Protecting Your APIs with OAuth

Dan Moore

Beer City Code

Aug 6, 2022

@mooreds

About FusionAuth

- Authentication and Authorization
- Built for Devs, by Devs
- Empower Core Competencies
- Protect APIs
- 10M+ downloads

About Me

About Me

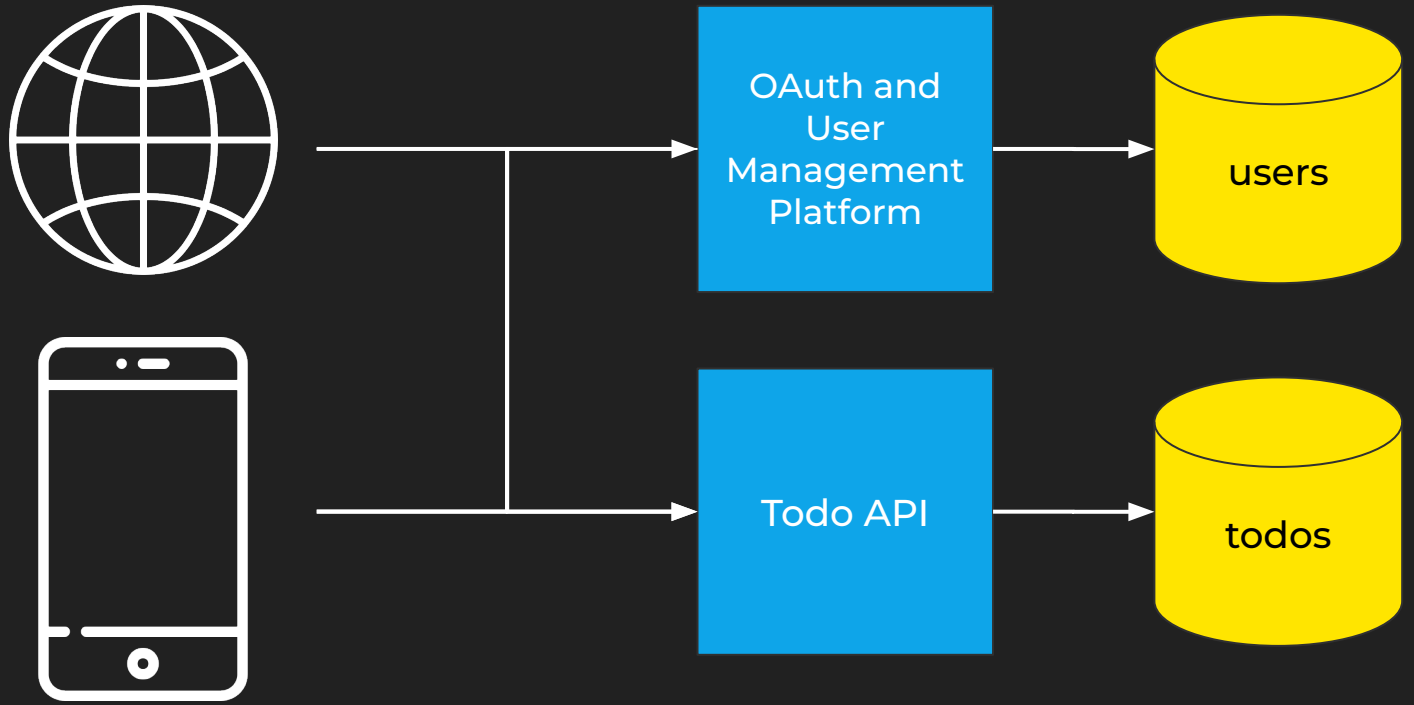
- Who cares

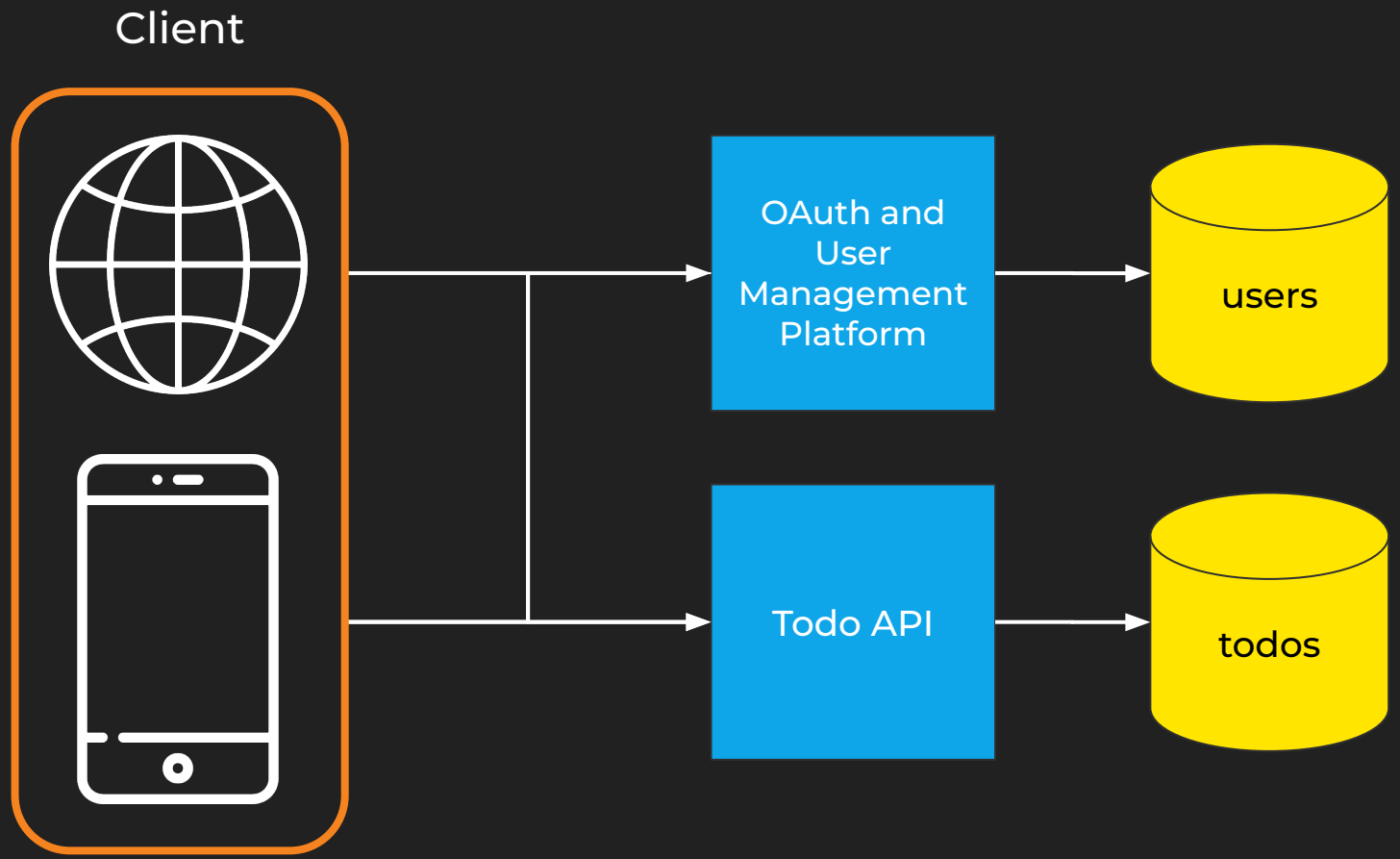
Questions

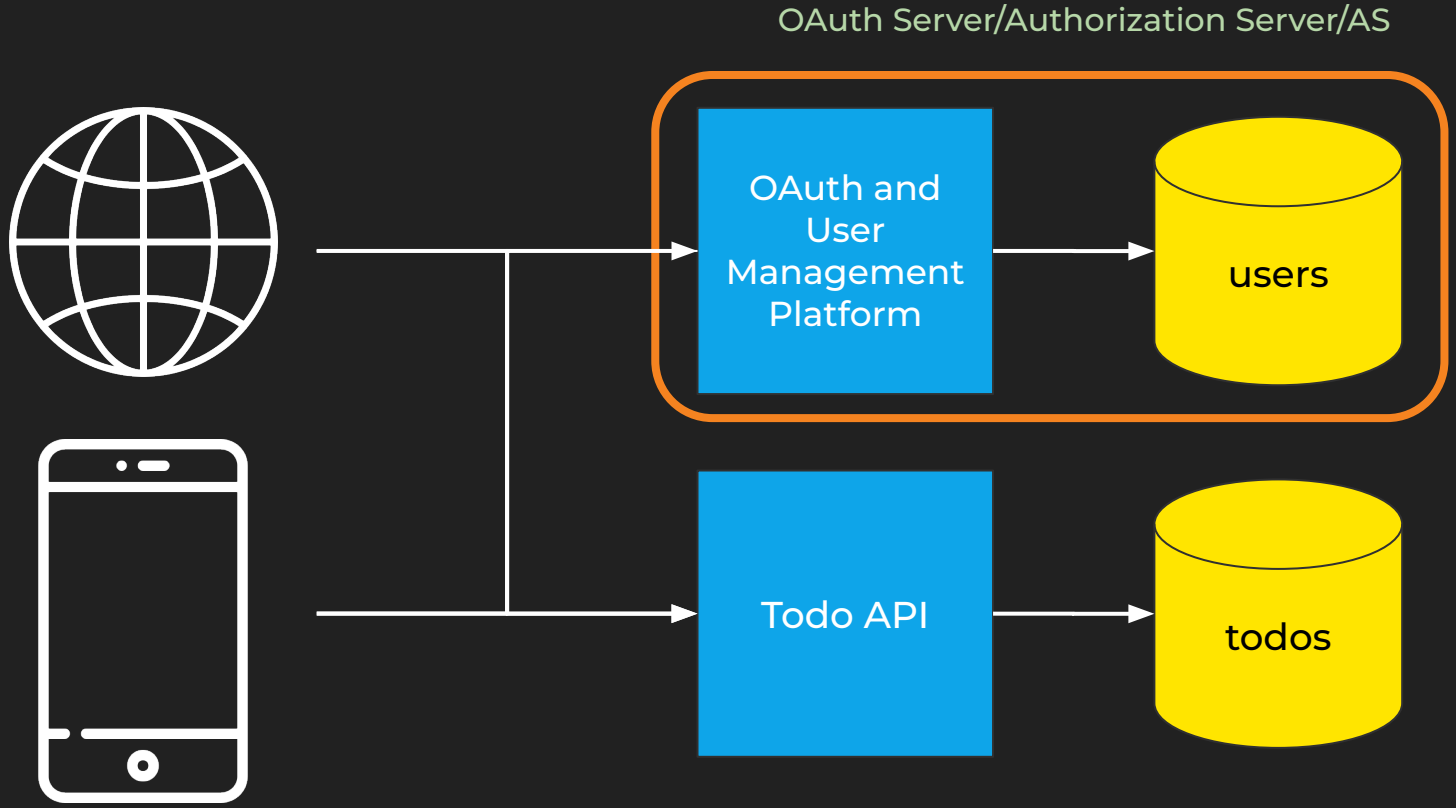
- Just ask

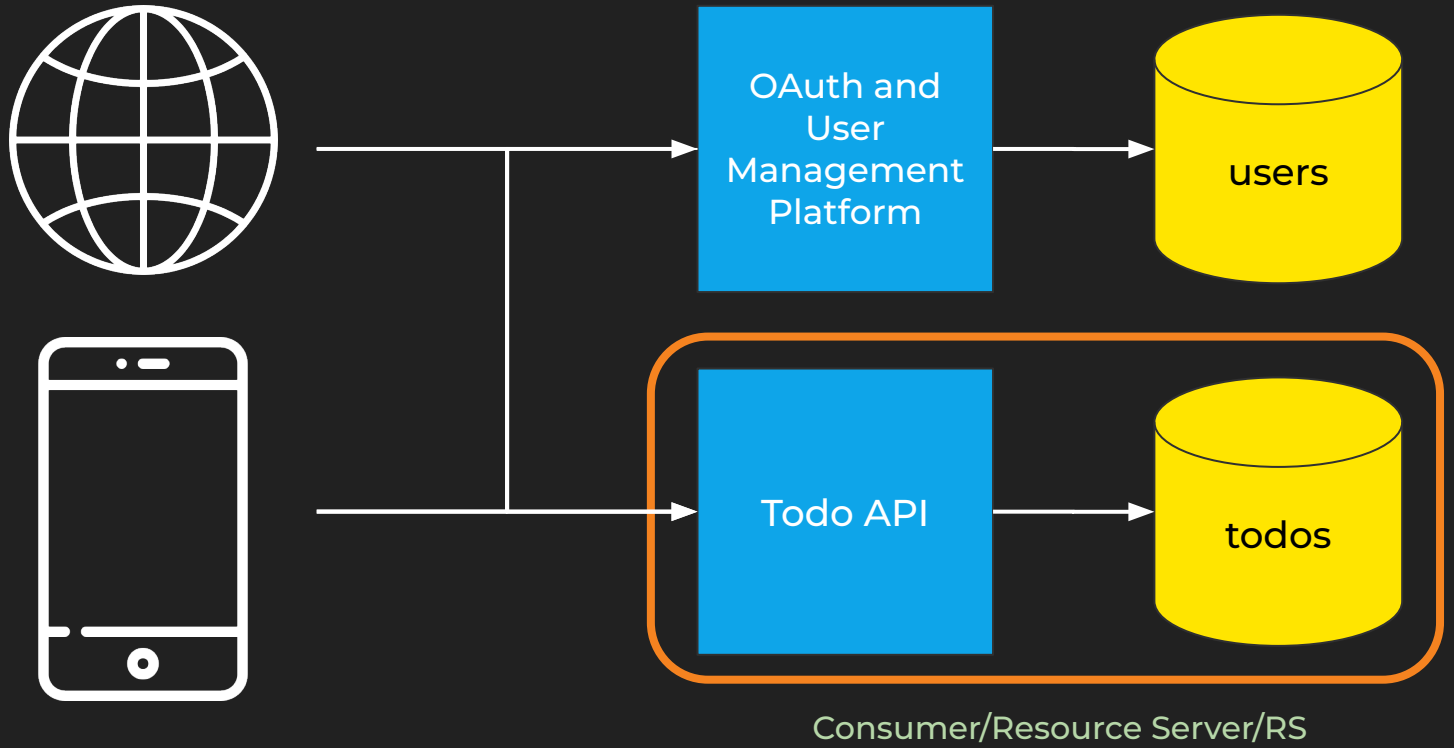
What We'll Cover

- OAuth
- Get tokens
- Tokens
- Care for tokens
  - Client
  - Consumer
- Not Google


OAuth and User Management Platform
users
Todo API
todos

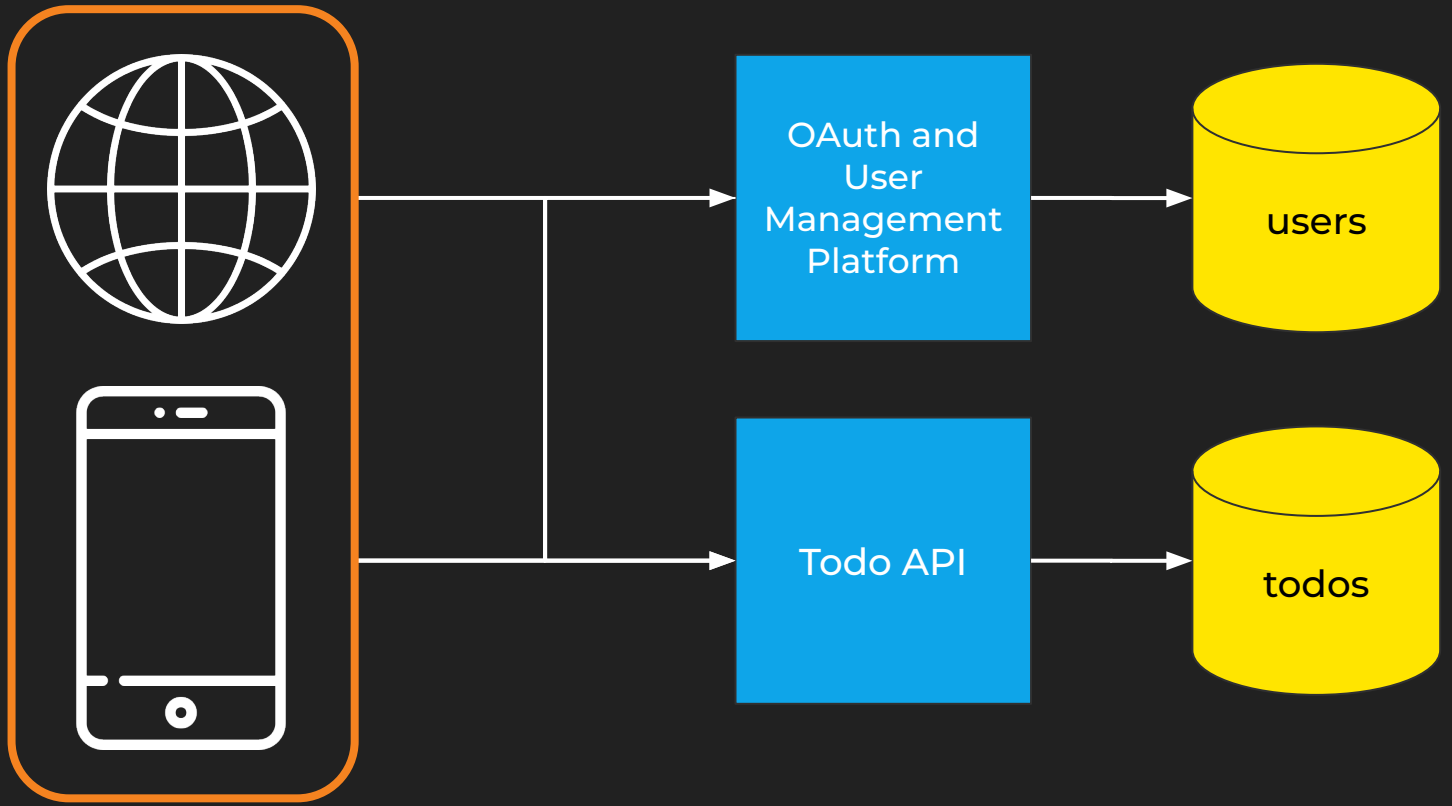

Client
OAuth and User Management Platform
users
Todo API
todos

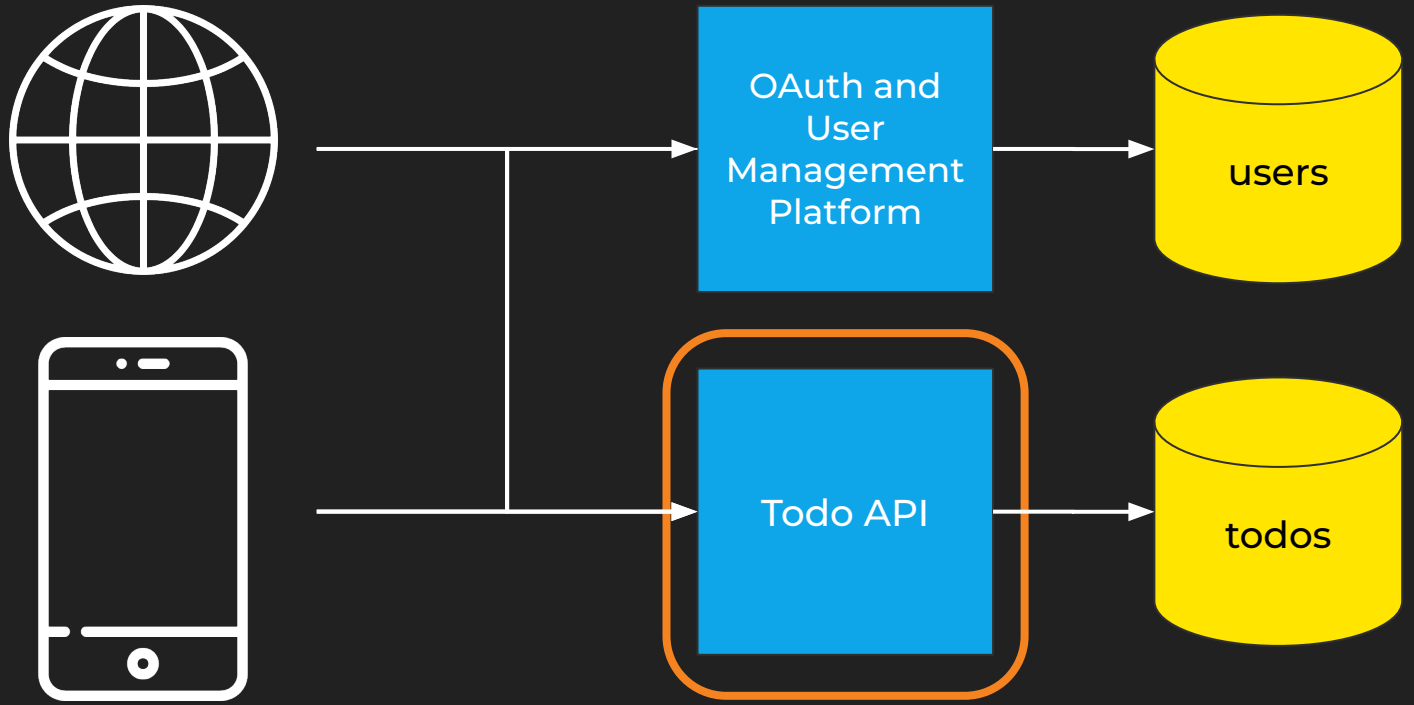

OAuth Server/Authorization Server/AS
OAuth and User Management Platform
users
Todo API
todos

