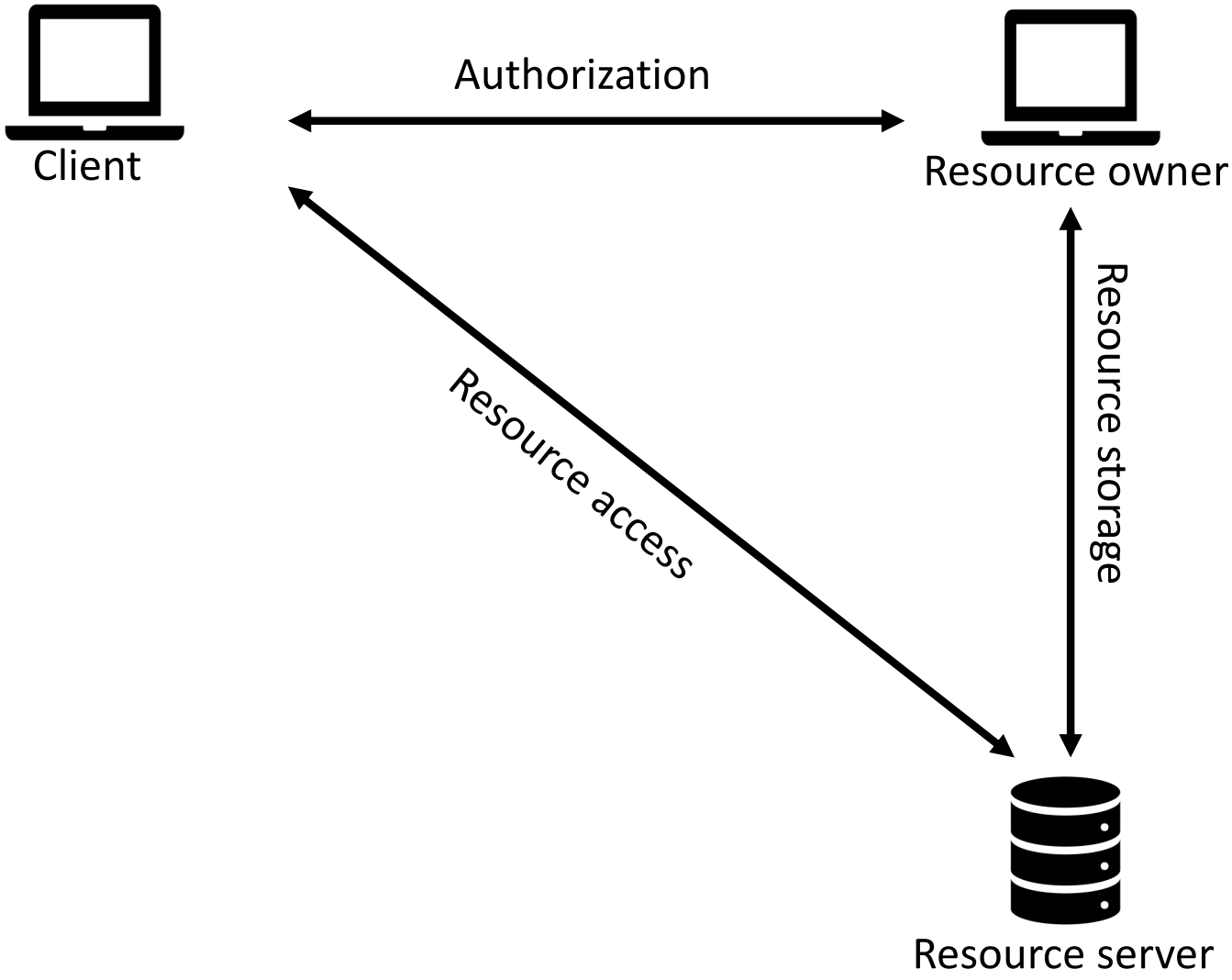
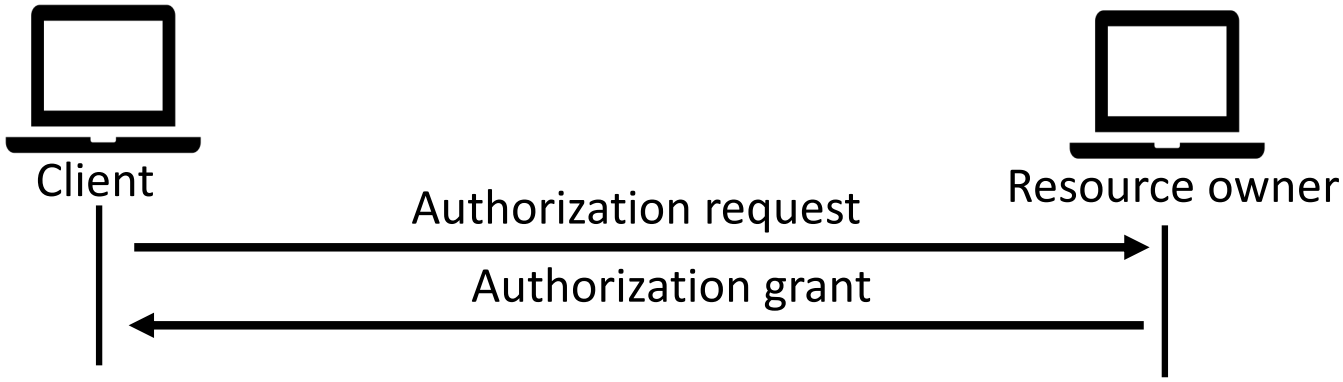
OAuth 2.0 authorization using blockchain-based tokens

Nikos Fotiou, Iakovos Pittaras, Vasilios A. Siris, Spyros Voulgaris, George C. Polyzos

