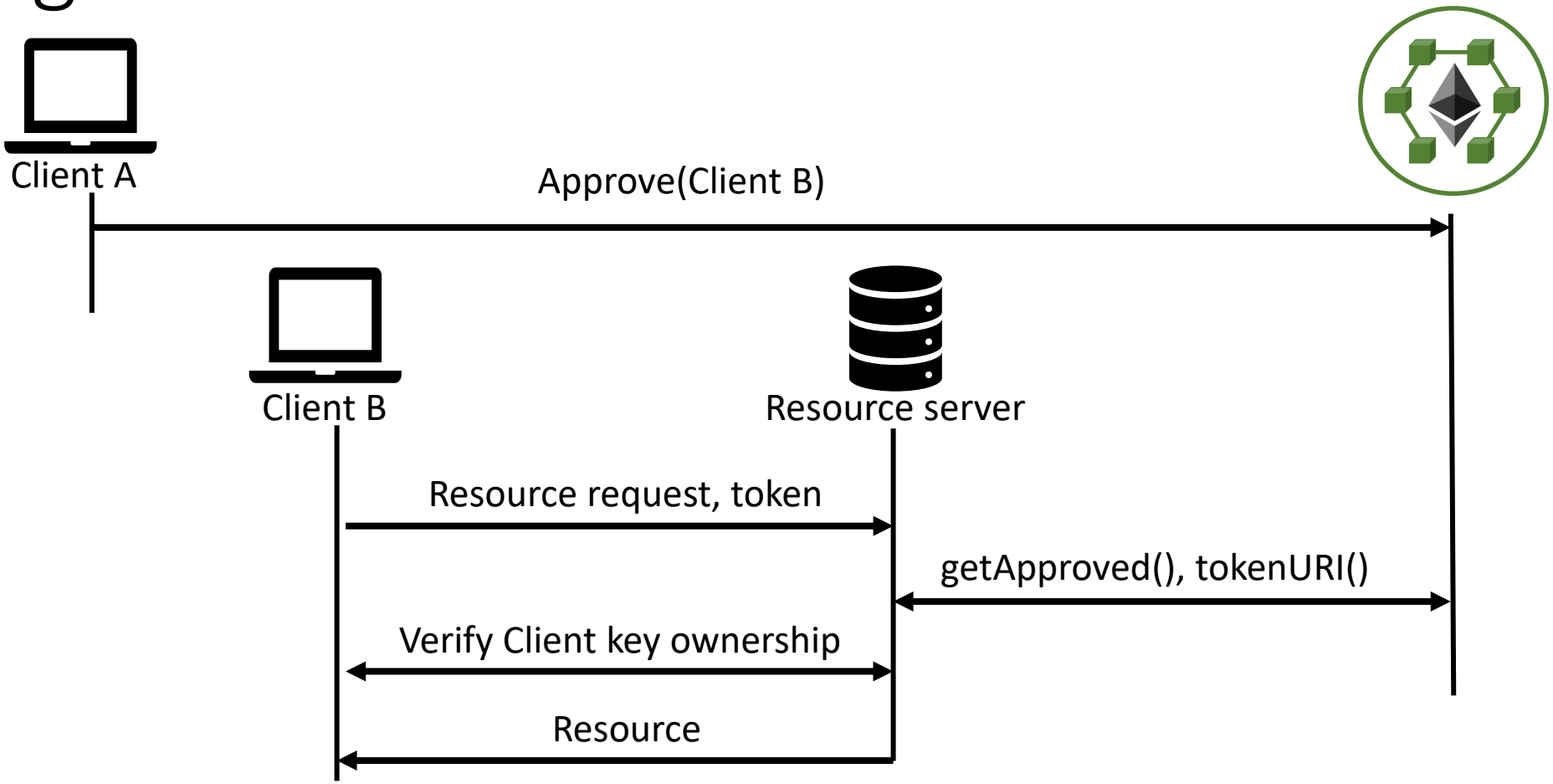


Revocation



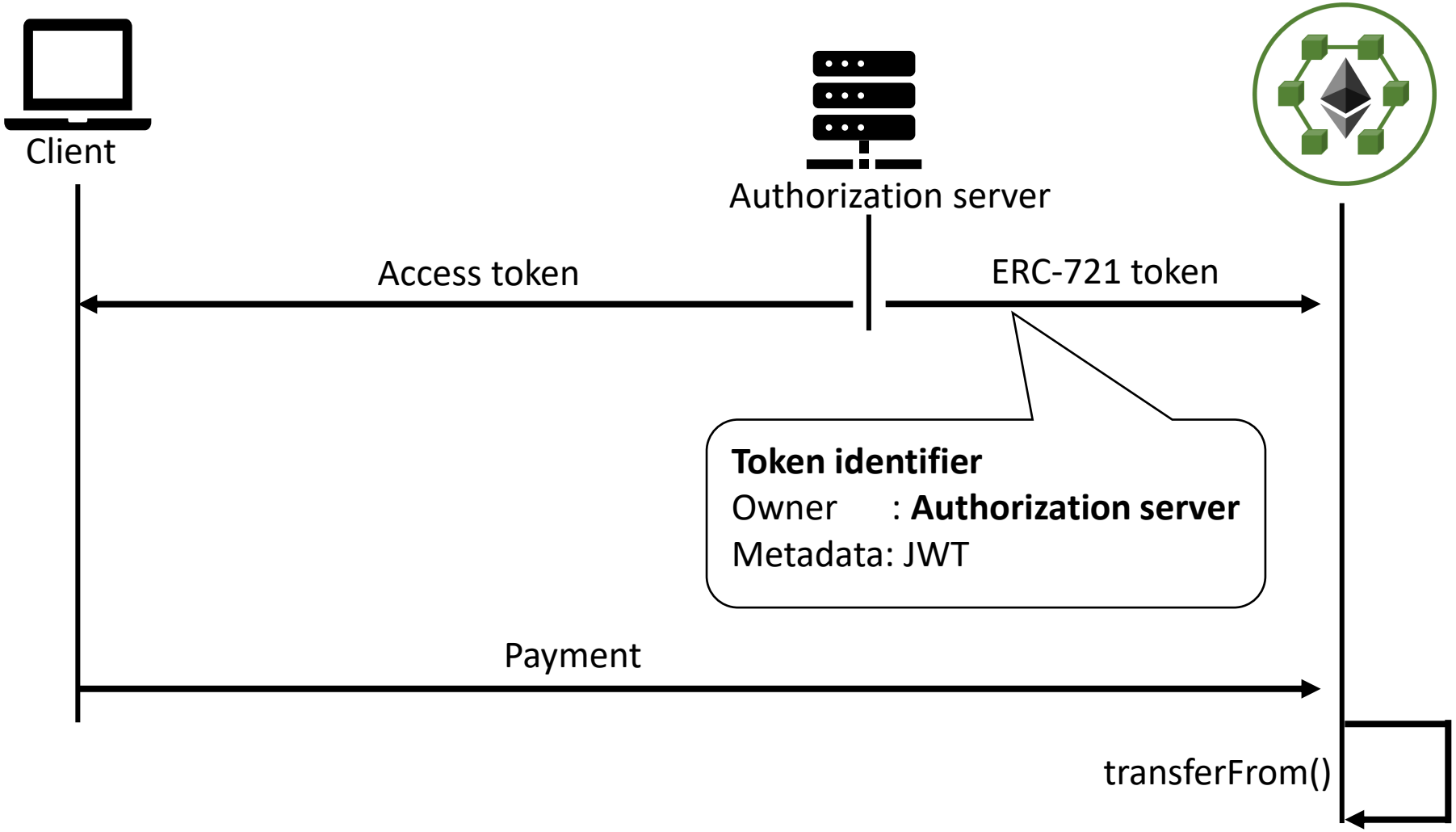
- Revocation is asynchronous
- Authorization server does not have to be online

Delegation



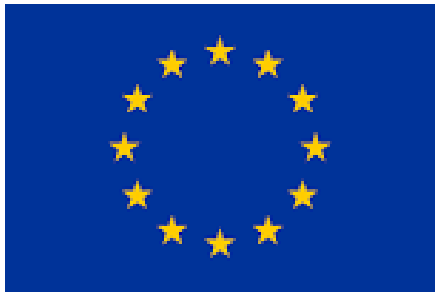
- Delegation is not transitive
- Revocation is not affected

Fair exchange



A note about blockchains

- (Public) blockchains have privacy issues, introduce delays (~13sec per transaction) and monetary costs (~$0.10 to create a token, $0.02 to revoke or delegate)
  - In no payments are involved then private, or testing chains can be used.



Thank you

fotiou@aueb.gr

https://www.sofie-iot.eu/

https://github.com/SOFIE-project/Framework

https://www.sofie-iot.eu/news/integrating-verifiable-credentials-and-decentralized-identifiers-for-identification-and-author