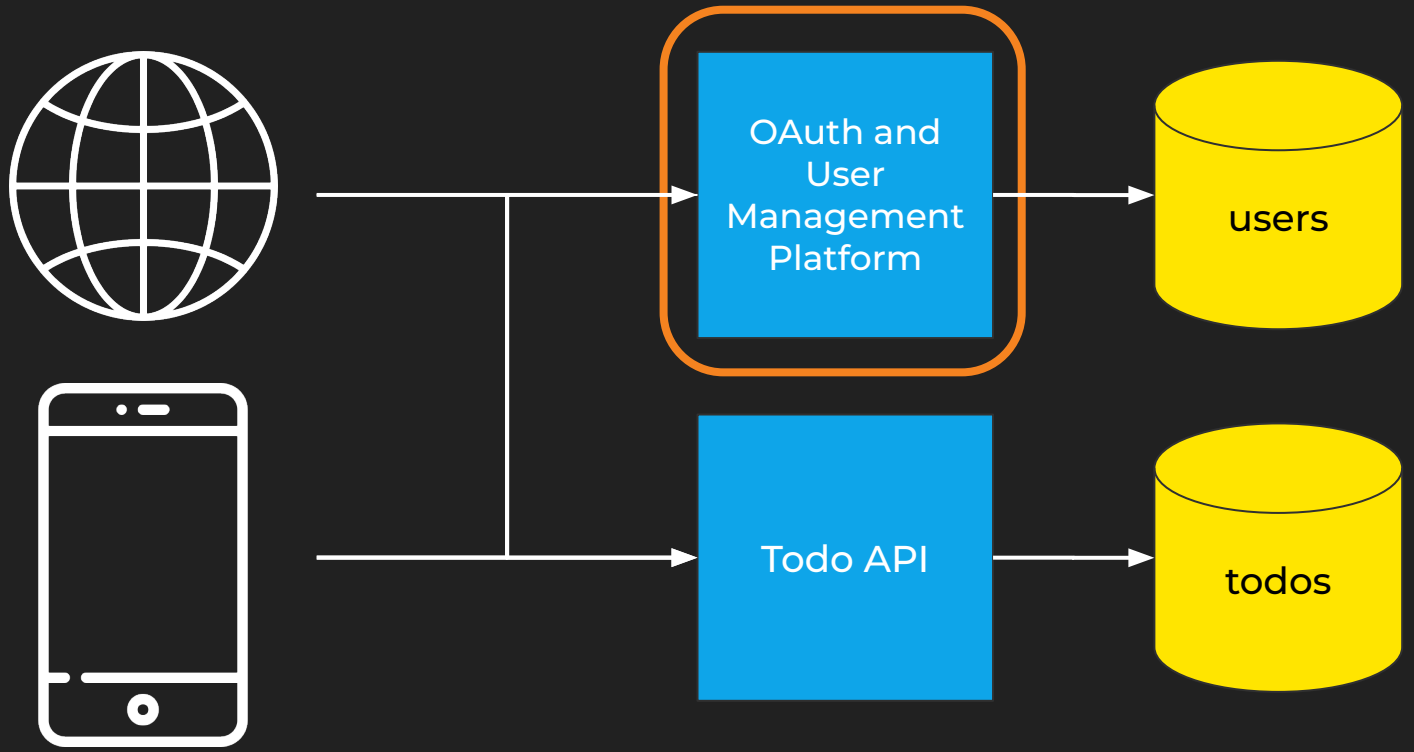

OAuth and User Management Platform
users
Todo API
todos
Consumer/Resource Server/RS

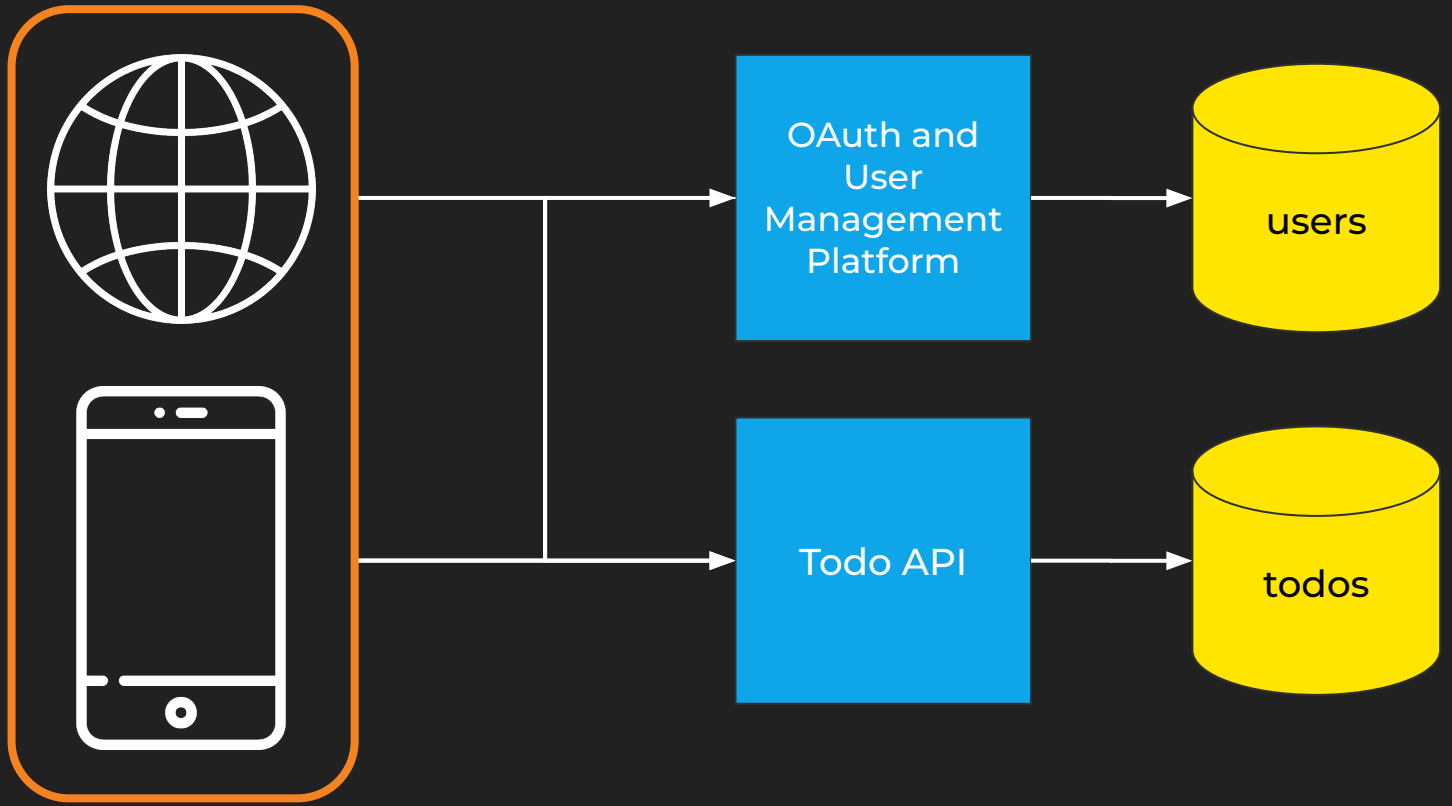
What Problem
Does OAuth Solve?