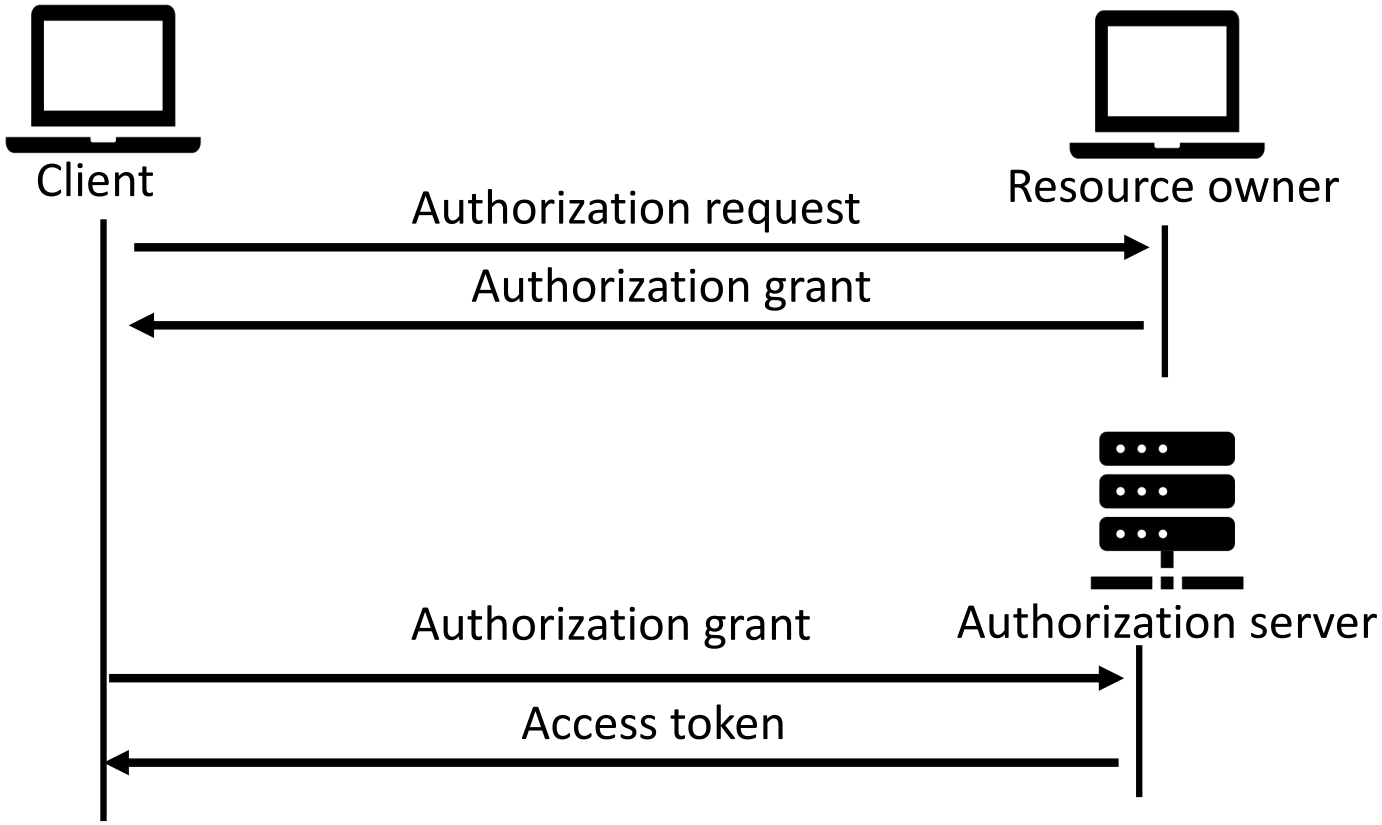
Resource sharing



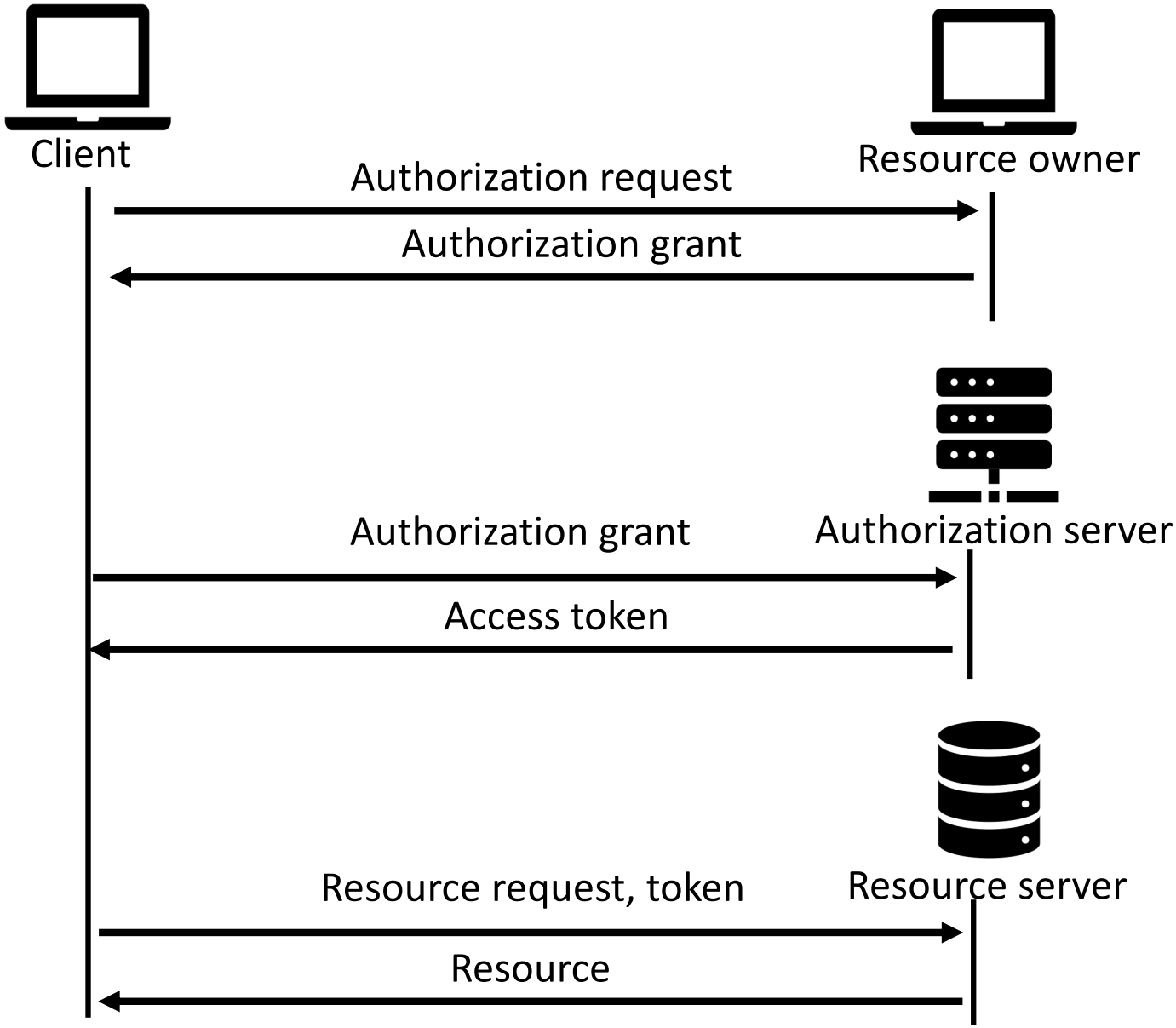
OAuth 2.0-based authorization



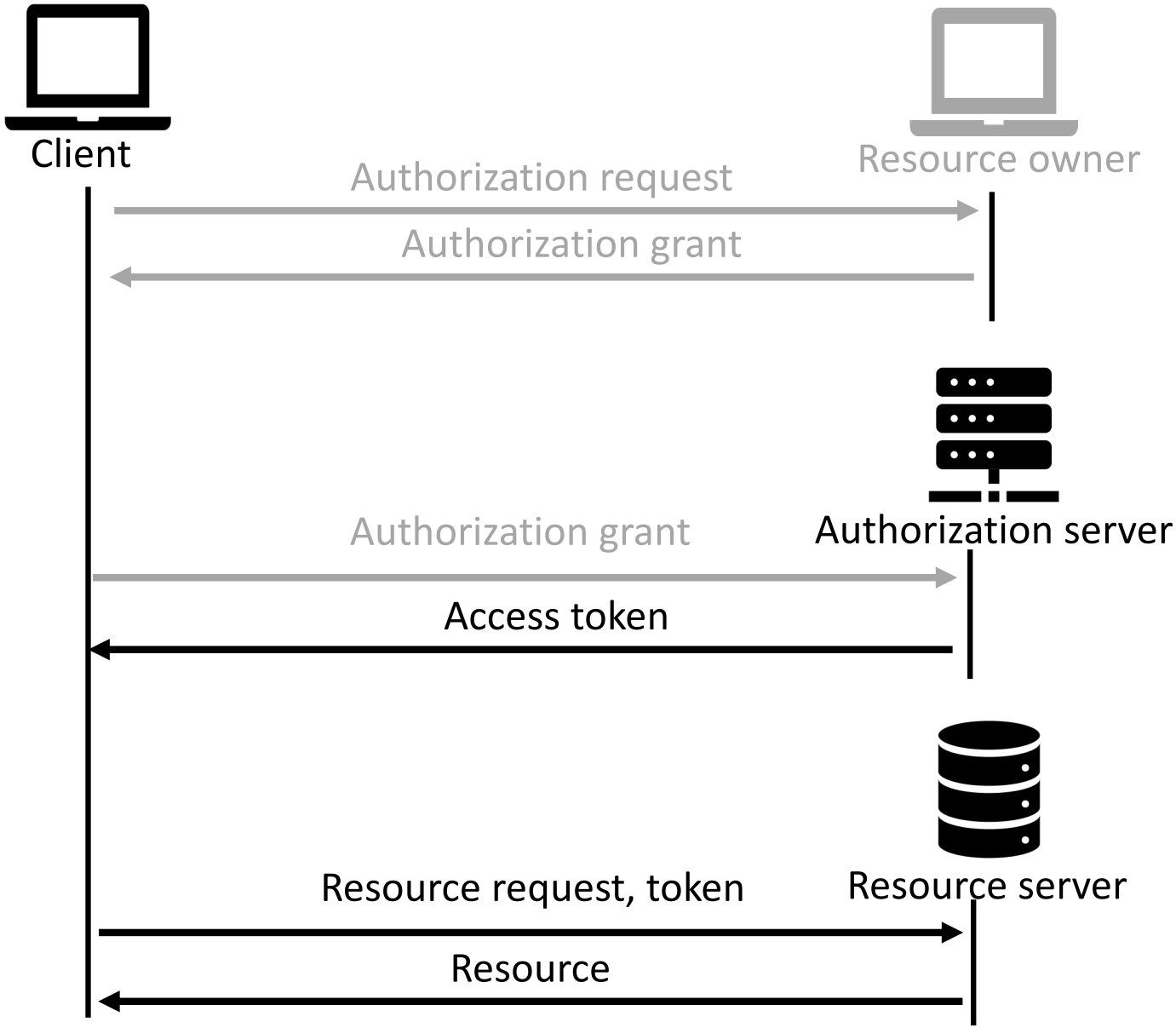
OAuth 2.0-based authorization



OAuth 2.0-based authorization

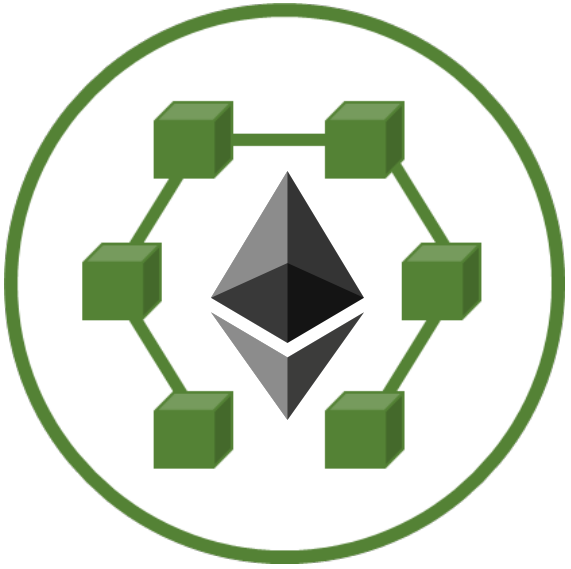


Our work


Client
Resource owner
Authorization request
Authorization grant
Authorization grant
Authorization server
Access token
Resource request, token
Resource server
Resource

The Ethereum blockchain

- Data “recorded” in the ledger are immutable
- Decentrilized “smart contract” can be executed by untrusted nodes in a deterministic way



ERC-721

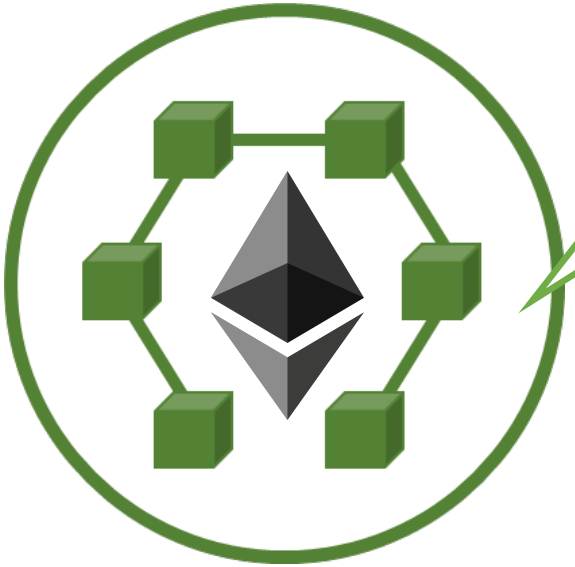
ERC-721 tokens

- Token Id
- Owner Id
- Metadata

ERC-721

ERC-721 tokens

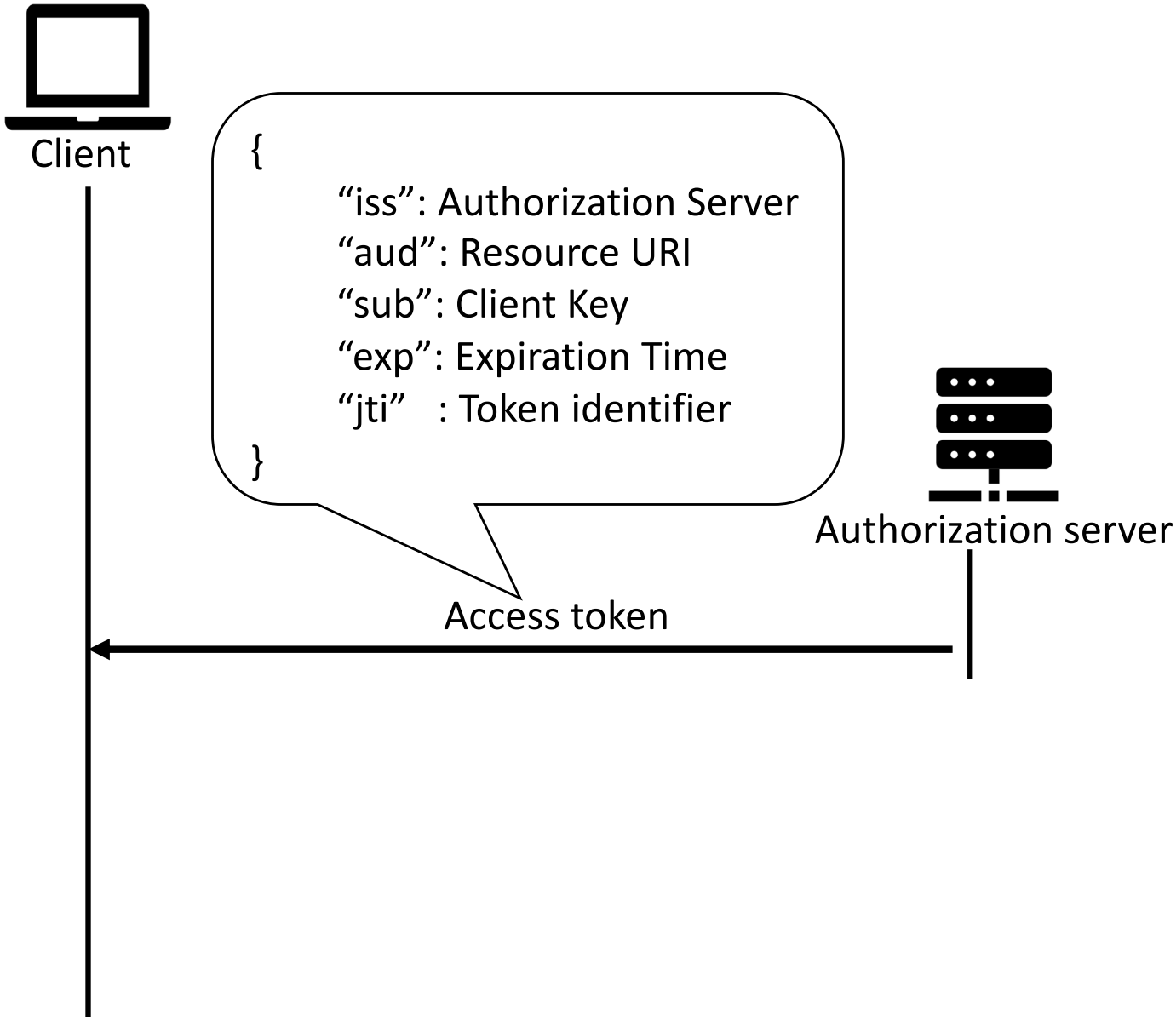
- Token Id
- Owner Id
- Metadata



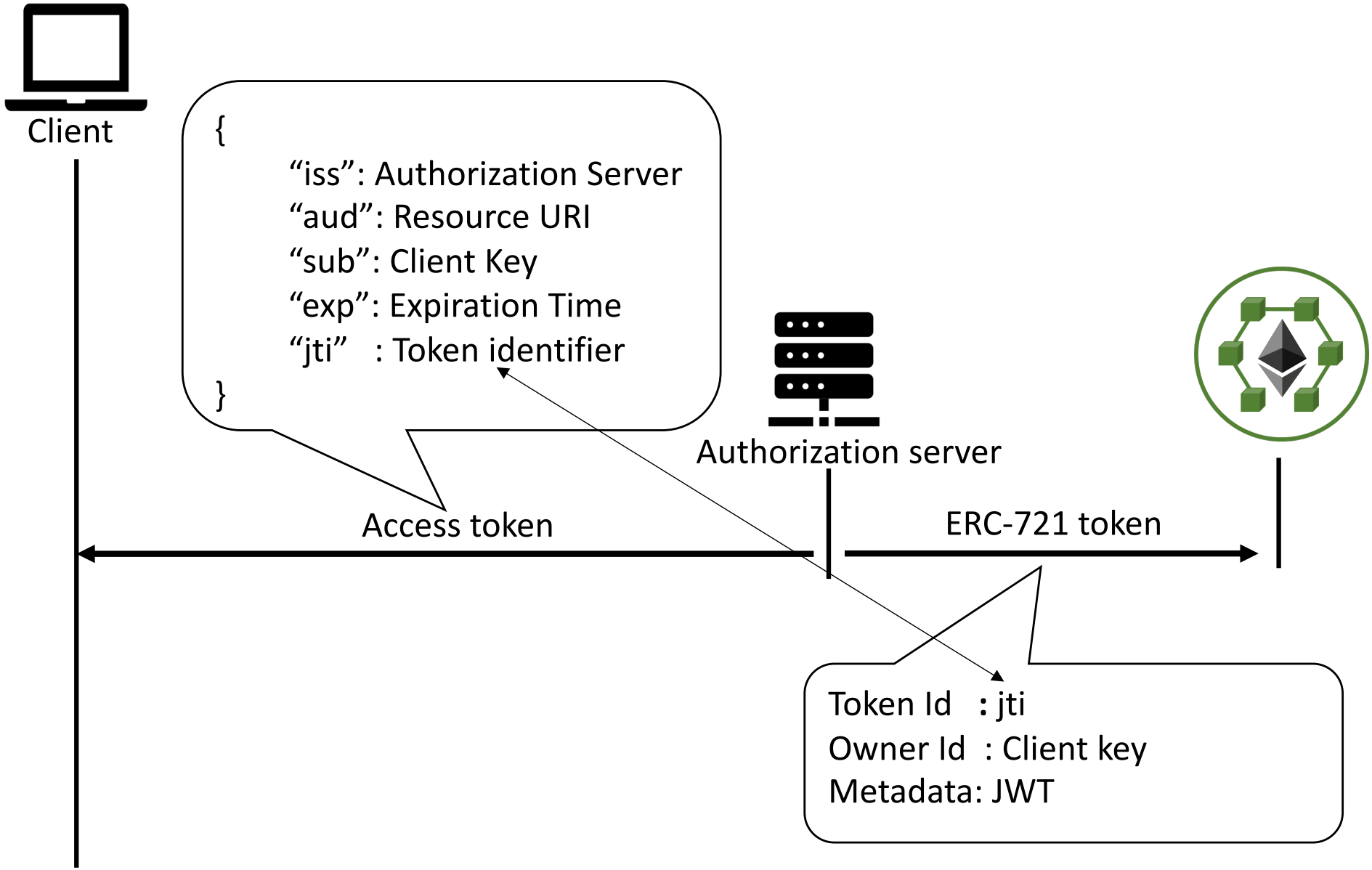
ERC-721 token management contract