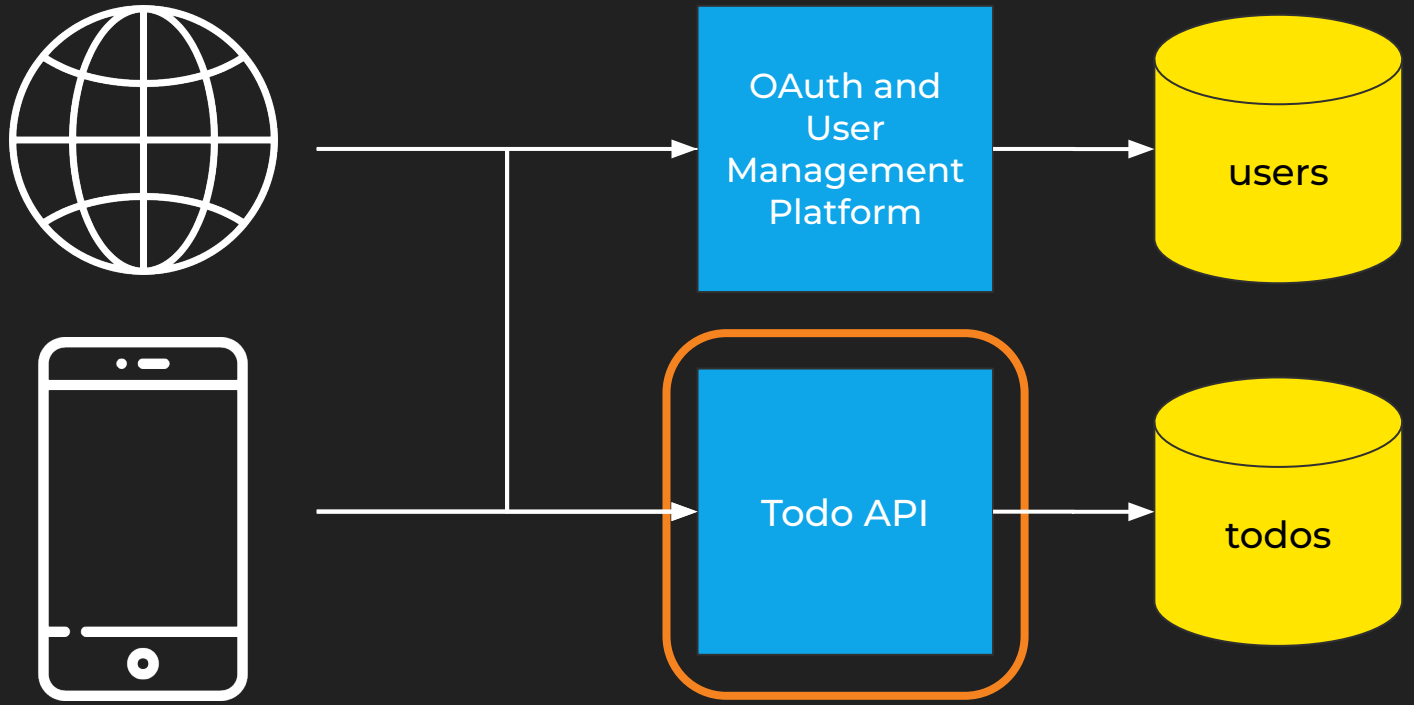
Secure
Delegated
Access


OAuth and User Management Platform
users
Todo API
todos


OAuth and User Management Platform
users
Todo API
todos


OAuth and User Management Platform
users
Todo API
todos


OAuth and User Management Platform
users
Todo API
todos

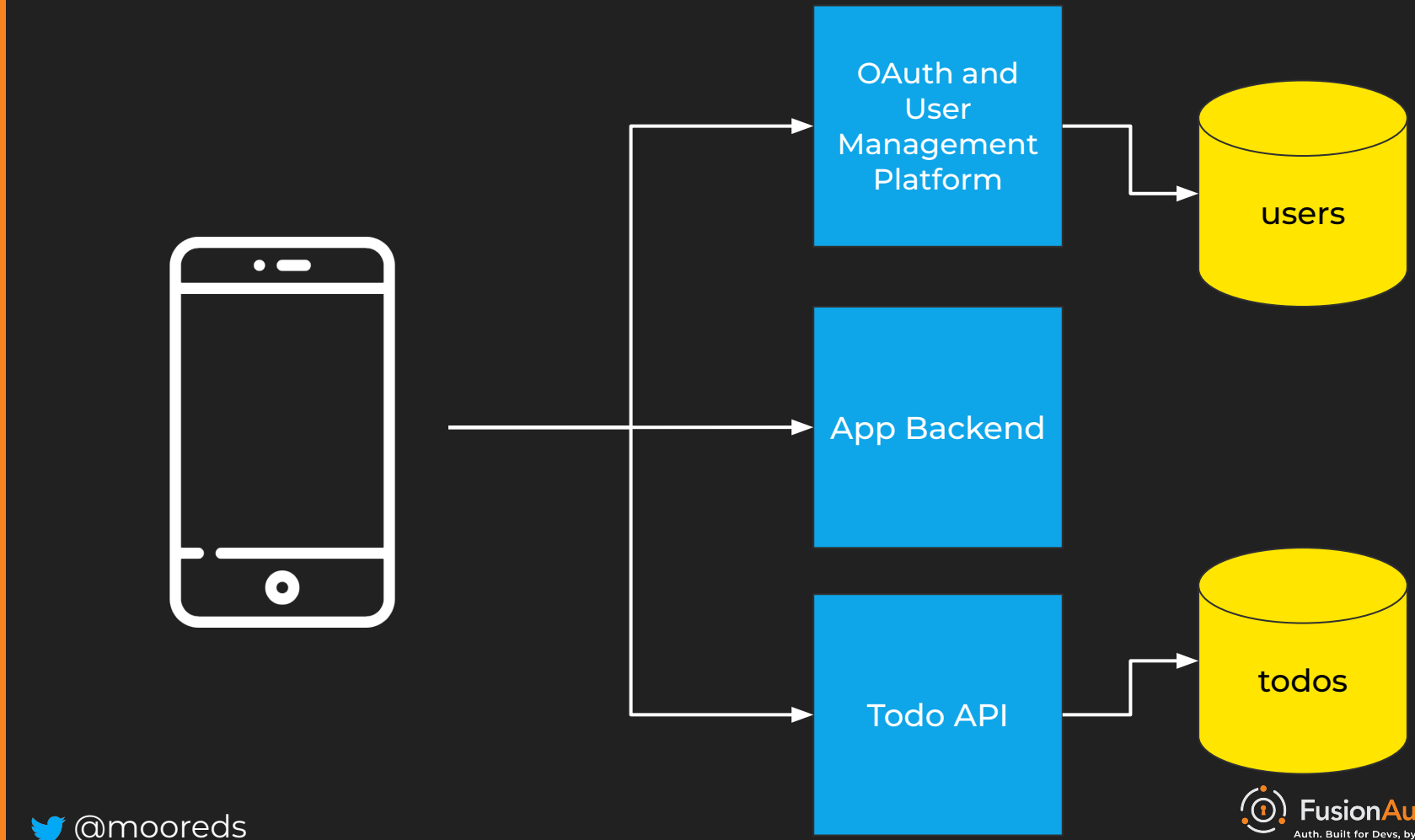

OAuth and User Management Platform
users
Todo API
todos

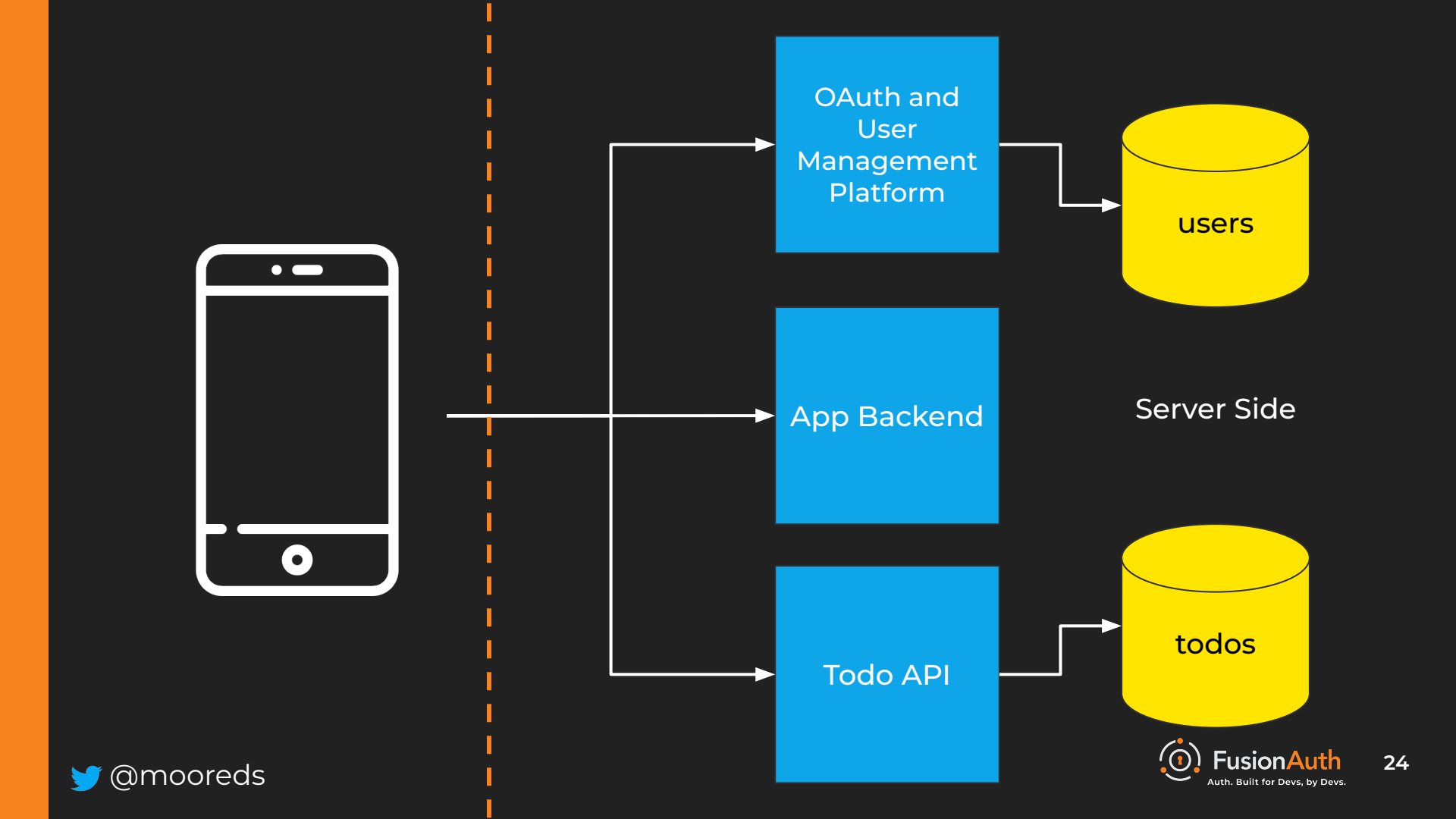
How To Get a Token

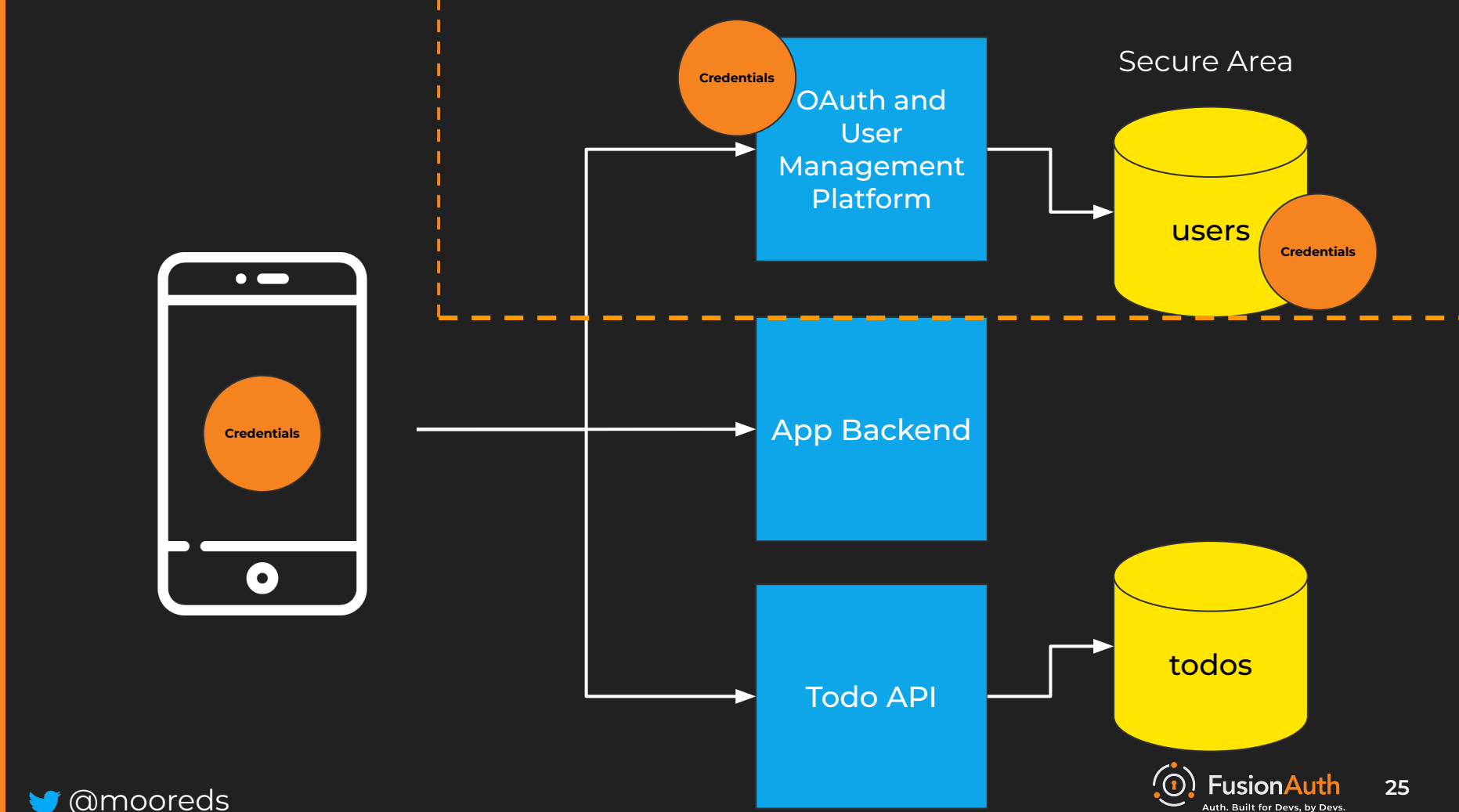
Authorization Code Grant

Client Credentials Grant

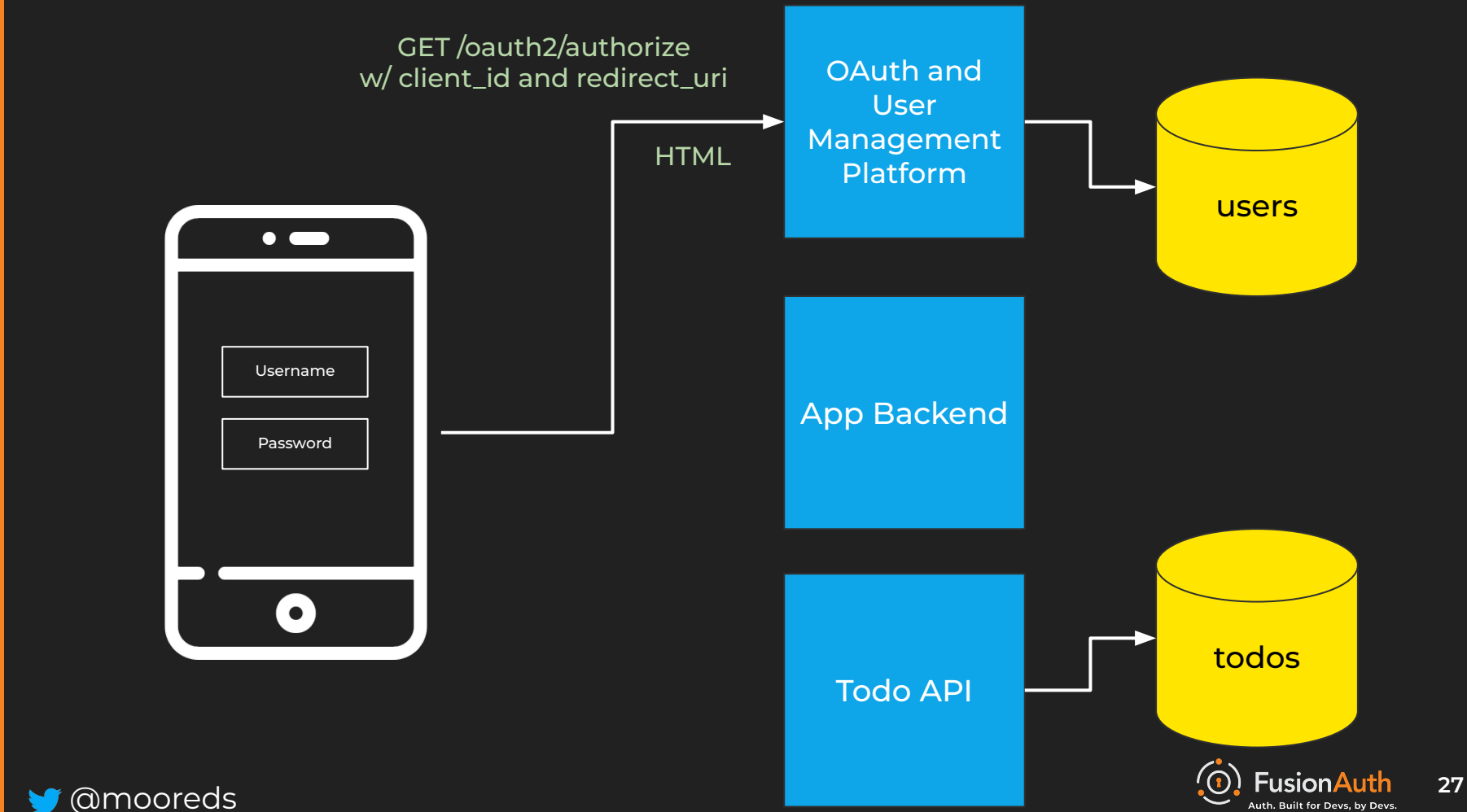
Authorization Code Grant

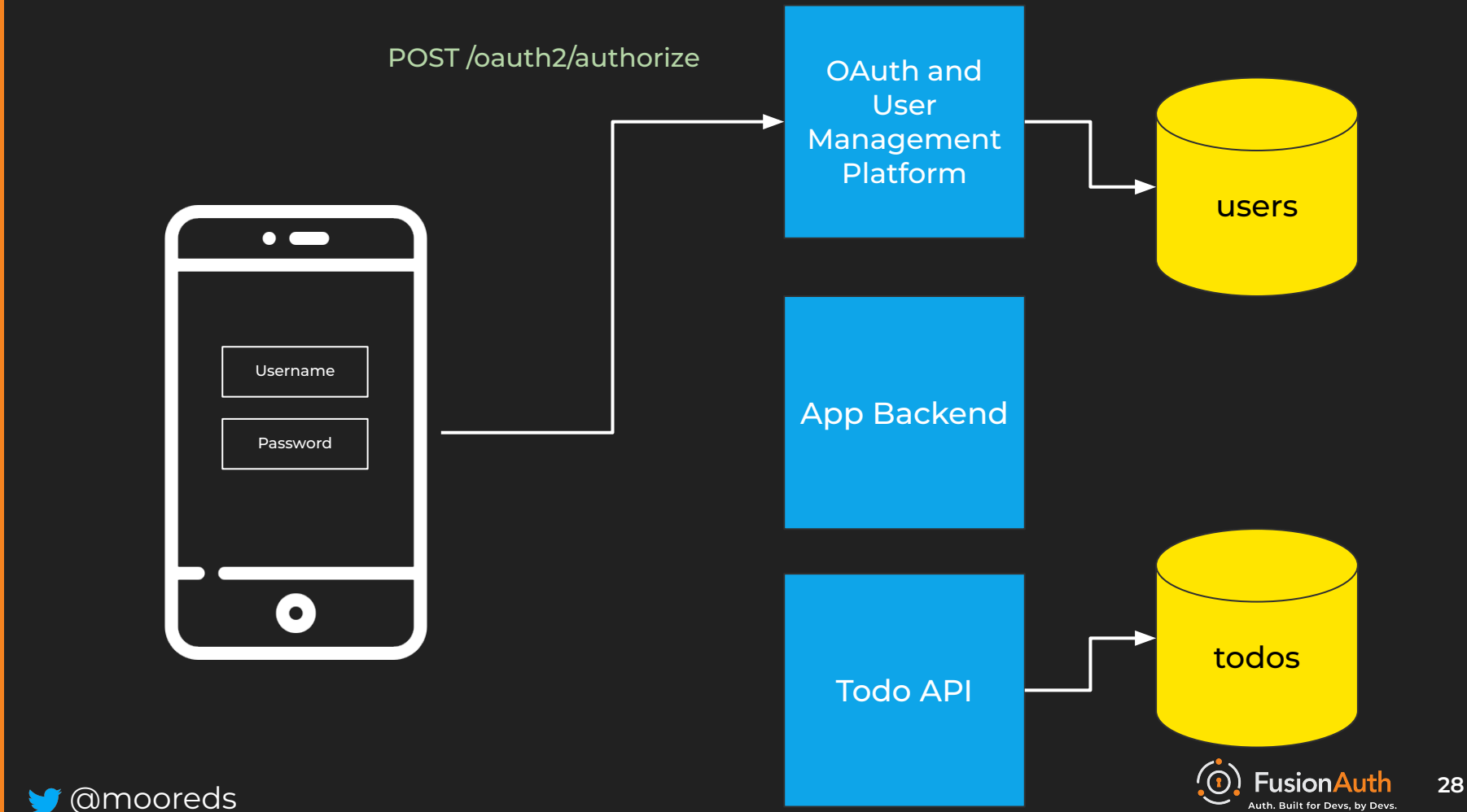

OAuth and User Management Platform
users
App Backend
Todo API
todos

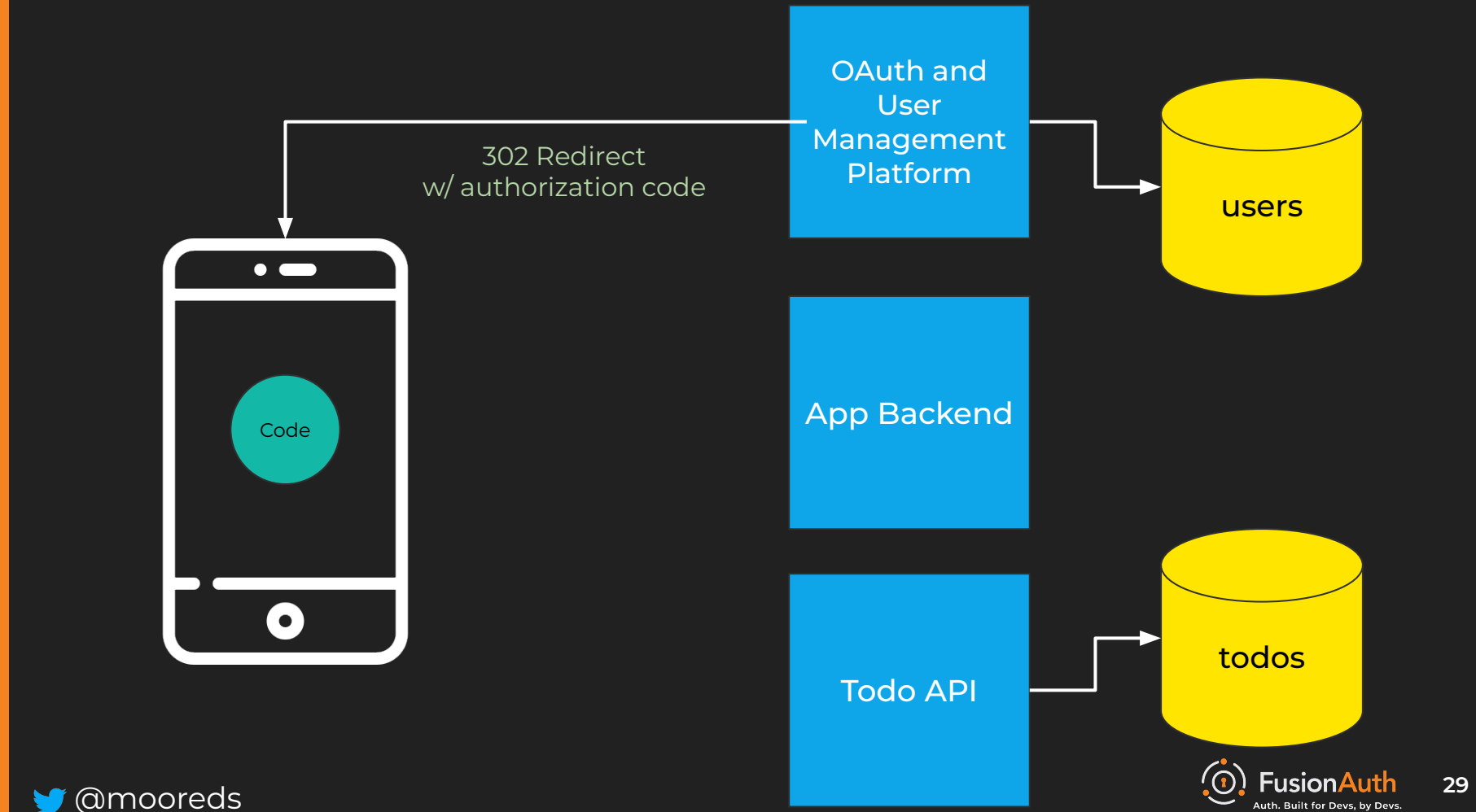

OAuth and User Management Platform
users
App Backend
Server Side
Todo API
todos


Credentials
OAuth and User Management Platform
Secure Area
users
Credentials
Credentials
App Backend
Todo API
todos

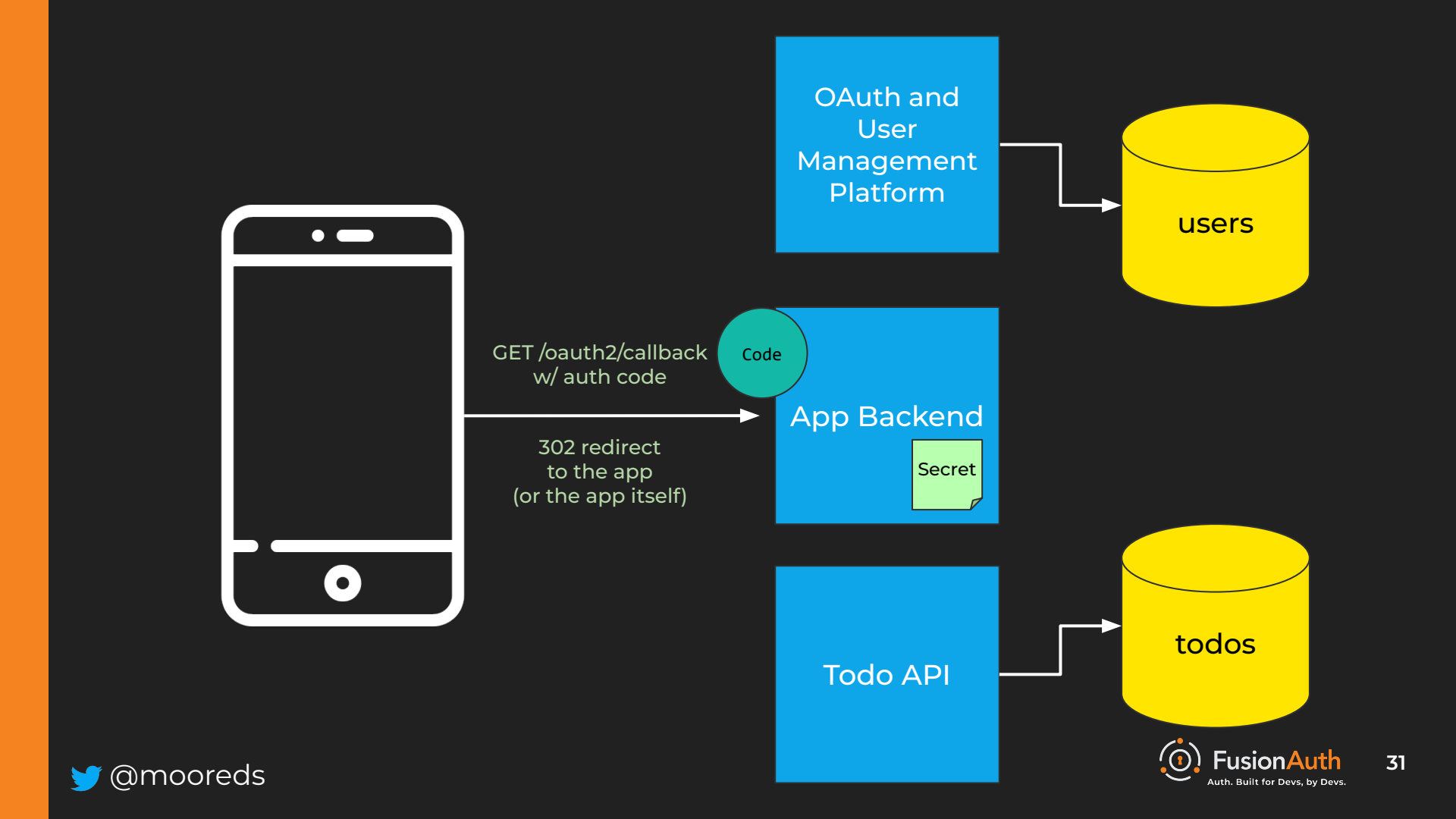
How Does the Authorization Code Grant **Work?**

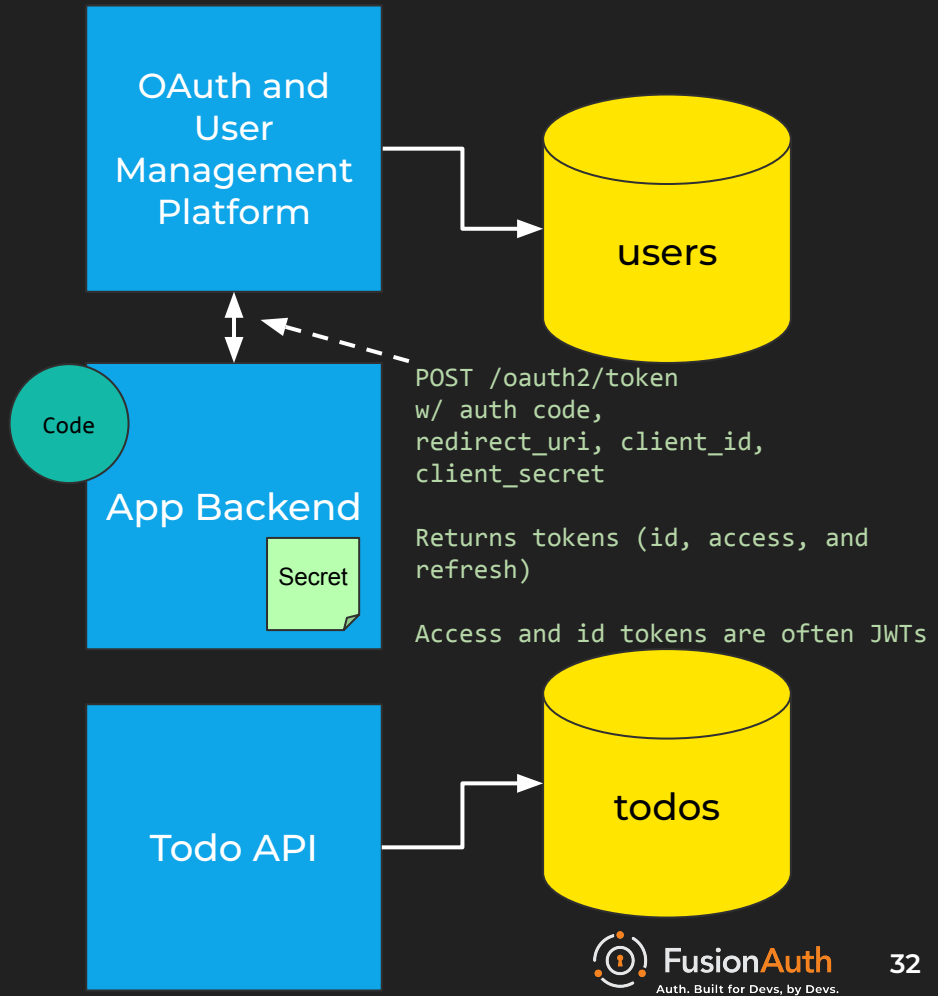

GET /oauth2/authorize
w/ client_id and redirect_uri
HTML
OAuth and User Management Platform
users
Username
Password
App Backend
Todo API
todos

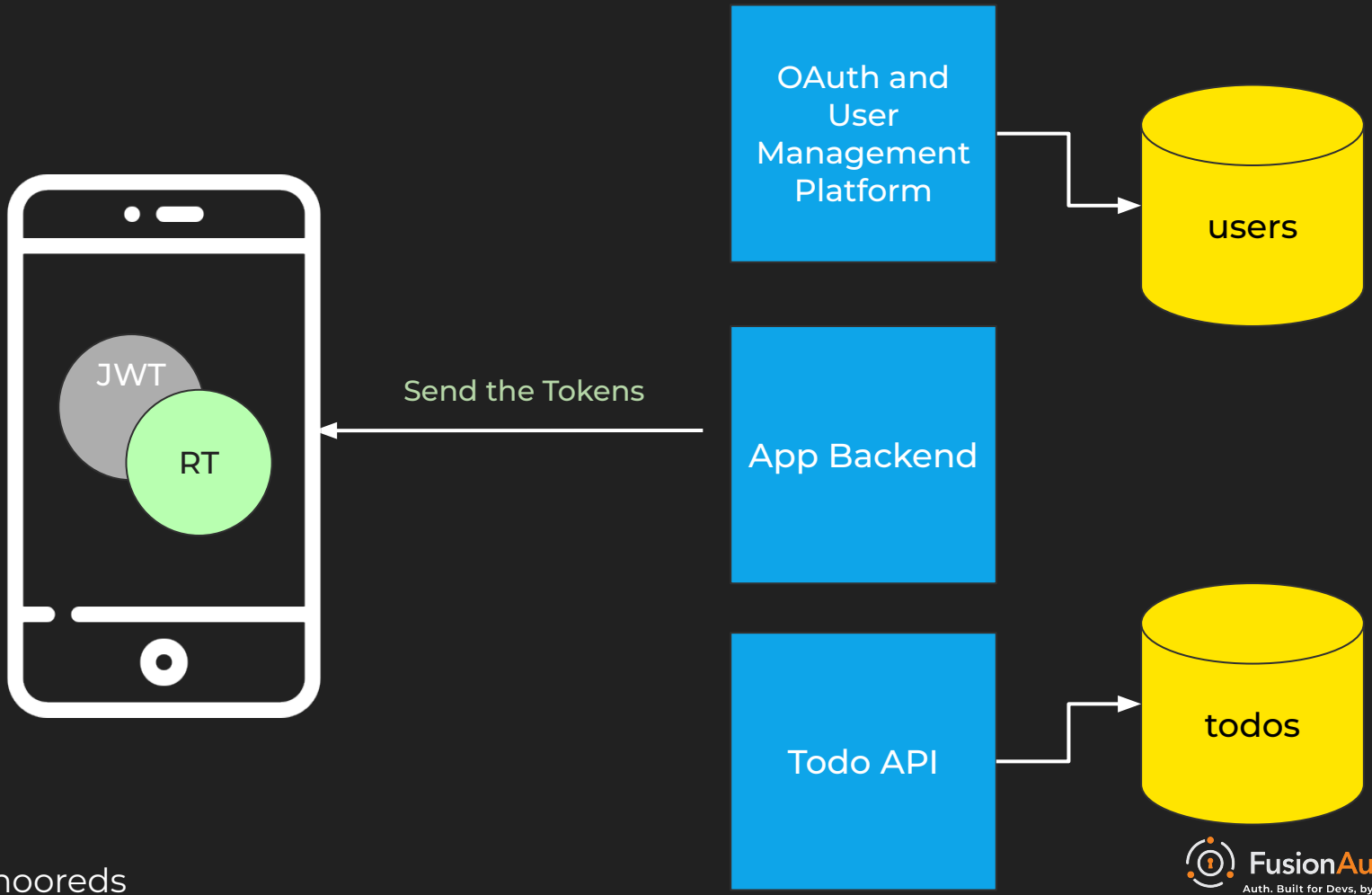

POST /oauth2/authorize
OAuth and User Management Platform
users
Username
Password
App Backend
Todo API
todos