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

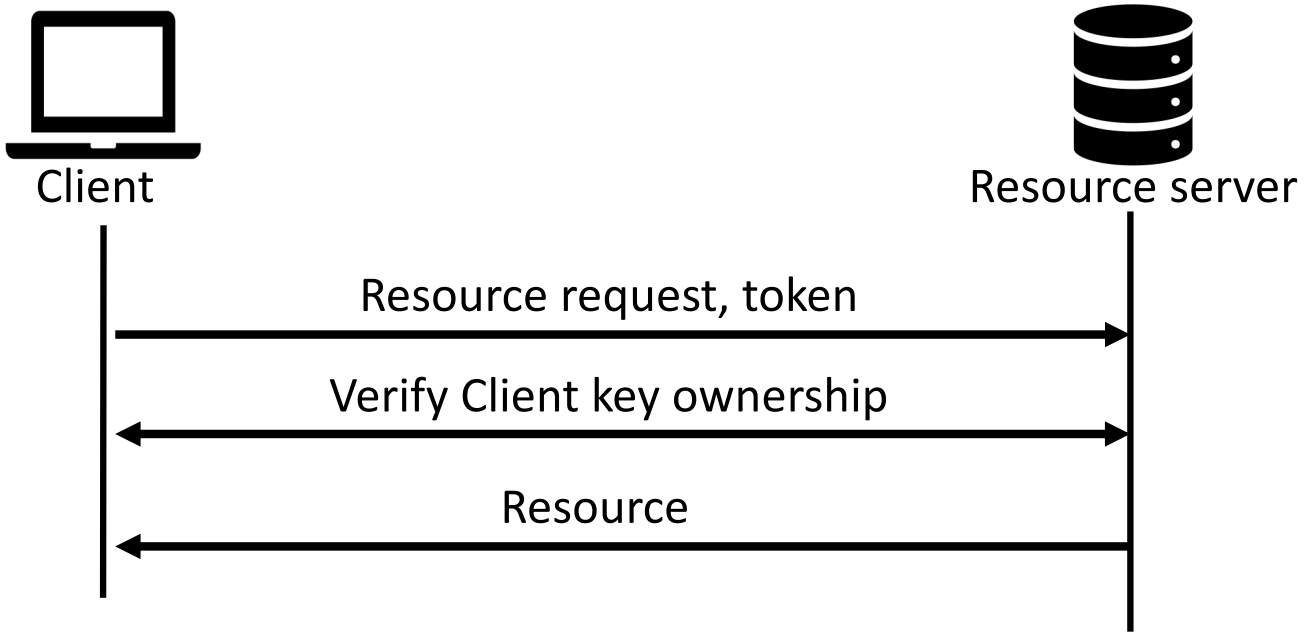
JWT


Client
{
“iss”: Authorization Server
“aud”: Resource URI
“sub”: Client Key
“exp”: Expiration Time
“jti” : Token identifier
}
Authorization server
Access token

JWT + ERC-721