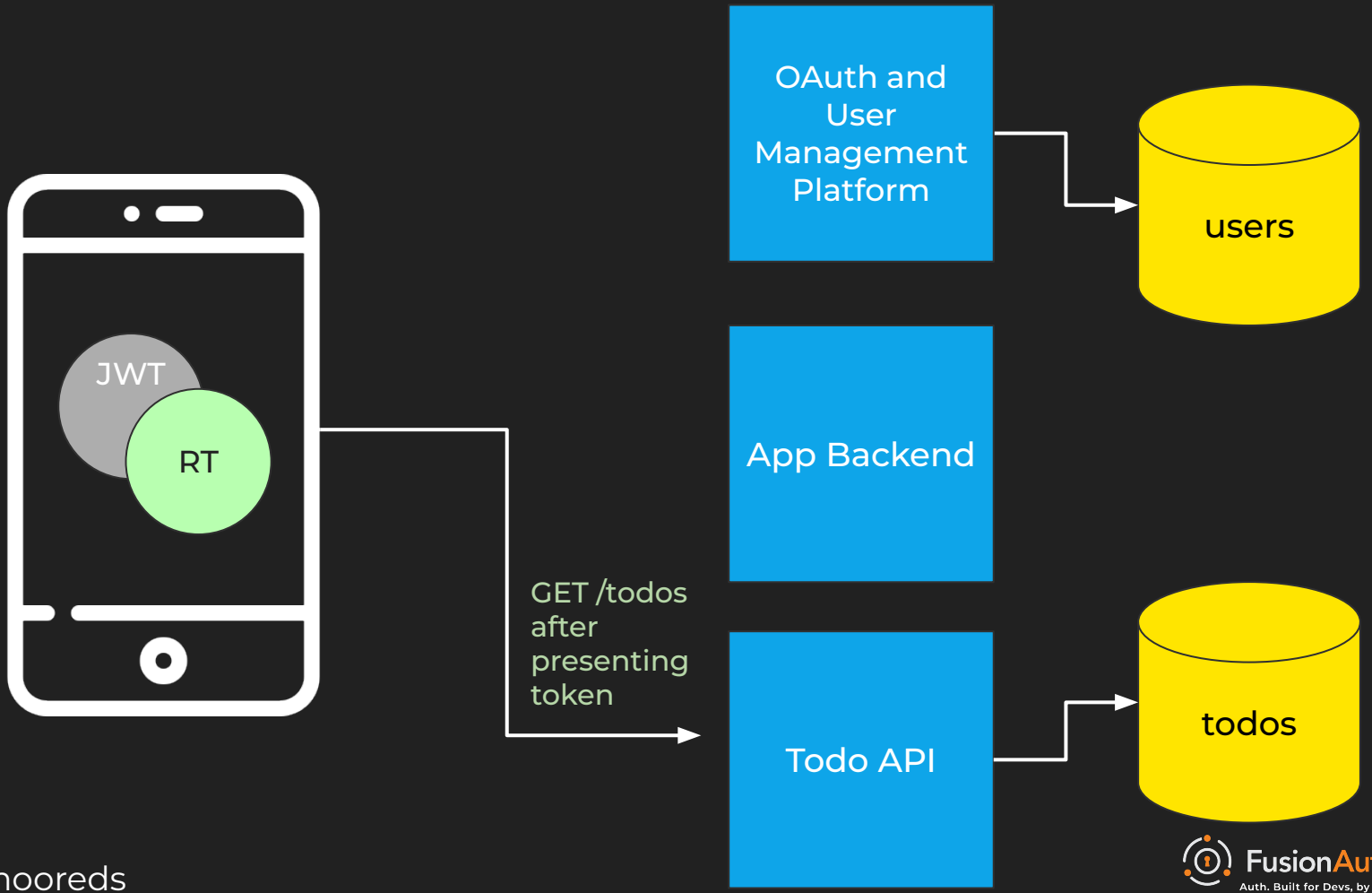

OAuth and User Management Platform
users
302 Redirect
w/ authorization code
Code
App Backend
Todo API
todos

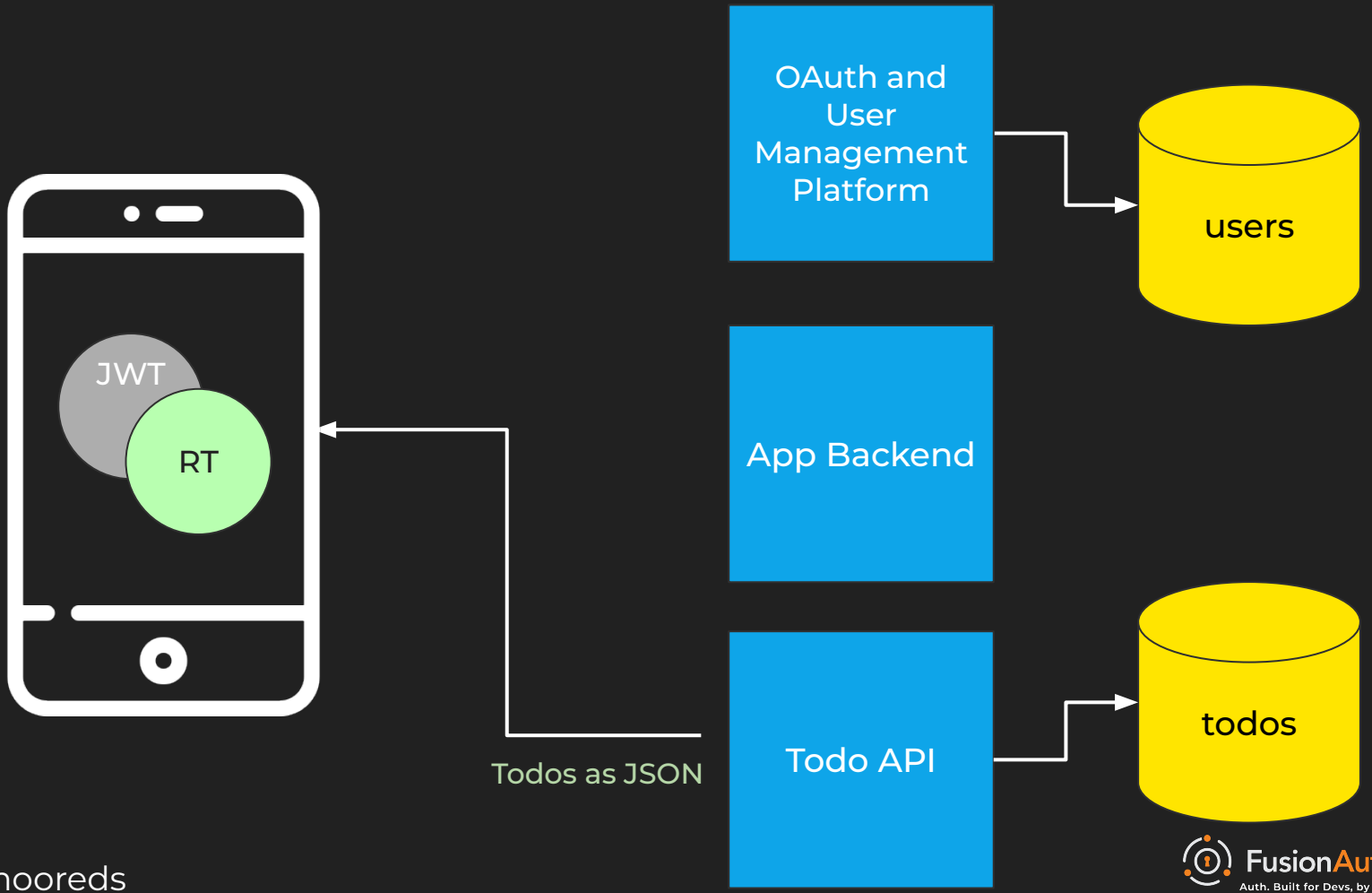
SplxlOBeZQQYbYS6WxSbIA


OAuth and User Management Platform
users
GET /oauth2/callback w/ auth code
Code
App Backend
Secret
302 redirect to the app (or the app itself)
Todo API
todos

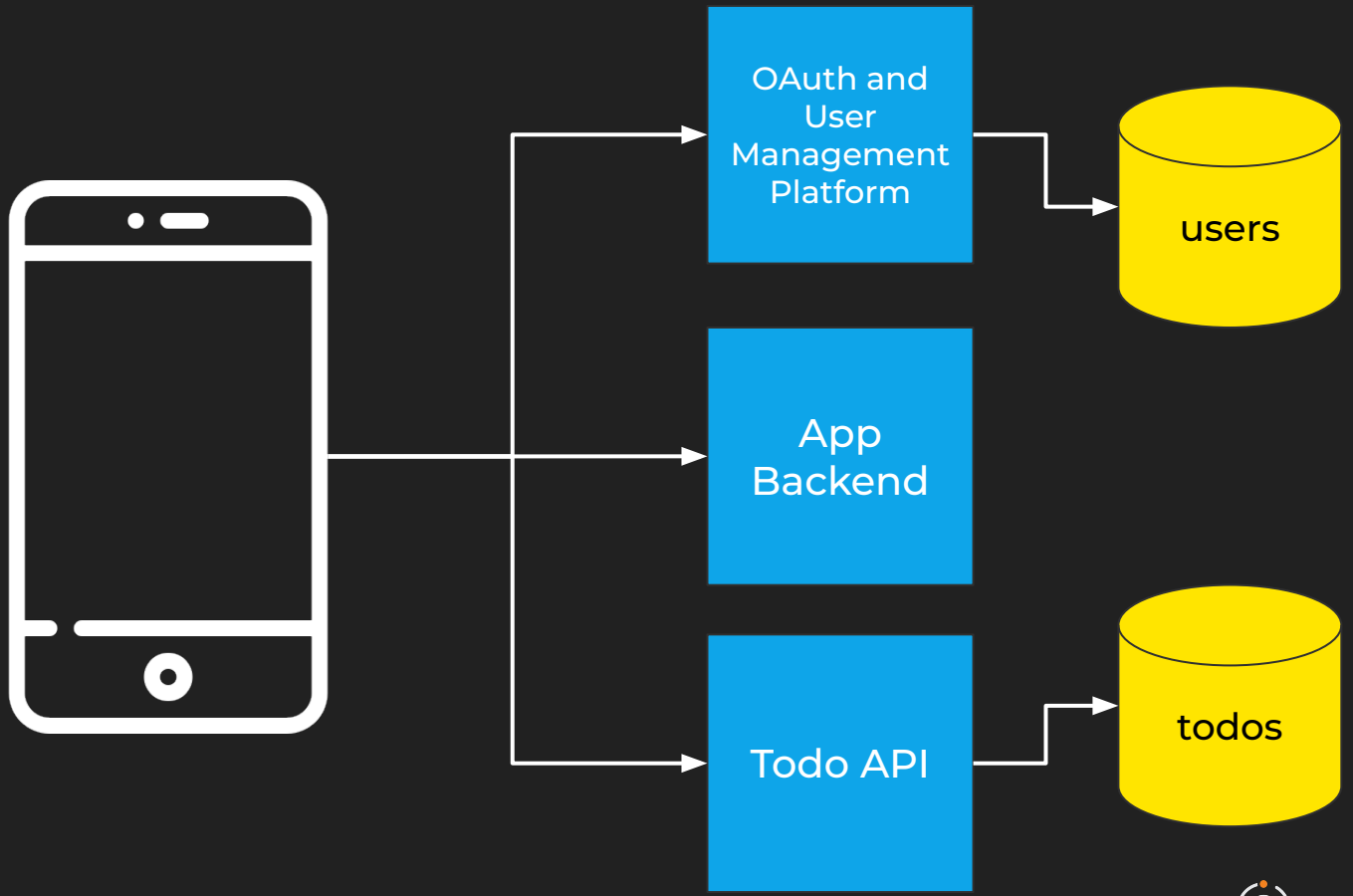

OAuth and User Management Platform
users
Code
App Backend
Secret
POST /oauth2/token
w/ auth code,
redirect_uri, client_id,
client_secret
Returns tokens (id, access, and refresh)
Access and id tokens are often JWTs
Todo API
todos


OAuth and User Management Platform
users
JWT
RT
Send the Tokens
App Backend
Todo API
todos

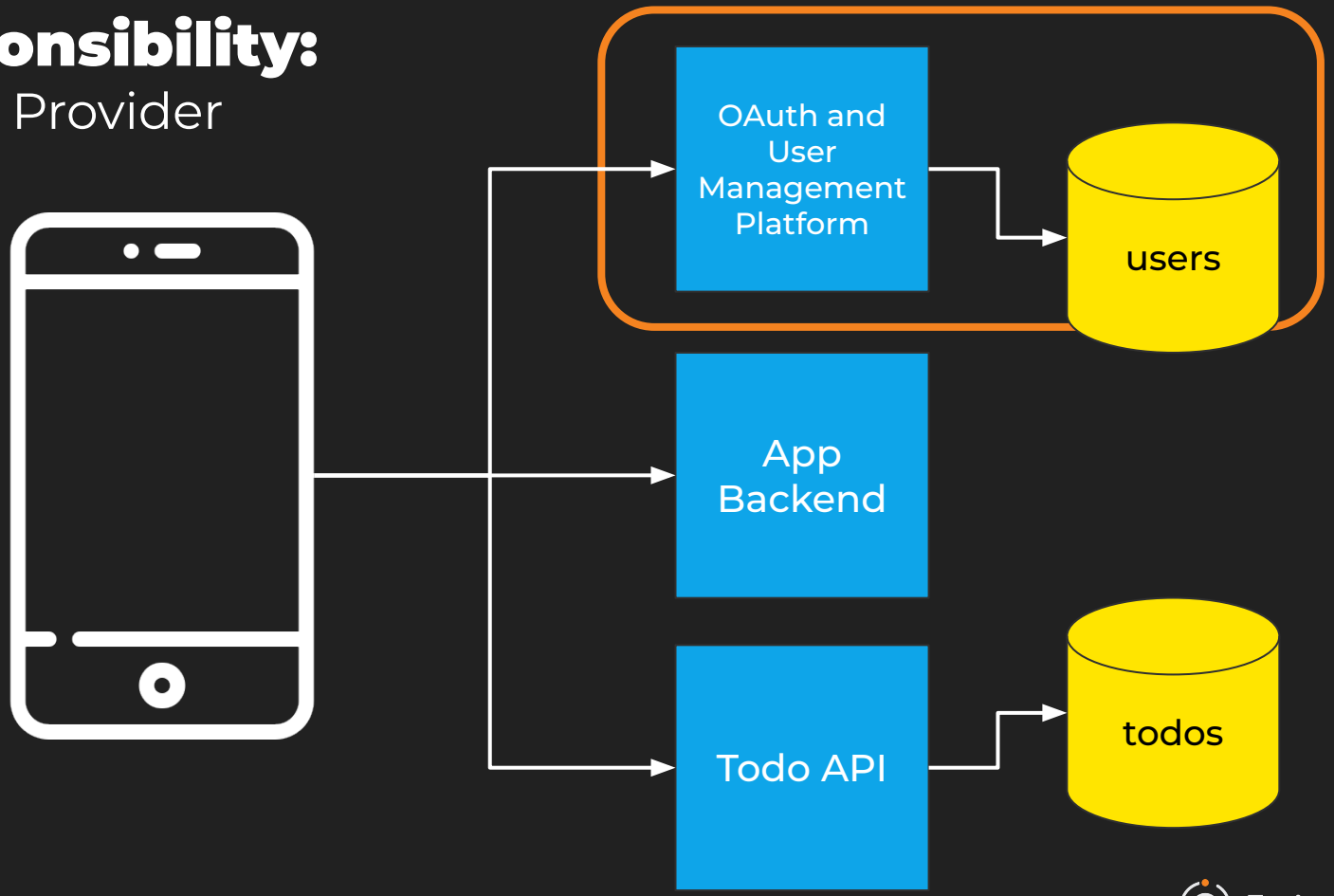

OAuth and User Management Platform
users
JWT
RT
App Backend
GET /todos after presenting token
Todo API
todos


OAuth and User Management Platform
users
JWT
RT
App Backend
Todos as JSON
Todo API
todos