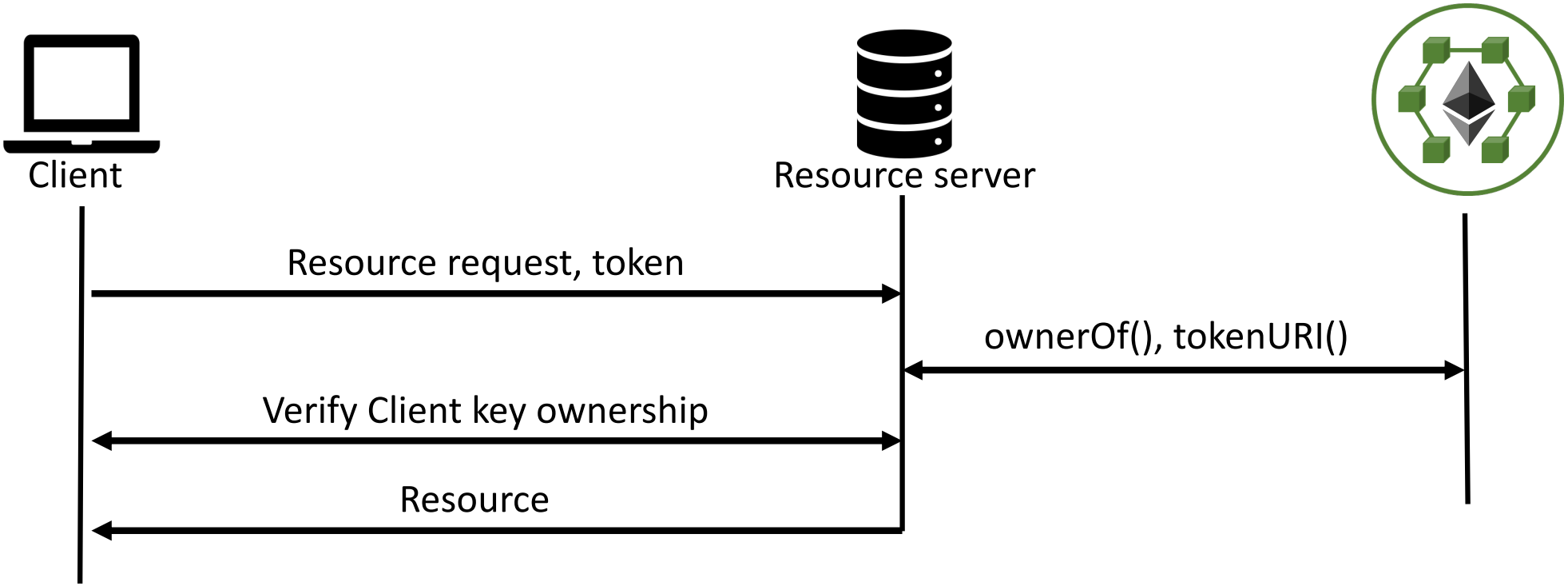

Client
{
"iss": Authorization Server
"aud": Resource URI
"sub": Client Key
"exp": Expiration Time
"jti" : Token identifier
}
Authorization server
Access token
ERC-721 token
Token Id : jti
Owner Id : Client key
Metadata: JWT