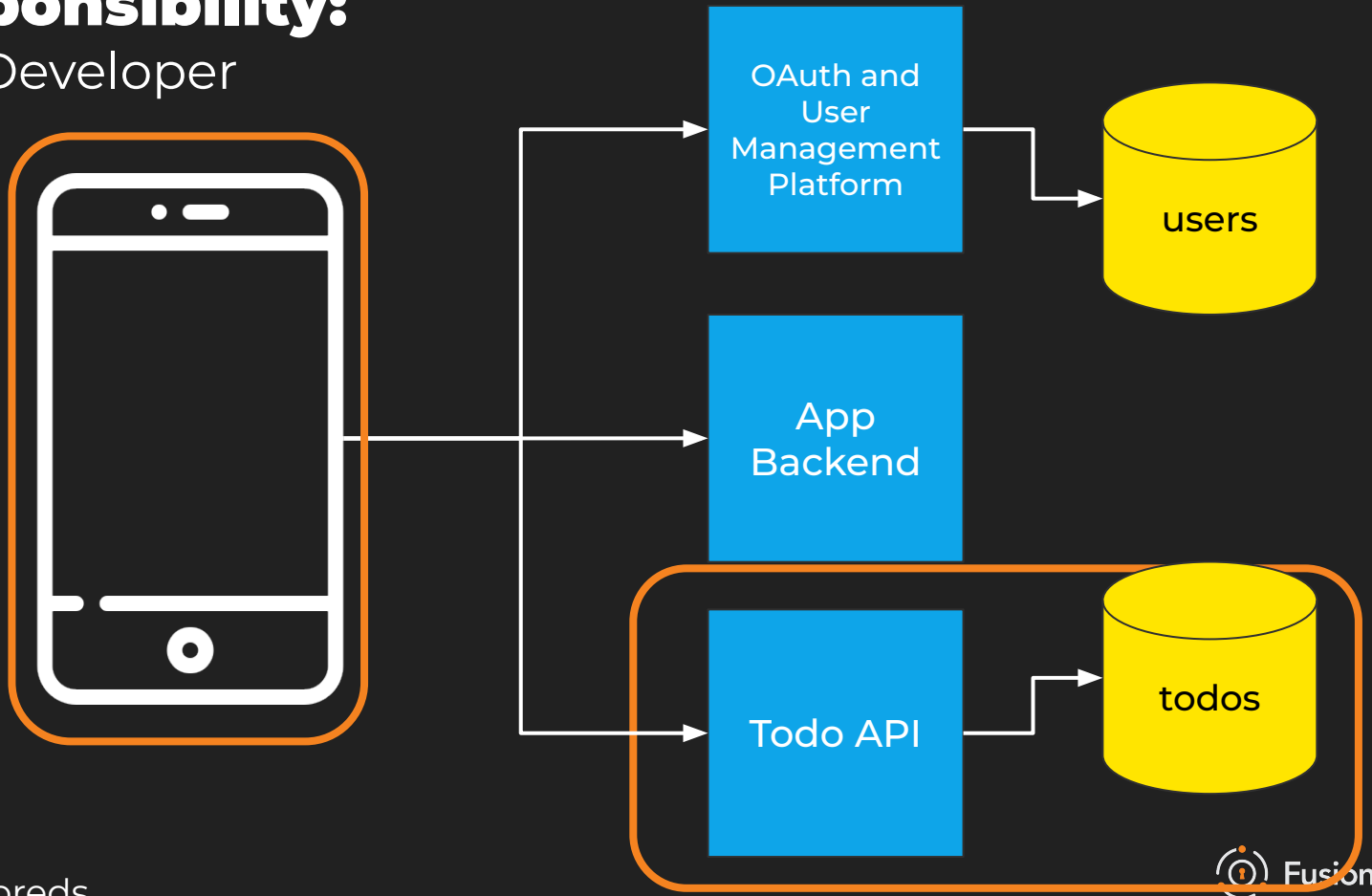
Responsibilities


OAuth and User Management Platform
users
App Backend
Todo API
todos

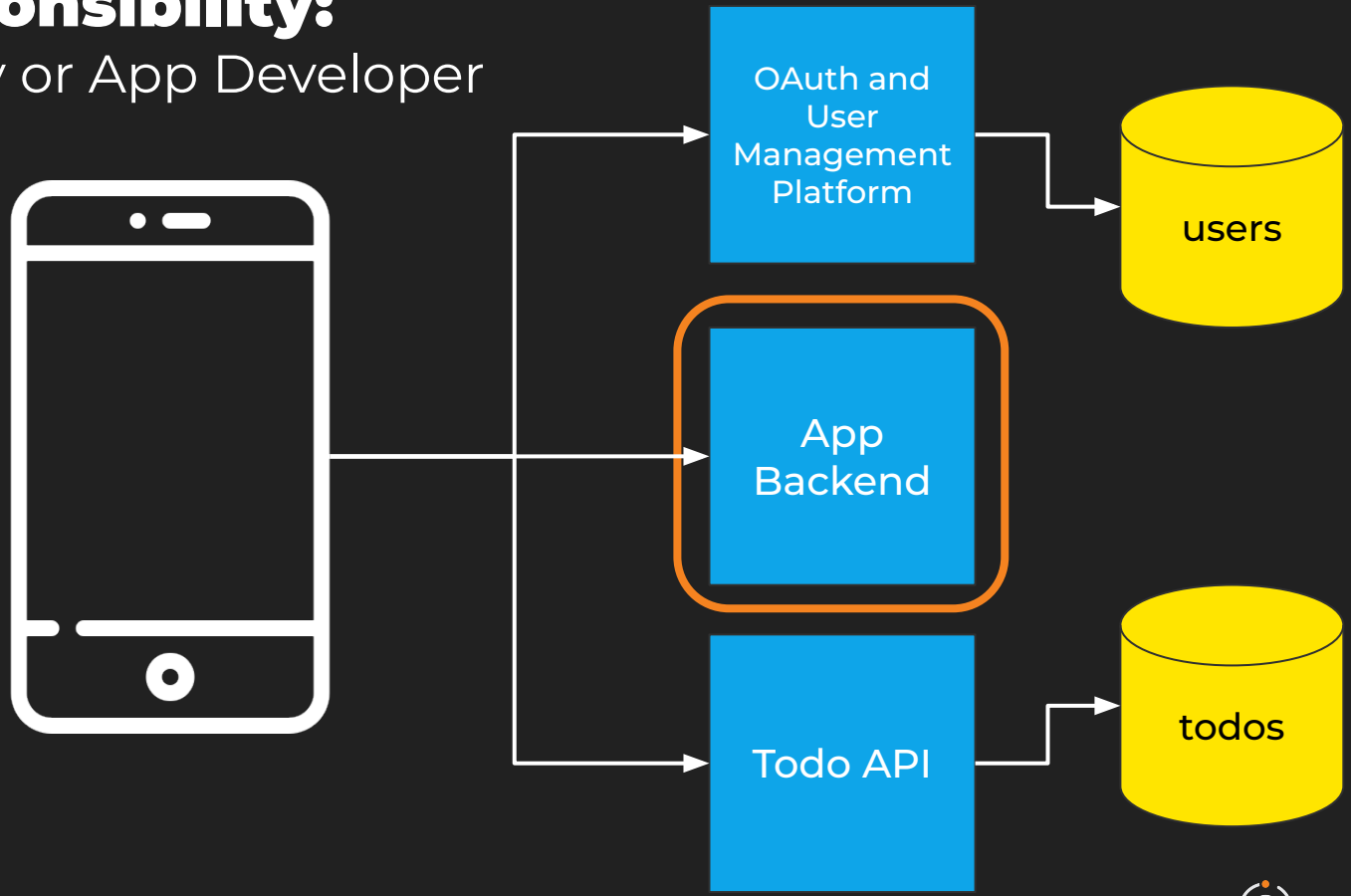
Responsibility:
OAuth Provider



Responsibility:
App Developer



Responsibility:
Library or App Developer



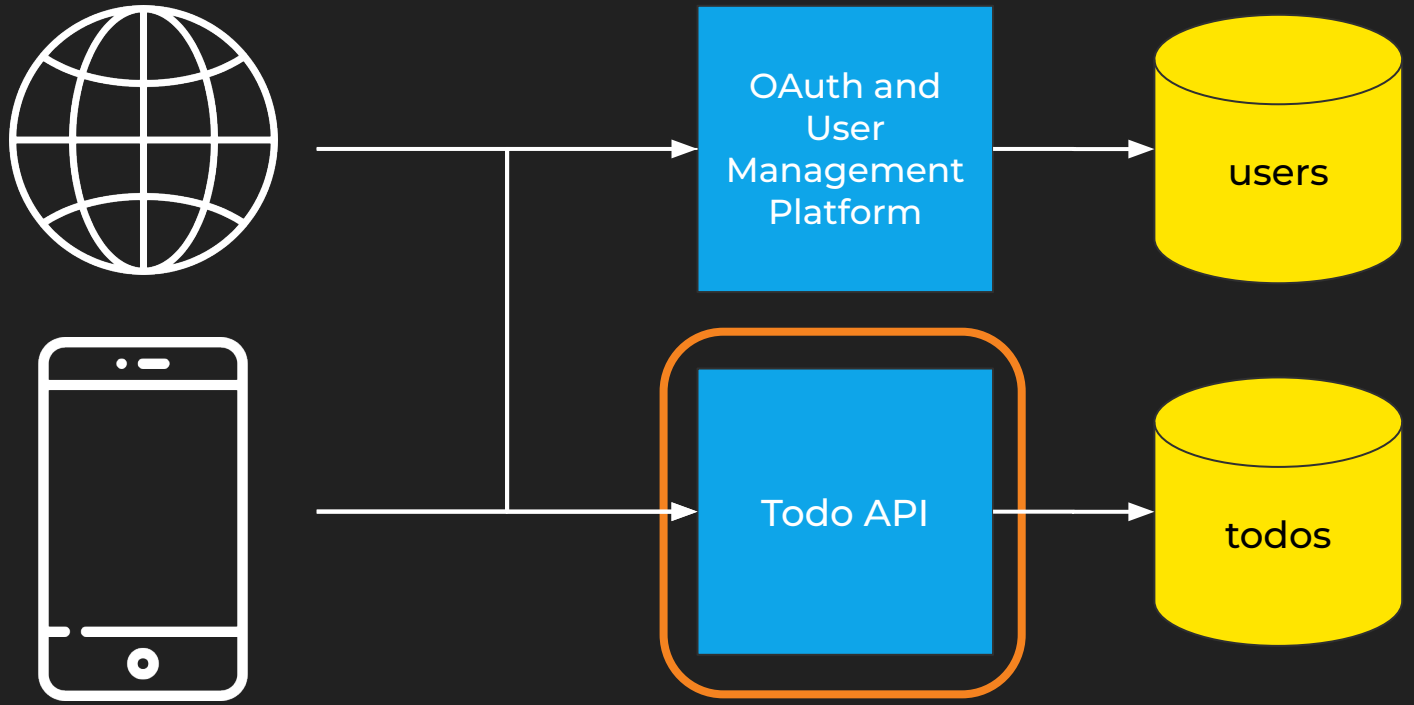
Tokens

Tokens

- **OAuth**
  - Access
  - Refresh
- **OIDC**
  - ID

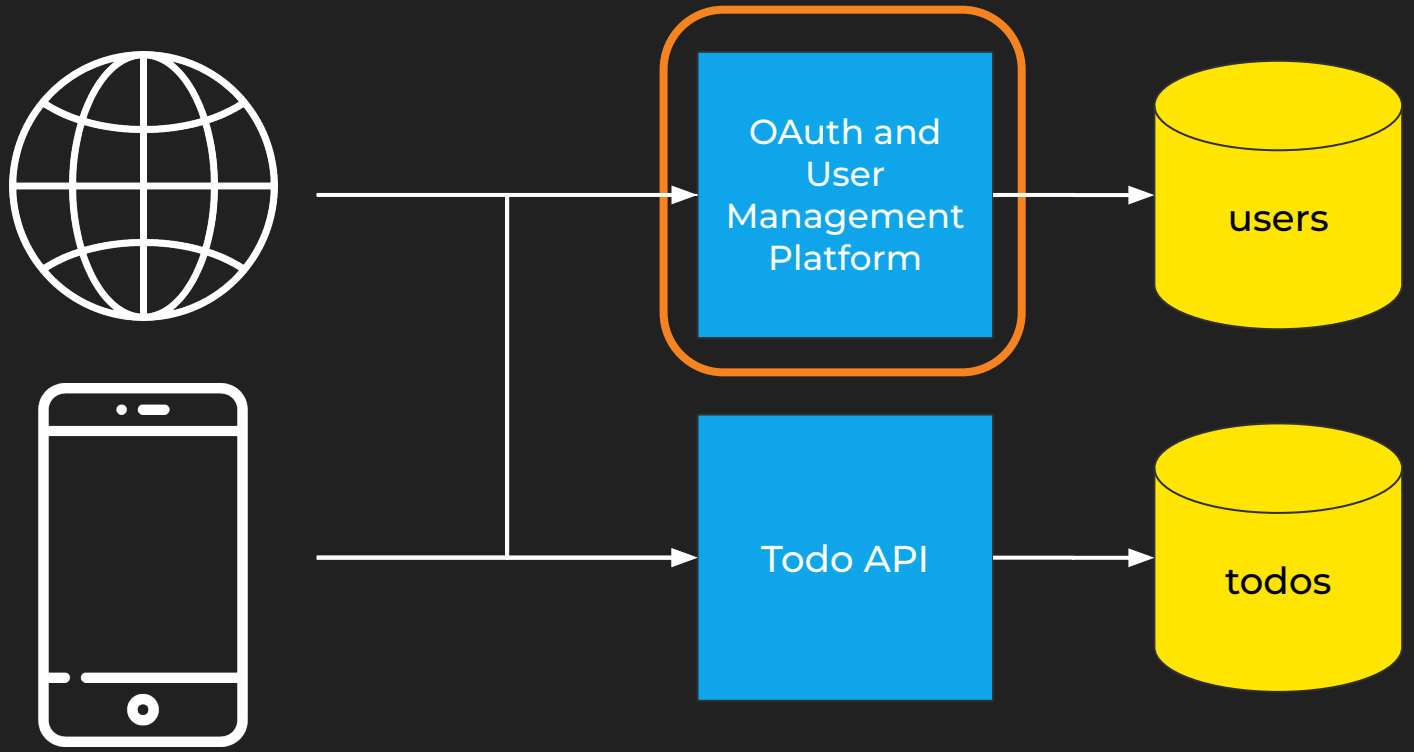
Access Tokens

- Opaque
- JSON Web Tokens (JWTs, “jots”)
- Consumer


OAuth and User Management Platform
users
Todo API
todos

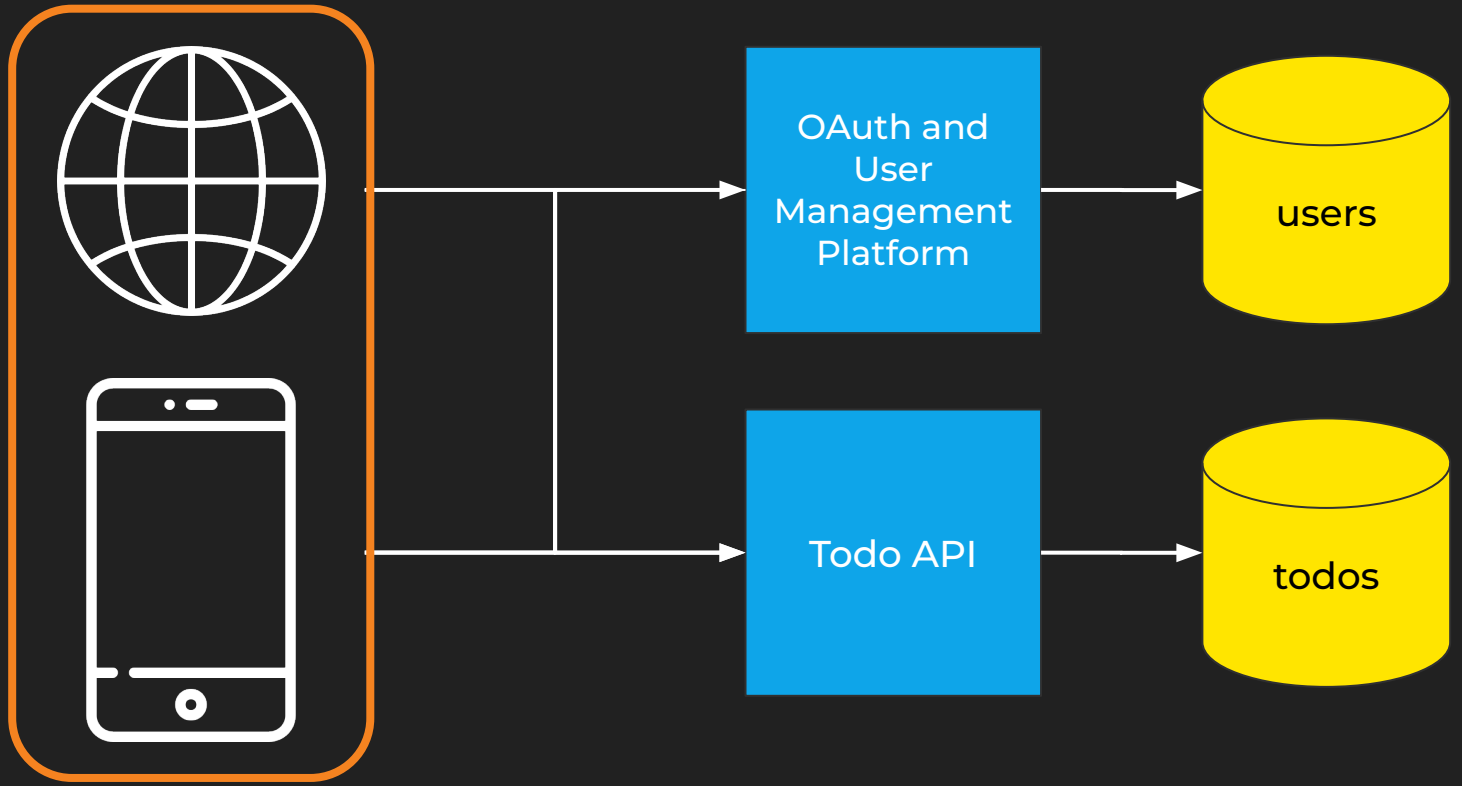
Refresh Tokens

- Opaque
- New access tokens
- OAuth server

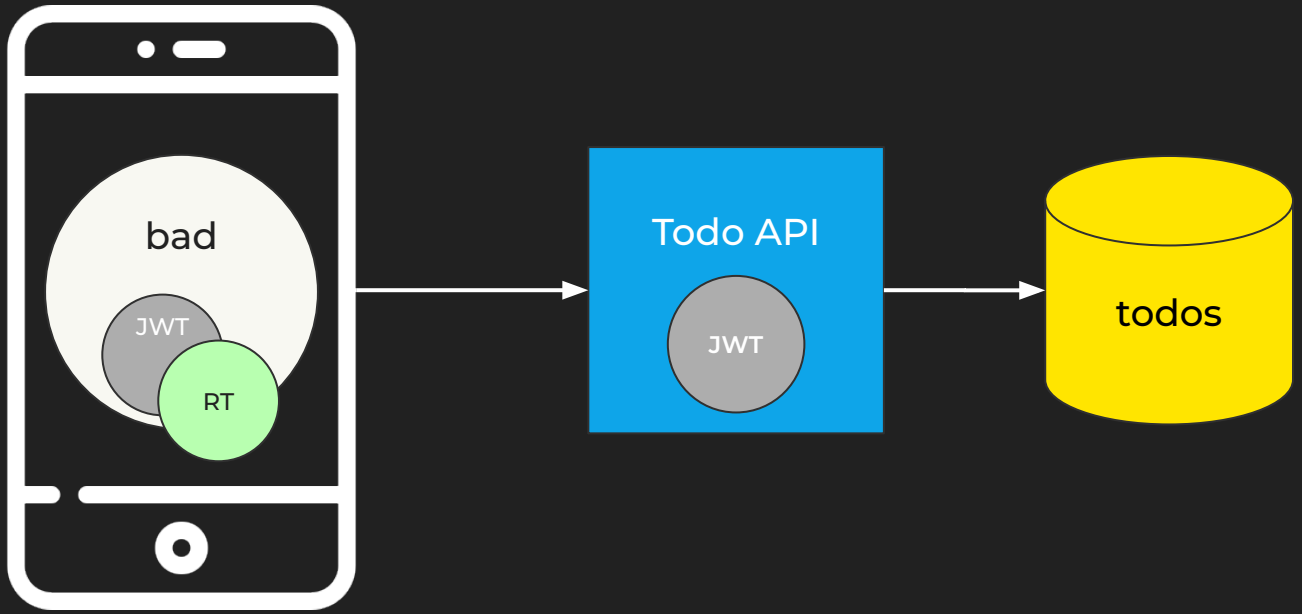

OAuth and User Management Platform
users
Todo API
todos

Id Tokens

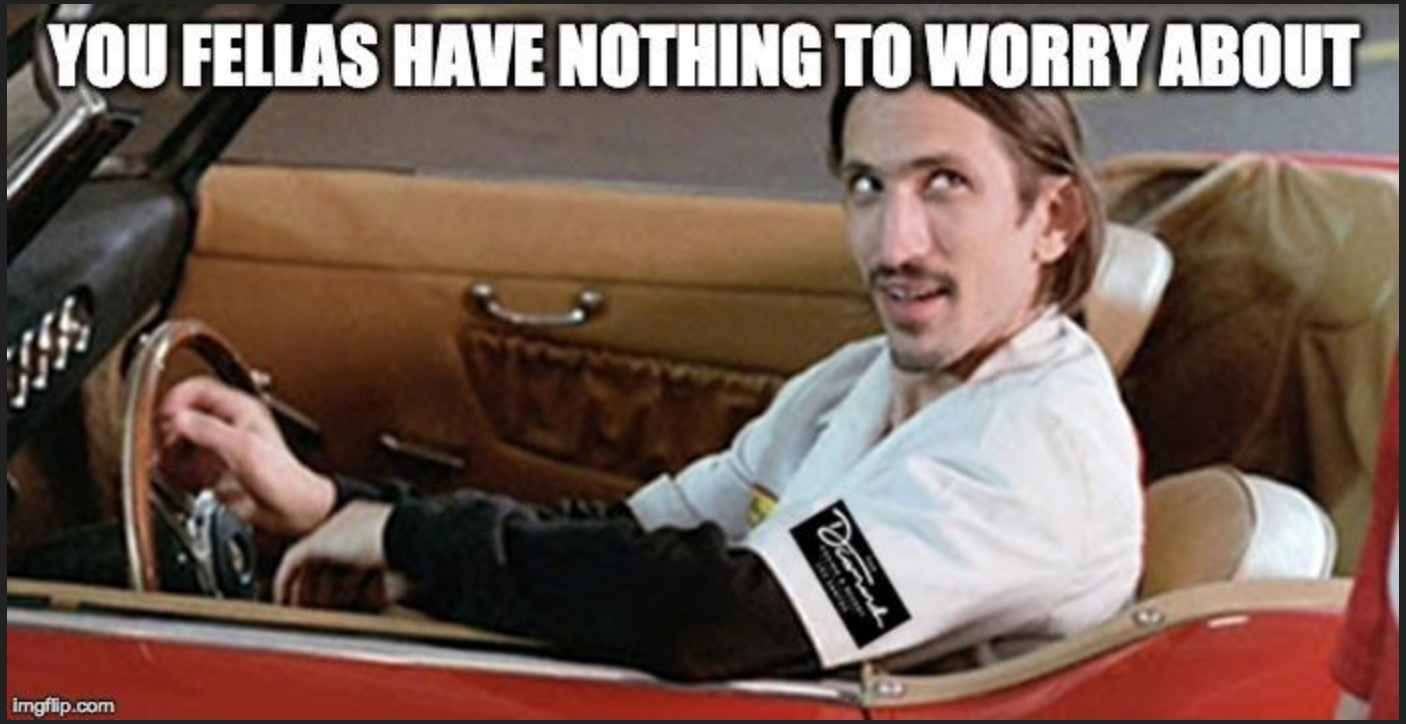
- OIDC
- JWTs
- Not Authorization
- Client


OAuth and User Management Platform
users
Todo API
todos

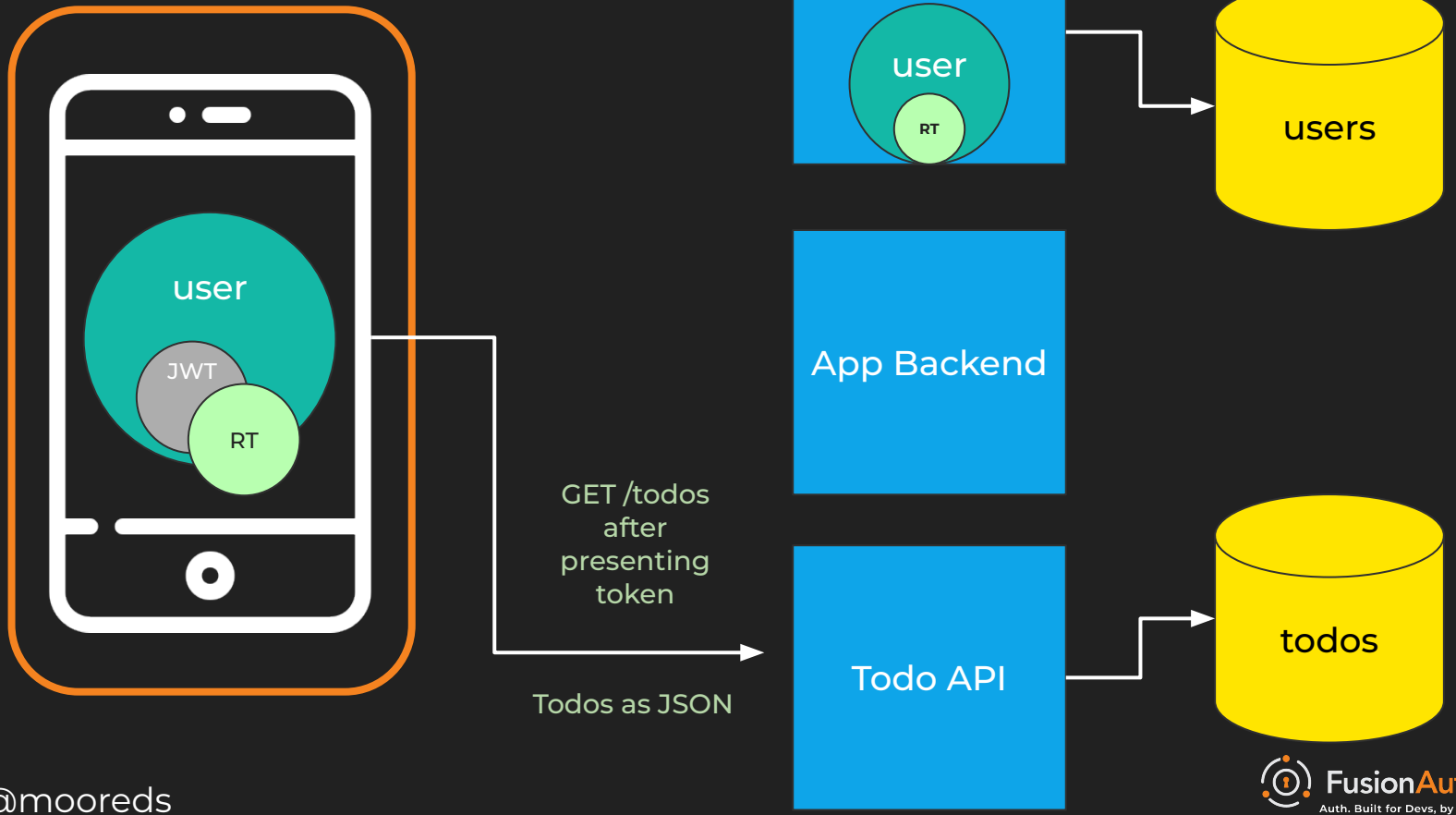
Bearer Tokens


bad
JWT
RT
Todo API
JWT
todos

Protecting Tokens


YOU FELLAS HAVE NOTHING TO WORRY ABOUT
imgflip.com

Client Concerns


OAuth System
user
RT
users
user
JWT
RT
App Backend
GET /todos after presenting token
Todos as JSON
Todo API
todos

Tokens In Transit

- HTTPS

Tokens In Transit

- HTTPS
- No Caches

Tokens In Transit

- HTTPS
- No Caches
  - URLs
  - Query Strings

Token Storage On the Client

- Mobile
- Browsers
- Side-Step Sessions

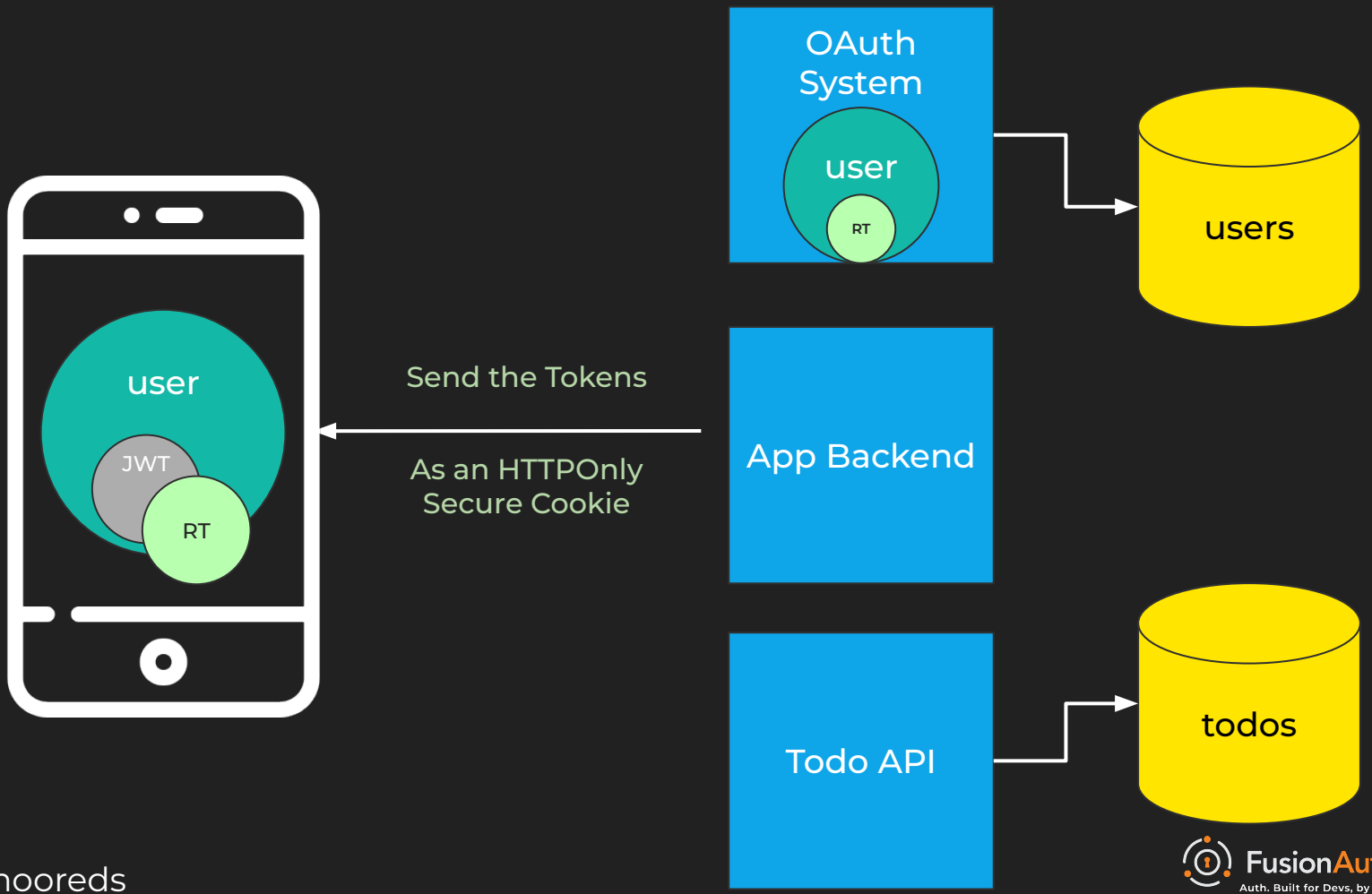
Mobile Application Token Storage

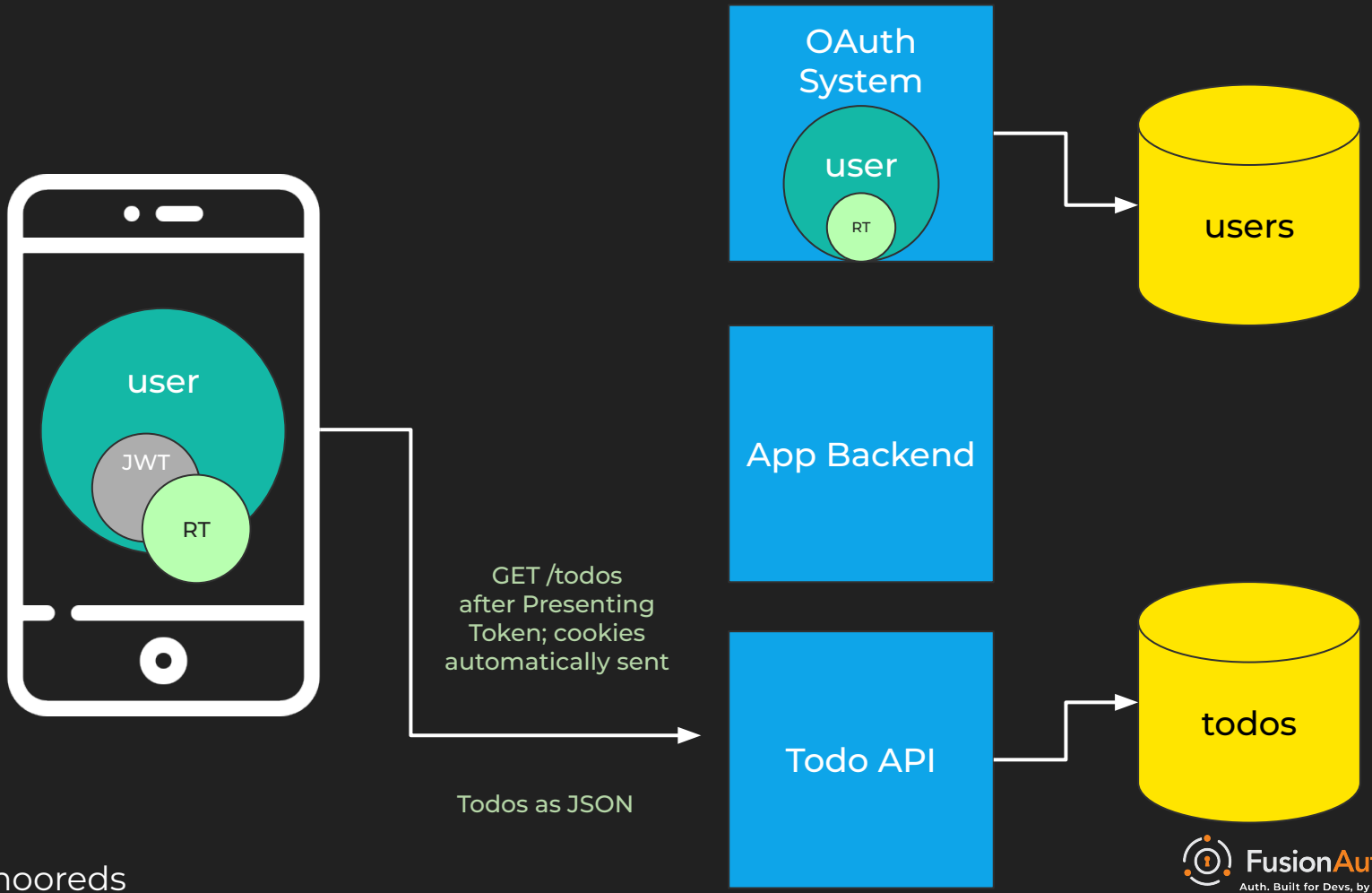
- **iOS**:
  - Encrypted storage
  - Keychain
- **Android**:
  - Encrypted storage
  - App preferences
- Auth libraries

Browser Storage

Browser Storage

- Cookies


OAuth System
user
RT
users
user
JWT
RT
Send the Tokens
As an HTTPOnly Secure Cookie
App Backend
Todo API
todos


OAuth System
user
RT
users
user
JWT
RT
App Backend
GET /todos after Presenting Token; cookies automatically sent
Todo API
todos
Todos as JSON

Browser Storage

- Cookies
- Memory

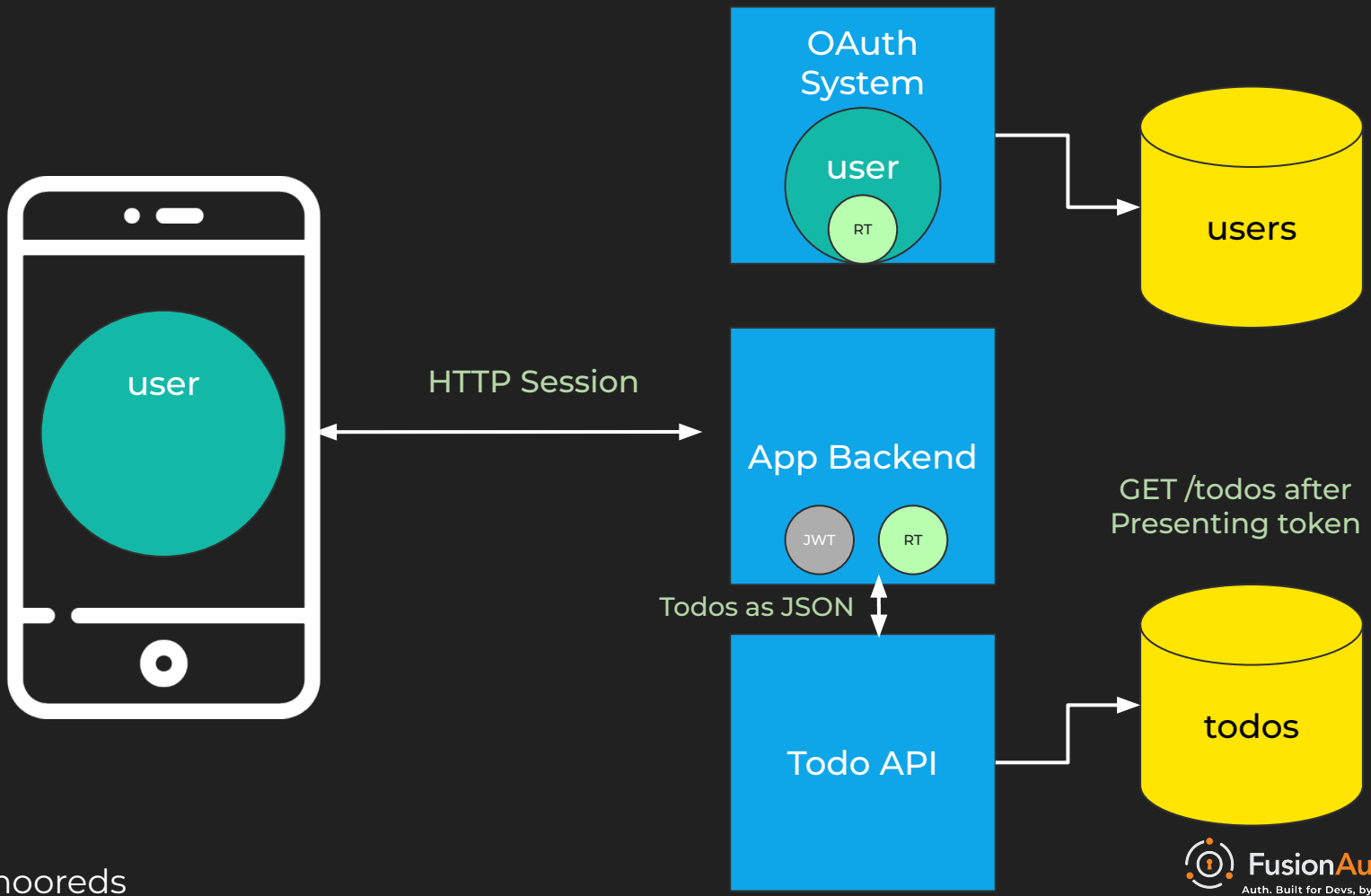
Browser Storage

- Cookies
- Memory
- Web Worker

BFF

BFF

- Back-end For Front-end Pattern


OAuth System
user
RT
users
user
HTTP Session
App Backend
JWT
RT
GET /todos after Presenting token
Todos as JSON
Todo API
todos

Token Lifetimes

Token Lifetimes

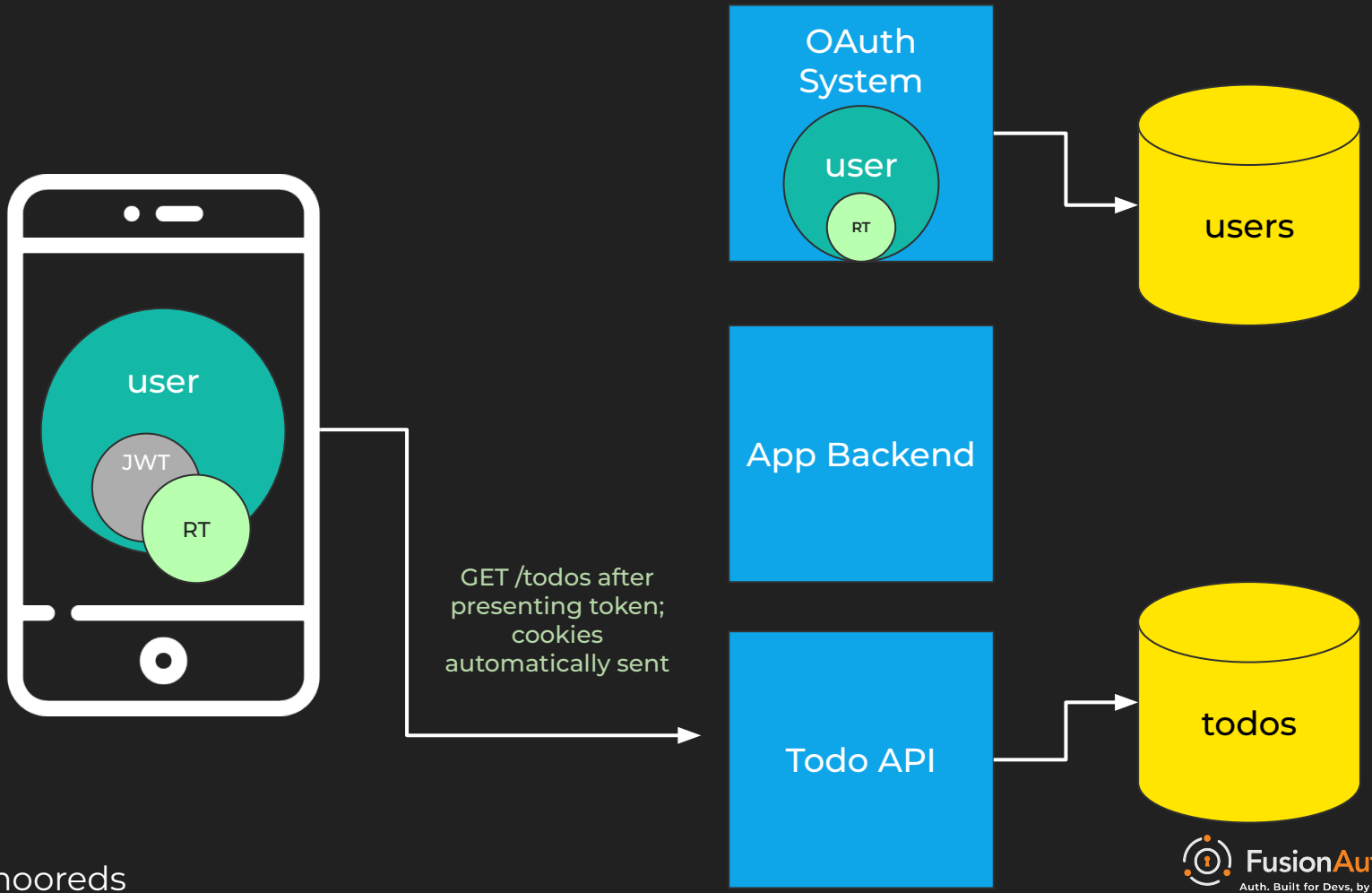
- Access tokens
  - Short Lived
  - Minutes or Seconds
- Refresh tokens
  - Long Lived
  - Days or Months