Accessing legacy resource servers

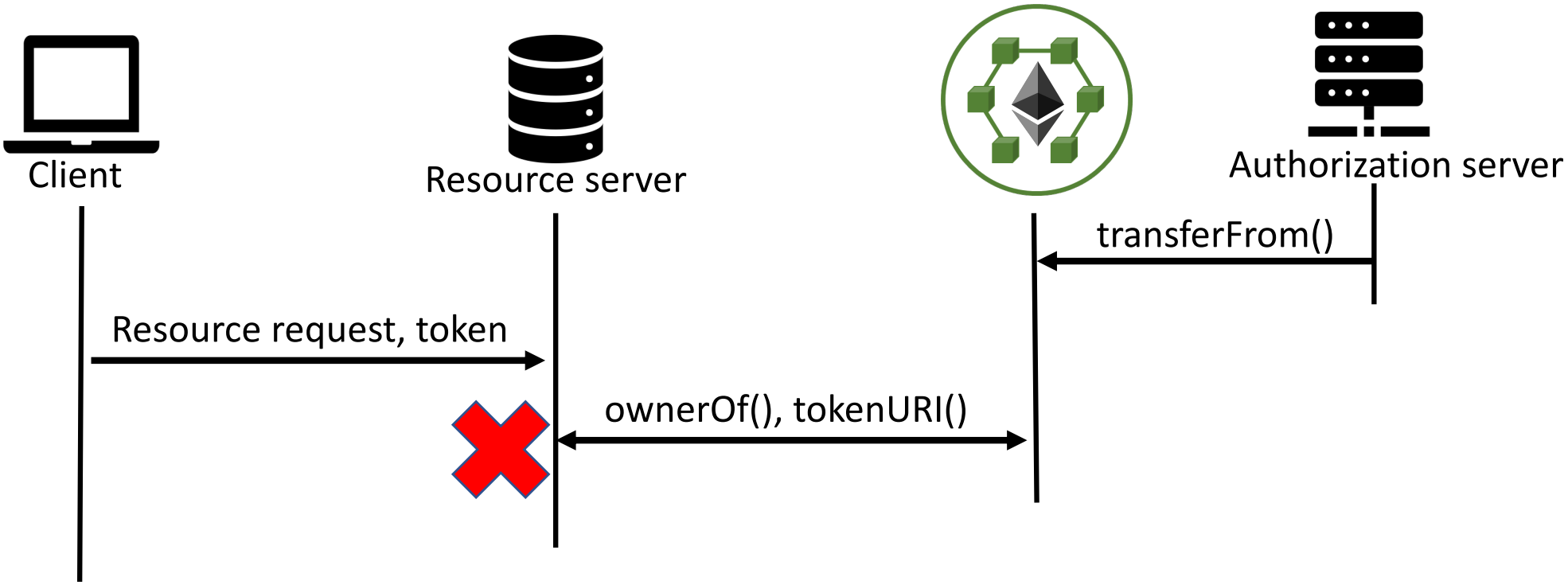


- It facilitates logging and auditing services
- Clients can at any time retrieve their access token from the blockchain

Accessing resource servers with BC read access

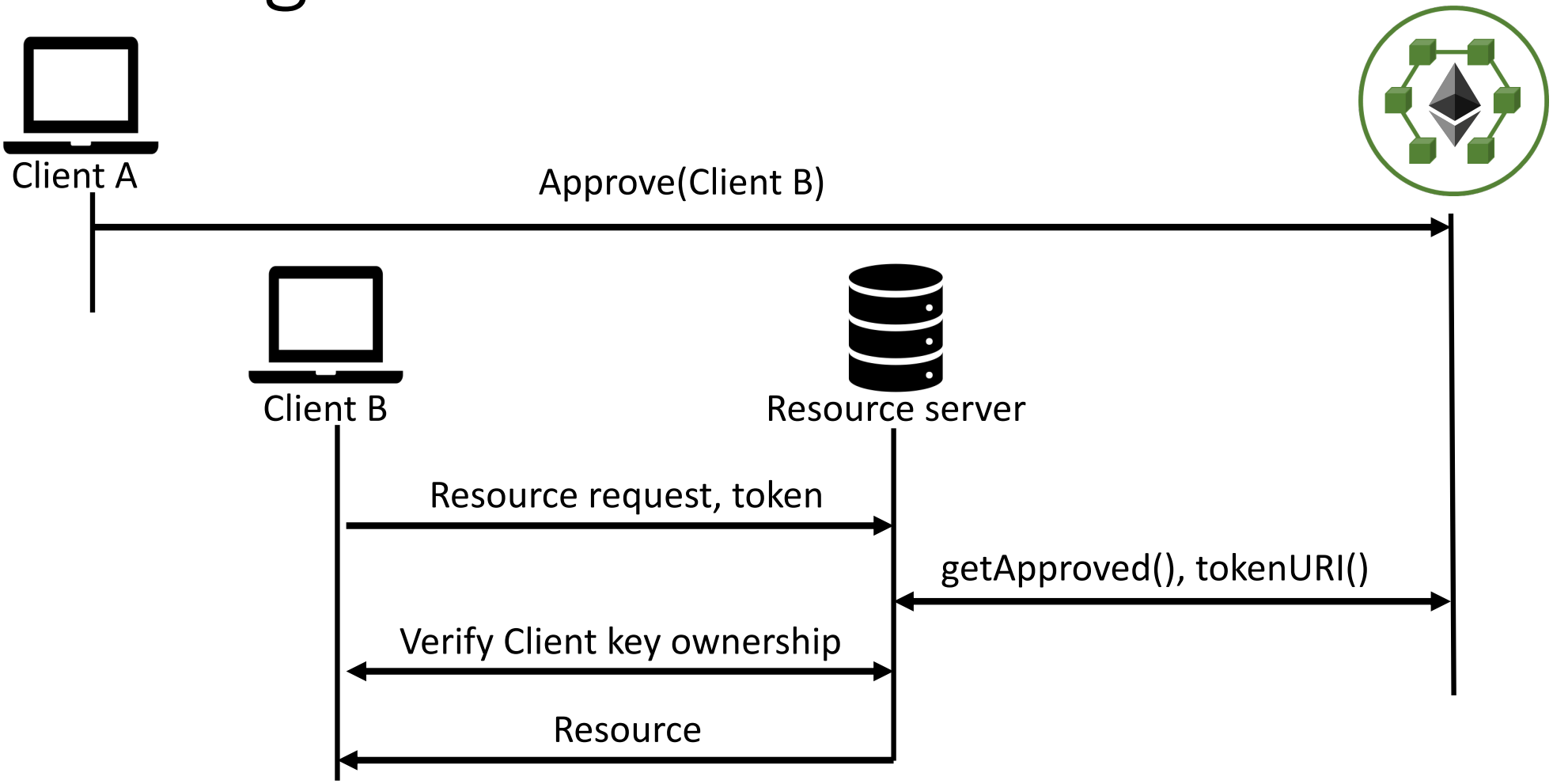


Revocation



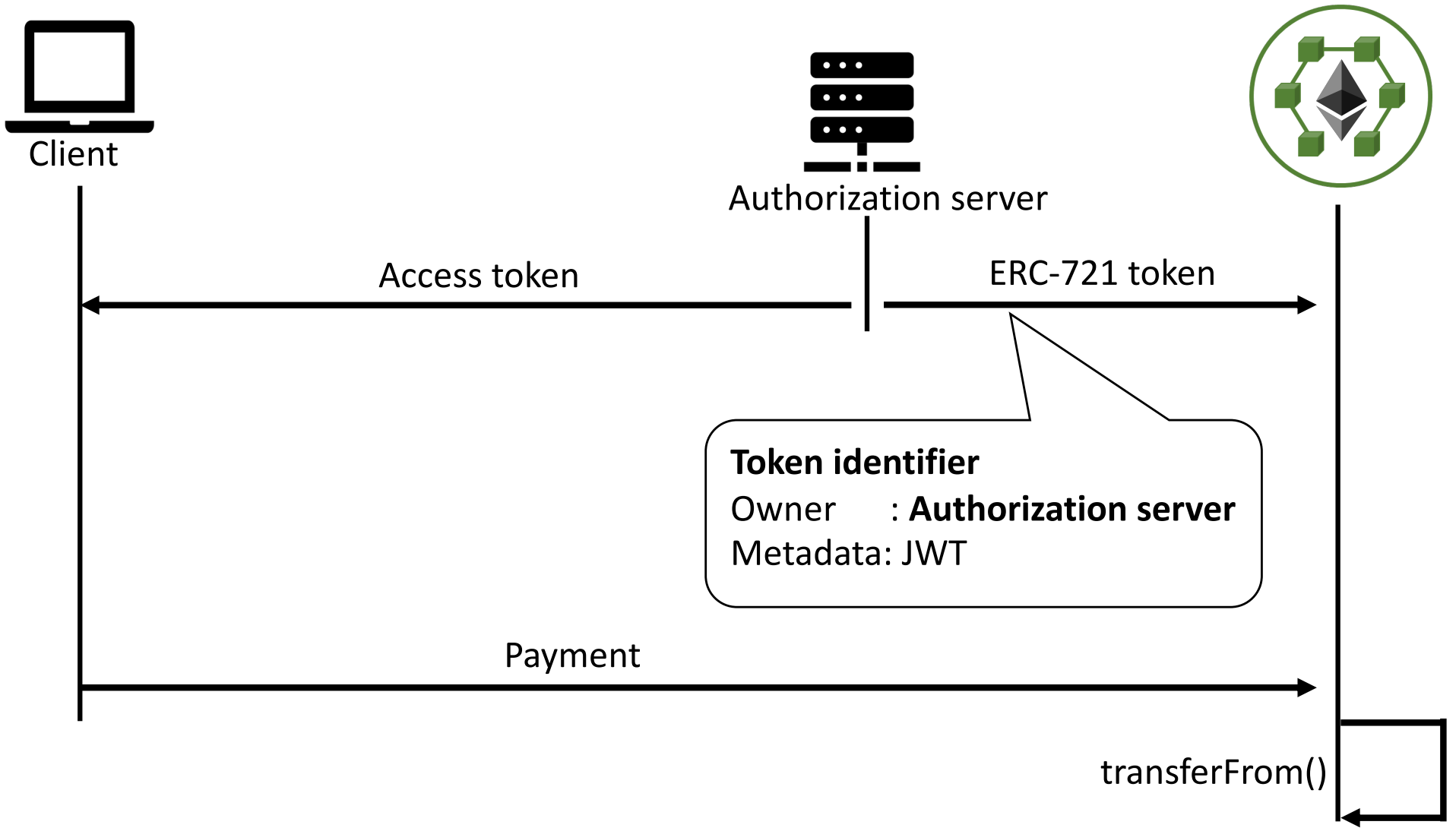
- Revocation is asynchronous
- Authorization server does not have to be online

Delegation



- Delegation is not transitive
- Revocation is not affected

Fair exchange



Discussion

- Existing OAuth 2.0 code-base can be re-used
  - In some cases our approach is transparent to OAuth endpoints
- In no payments are involved then private, or testing chains can be used.
- If the client does not interact with the blockchain, then ownerOf() may return any type of identifier.
- (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)

Thank you

fotiou@aueb.gr

https://mm.aueb.gr/blockchains