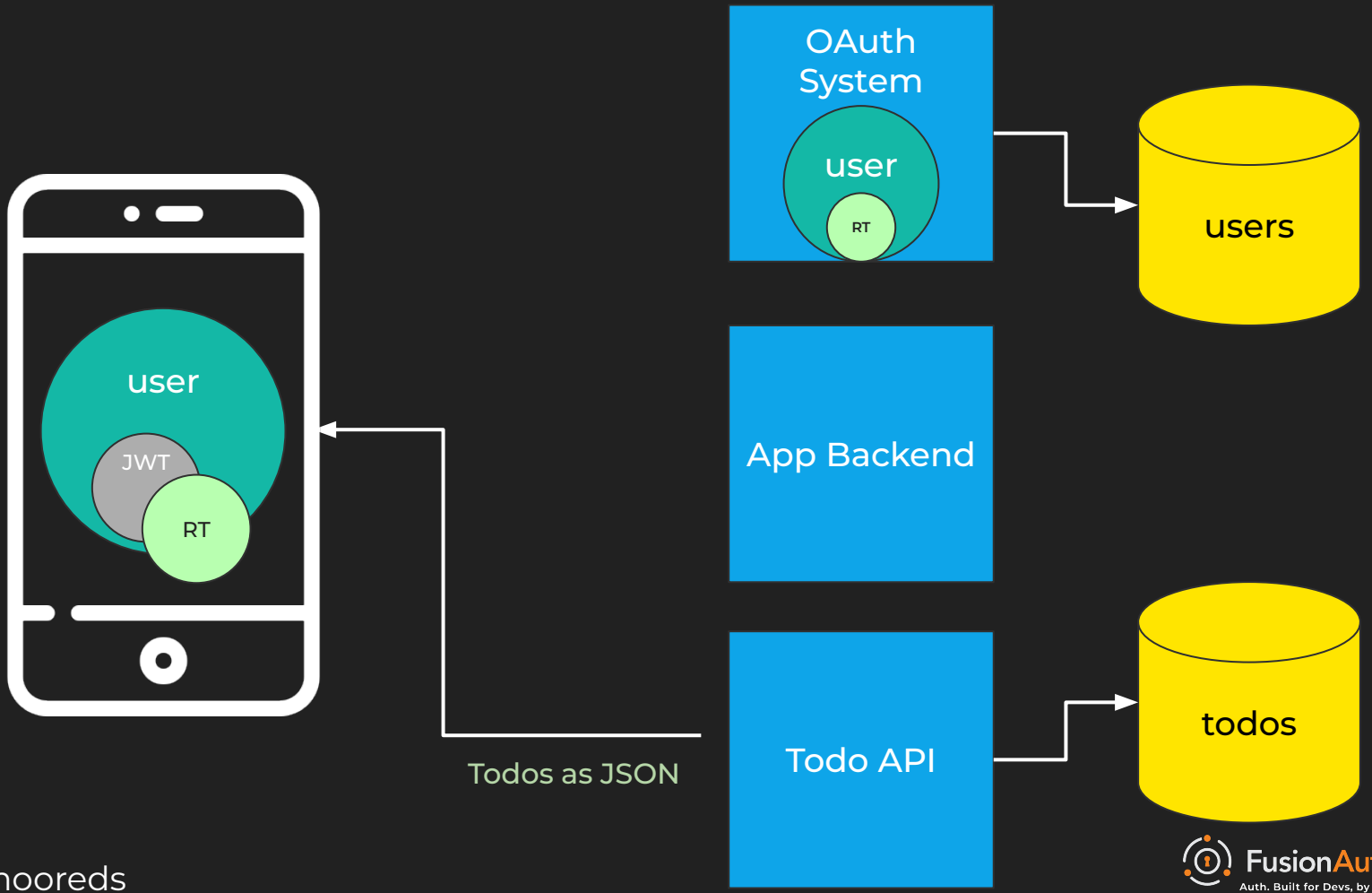
Without Refresh Tokens

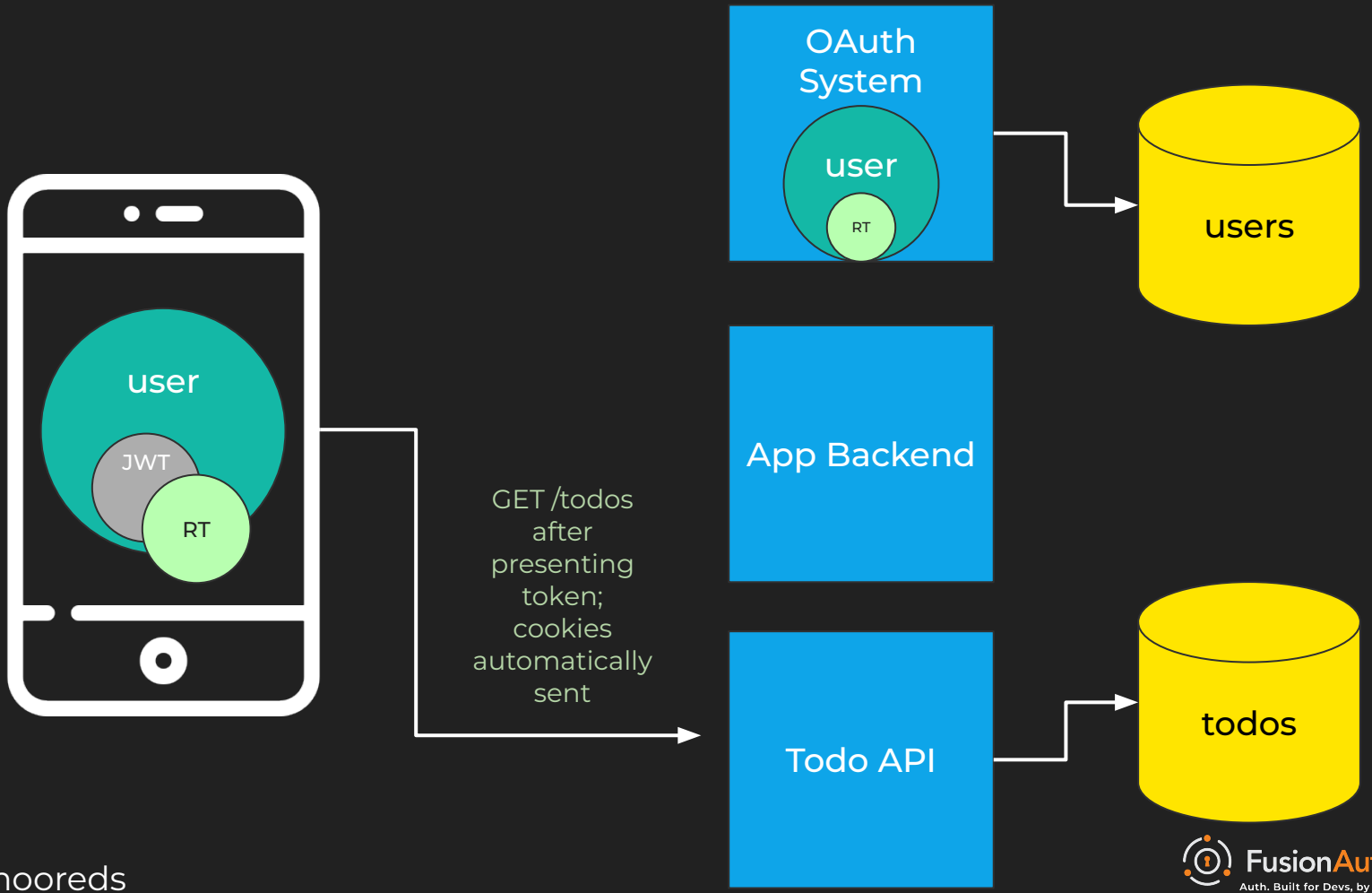
- Unsavory Results
  - Short Lived
    - Repeat Authentication
  - Long Lived
    - Security Risk

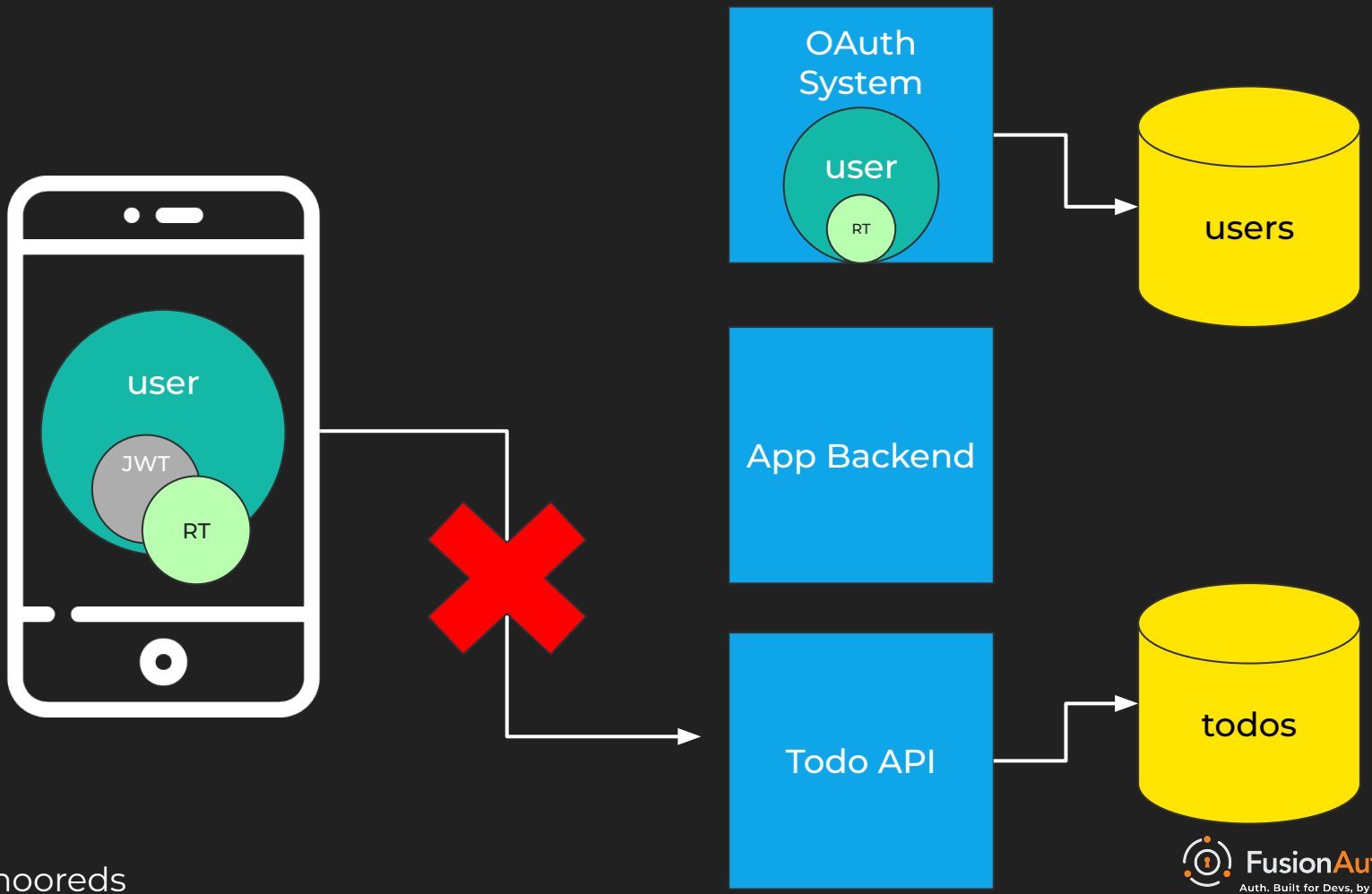

YOU'RE GONNA HAVE A BAD TIME
memegenerator.net

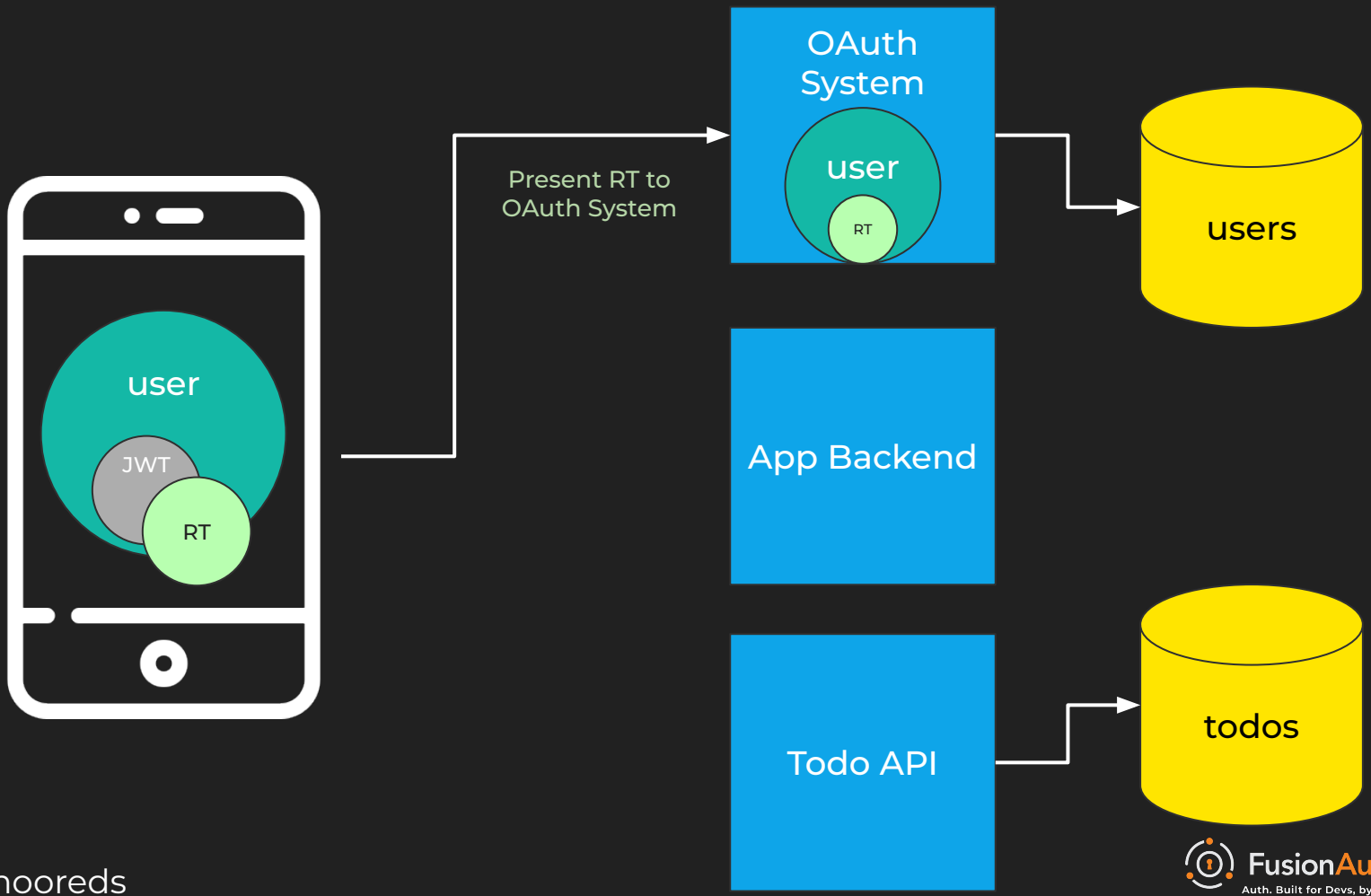
Refreshing Tokens

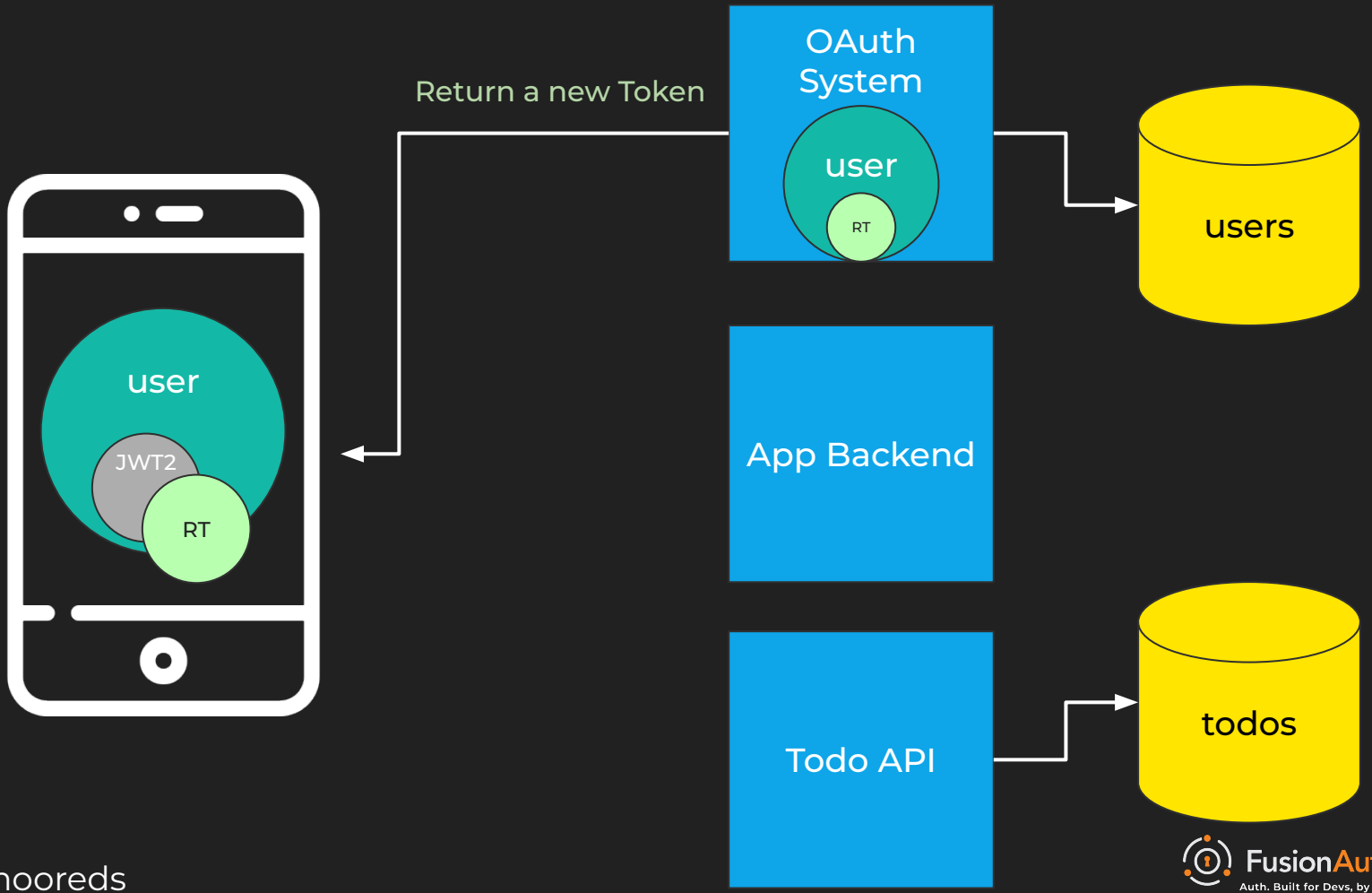

OAuth System
user
RT
users
user
JWT
RT
App Backend
GET /todos after presenting token; cookies automatically sent
Todo API
todos

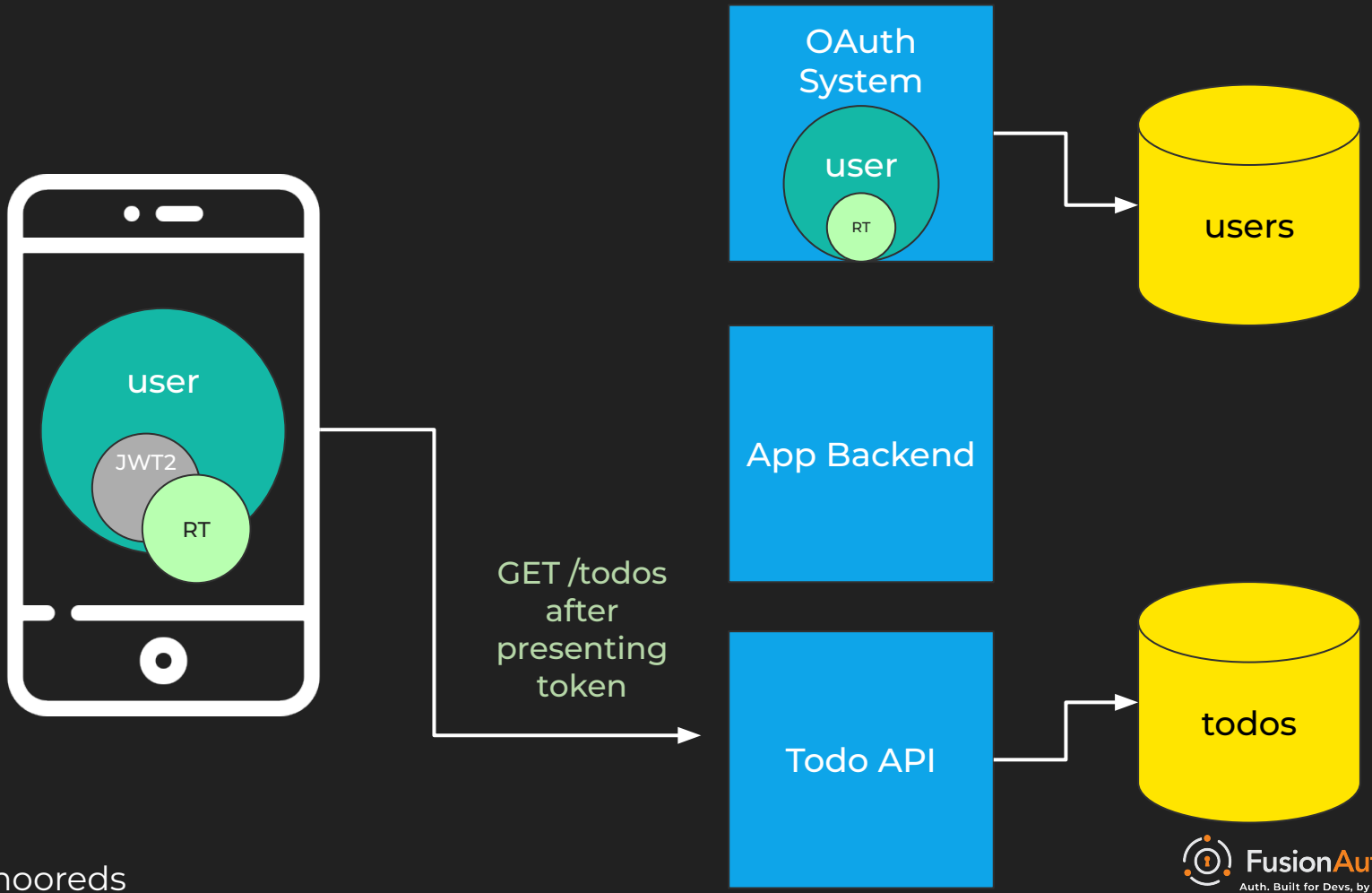

OAuth System
user
RT
users
user
JWT
RT
App Backend
Todos as JSON
Todo API
todos

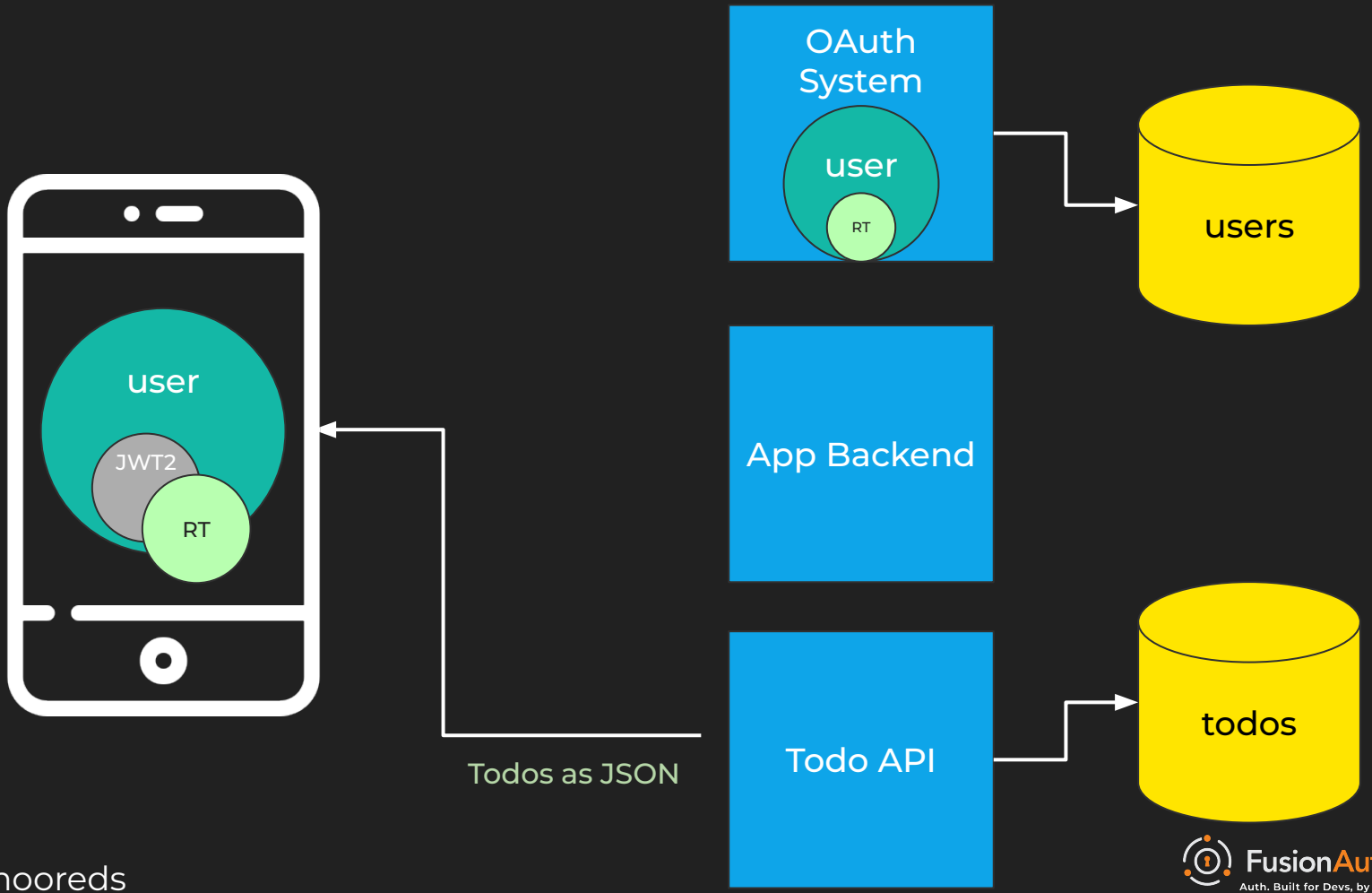

OAuth System
user
RT
users
user
JWT
RT
GET /todos after presenting token; cookies automatically sent
App Backend
Todo API
todos


OAuth System
user
RT
users
user
JWT
RT
App Backend
Todo API
todos


OAuth System
user
RT
users
Present RT to OAuth System
user
JWT
RT
App Backend
Todo API
todos


OAuth System
user
RT
Return a new Token
users
user
JWT2
RT
App Backend
Todo API
todos


OAuth System
user
RT
users
user
JWT2
RT
App Backend
GET /todos after presenting token
Todo API
todos


OAuth System
user
RT
users
user
JWT2
RT
App Backend
Todos as JSON
Todo API
todos

Refresh Token Takeaway

- Client Needs

Refresh Token Takeaway

- Client Needs
  - Store it

Refresh Token Takeaway

- Client Needs
  - Store it
  - Catch Access Denied

Refresh Token Takeaway

- Client Needs
  - Store it
  - Catch Access Denied
  - Present to OAuth Server


OH WHY? THE HORROR!
THE HORROR!!

Refresh Token Takeaway

- Client Needs
  - Store it
  - Catch Access Denied
  - Present to OAuth Server
  - Store new Access Token

Refresh Token Takeaway

- Client Needs
  - Store it
  - Catch Access Denied
  - Present to OAuth Server
  - Store new Access Token
- Zero Consumer Effort

Consumer Concerns

What Is A Consumer

- Resource Server / RS

What Is A Consumer

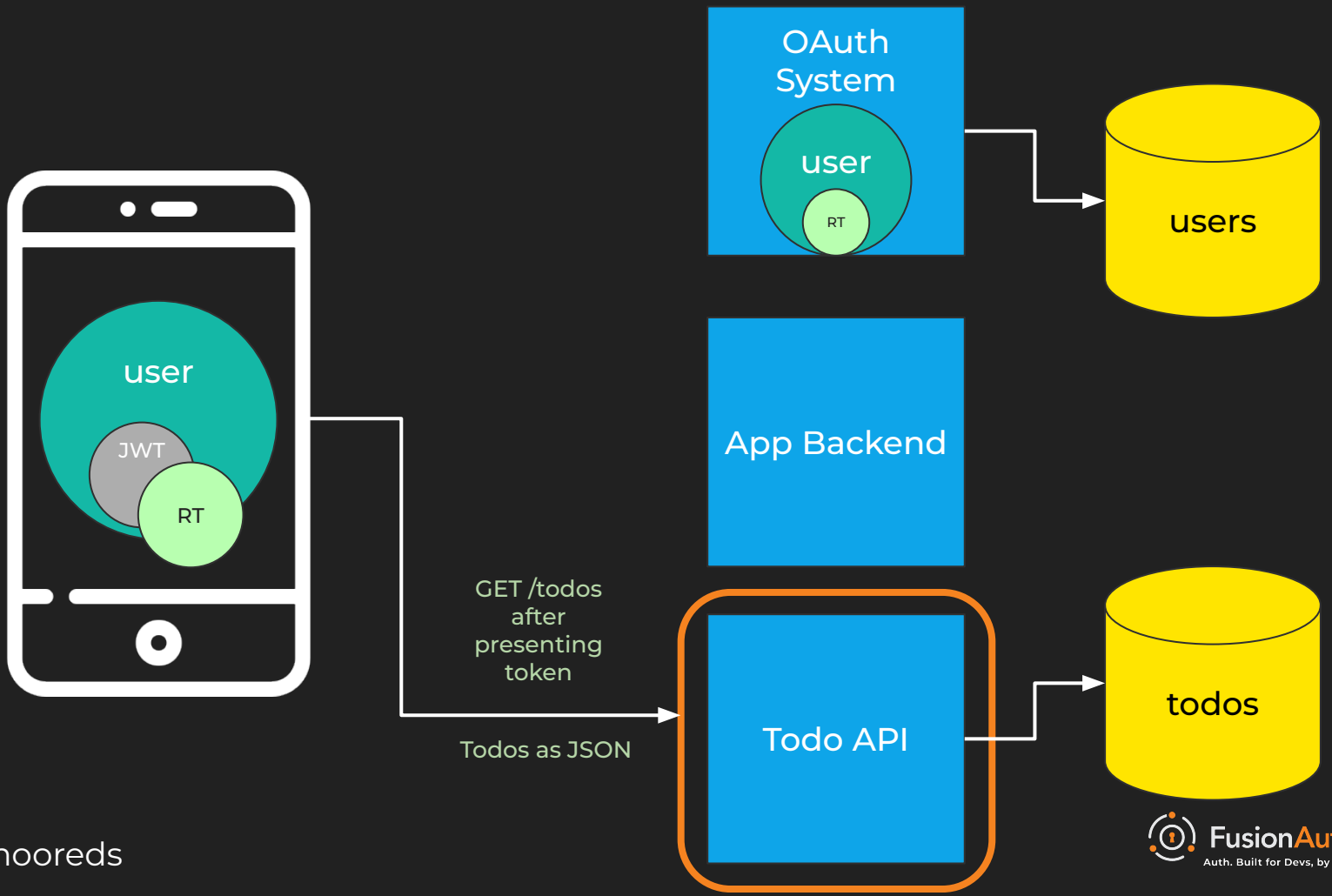
- Resource Server / RS
  - Accept Access Token

What Is A Consumer

- Resource Server / RS
  - Accept Access Token
  - Validate Access Token

What Is A Consumer

- Resource Server / RS
  - Accept Access Token
  - Validate Access Token
  - Return Data


OAuth System
user
RT
users
user
JWT
RT
App Backend
GET /todos after presenting token
Todos as JSON
Todo API
todos

Validating Tokens

Validating Tokens

- Examine

Validating Tokens

- Examine
- Introspect

Examining Tokens

- Internal Structure
  - JWT
  - PASETO

Examining Tokens

- Internal Structure
  - JWT
  - PASETO
- Validate Signature

Examining Tokens

- Internal Structure
  - JWT
  - PASETO
- Validate Signature
- Validate Claims

JWT

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJmdXNpb25hdX
RoLmlvIiwiZXhwIjoxNjE5NTU1MDE4LCJhdWQiOiIyMzhkNDc5My03MGR
lLTQxODMtOTcwNy00OGVkOGVjZDE5ZDkiLCJzdWIiOiIxOTAxNmI3My0z
ZmZhLTRiMjYtODBkOC1hYTkyODc3Mzg2NzciLCJuYW1lIjoiRGFuIE1vb
3JlIiwibWVtYmVyc2hpcEV4cGlyZWQiOmZhbHNlLCJyb2xlcyI6WyJSRV
RSSUVWRV9UT0RPUyIsIkFETUlOIl19.cPL36Al_8eT7YQVowIOruitxXb
0n8w4DKaWVthfEwfc

JWT Header

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9
```

=

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

JWT Body

eyJpc3MiOiJmdXNpb25hdXRoLmlvIiwiZXhwIjoxNjE5NTU1MDE4LCJhdWQiOiIyMzhkNDc5My03MGRlLTQxODMtOTcwNy00OGVkOGVjZDE5ZDkiLCJzdWIiOiIxOTAxNmI3My0zZmZhLTRiMjYtODBkOC1hYTkyODc3Mzg2NzciLCJuYW1lIjoiRGFuIE1vb3JlIiwibWVtYmVyc2hpcEV4cGlyZWQiOmZhbHNlLCJyb2xlcyI6WyJSRVRSSUVWRV9UT0RPUyIsIkFETUlOIl19

=

```
{
  "iss": "fusionauth.io",
  "exp": 1619555018,
  "aud": "238d4793-70de-4183-9707-48ed8ecd19d9",
  "sub": "19016b73-3ffa-4b26-80d8-aa9287738677",
  "name": "Dan Moore",
  "roles": ["RETRIEVE_TODOS", "ADMIN"]
}
```

JWT Signing


```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9

eyJpc3MiOiJmdXNpb25hdXRoLmlvIiwiZXhwIjoxNjE5NTU1MDE4LCJhdWQiO
iIyMzhkNDc5My03MGRlLTQxODMtOTcwNy00OGVkOGVjZDE5ZDkiLCJzdWIiOi
IxOTAxNmI3My0zZmZhLTRiMjYtODBkOC1hYTkyODc3Mzg2NzciLCJuYW1lIjo
iRGFuIE1vb3JlIiwibWVtYmVyc2hpcEV4cGlyZWQiOmZhbHNlLCJyb2xlcyI6
WyJSRVRSSUVWRV9UT0RPUyIsIkFETUlOIl19
```

JWT Signature

`cPL36Al_8eT7YQVowIOruitxXb0n8w4DKaWVthfEwfc`

=

Signature

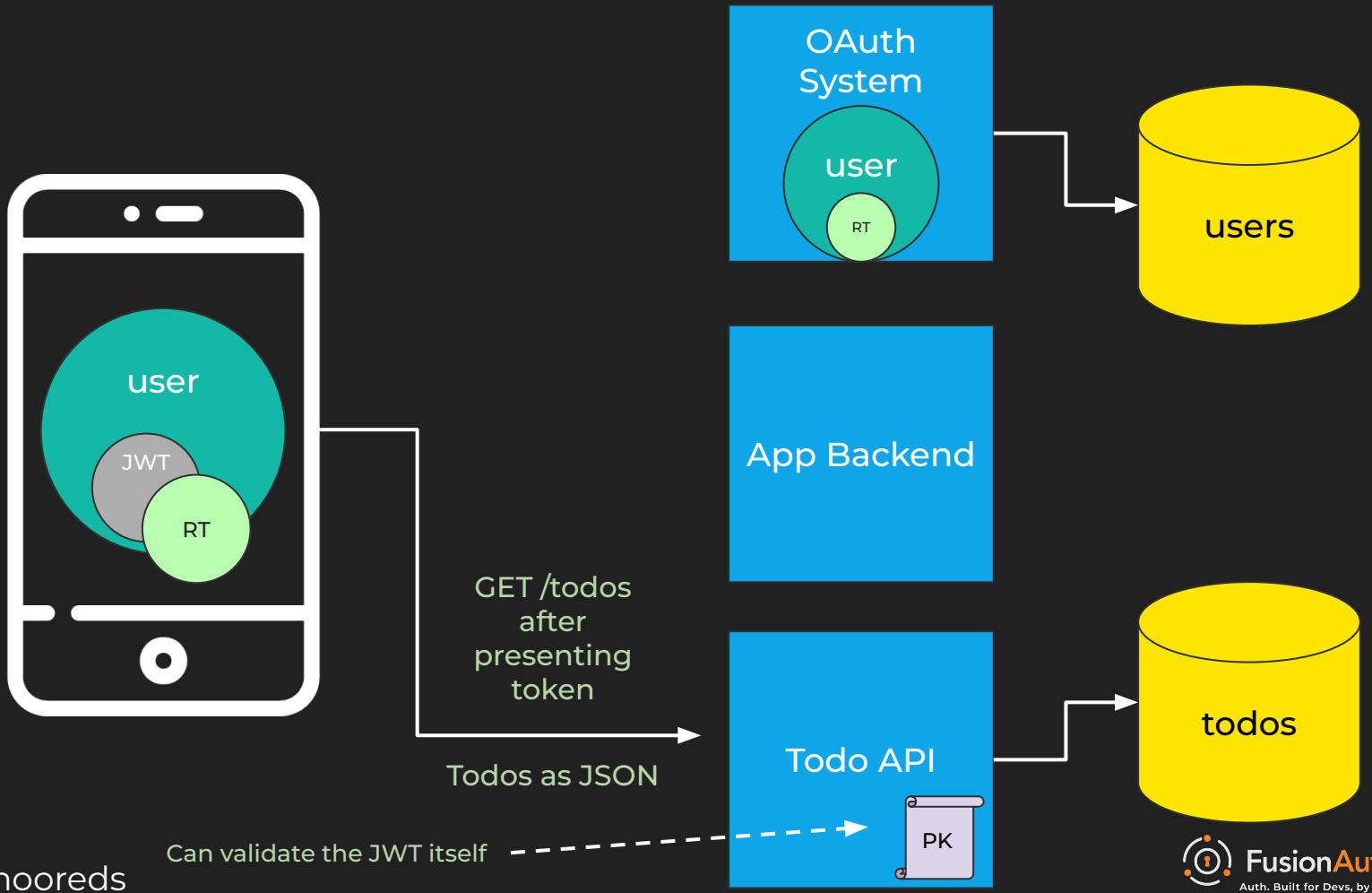
JWT Body

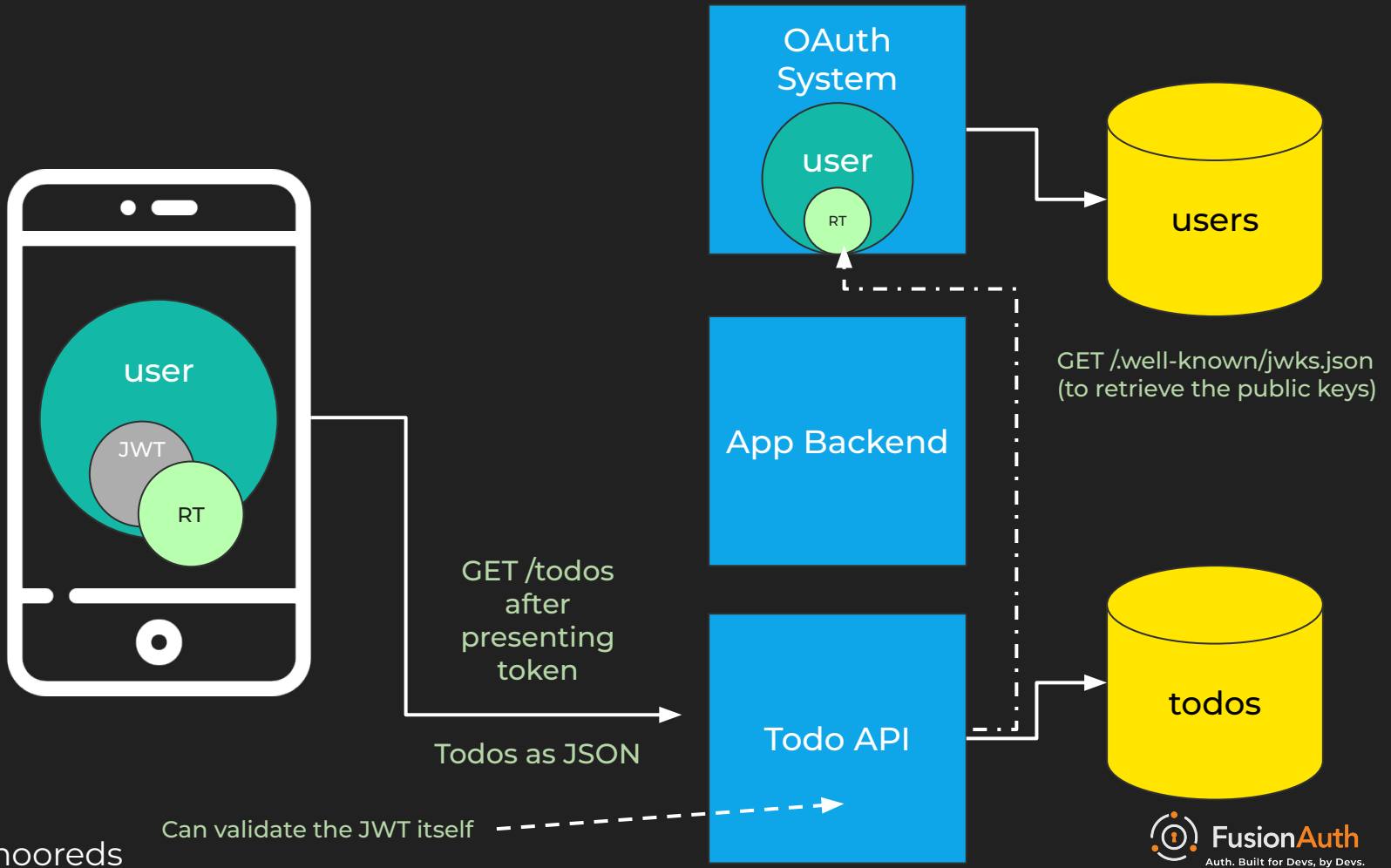
```
{
  "iss": "fusionauth.io",
  "exp": 1619555018,
  "aud": "238d4793-70de-4183-9707-48ed8ecd19d9",
  "sub": "19016b73-3ffa-4b26-80d8-aa9287738677",
  "name": "Dan Moore",
  "roles": ["RETRIEVE_TODOS", "ADMIN"]
}
```

JWT Body

```
{
  "iss": "fusionauth.io",
  "exp": 1619555018,
  "aud": "238d4793-70de-4183-9707-48ed8ecd19d9",
  "sub": "19016b73-3ffa-4b26-80d8-aa9287738677",
  "name": "Dan Moore",
  "roles": ["RETRIEVE_TODOS", "SUPER_ADMIN"]
}
```

Validating the Signature


OAuth System
user
RT
users
user
JWT
RT
App Backend
GET /todos after presenting token
Todos as JSON
Todo API
todos
PK
Can validate the JWT itself


OAuth System
user
RT
users
GET /.well-known/jwks.json
(to retrieve the public keys)
user
JWT
RT
App Backend
GET /todos
after
presenting
token
Todos as JSON
Todo API
todos
Can validate the JWT itself

```
{
  "keys" : [
    {
      "alg" : "RS256",
      "e" : "AQAB",
      "kid" : "uk0PWf8KkTKiJqWwrNjn16QoKKI",
      "kty" : "RSA",
      "n" :
"2xzTUGNSpIeNcvICSlFlhver42dR9CWYePEoLk6ncuk1nKLzwOr-hy3W2rmkG-x_DaVMVBT5jimClL_k7Fu5xlscexpmNTo3l
K_fqWv_qhnOONSaX0ETqWSrS9MXWnJcPTZkA37ZAwhGKaz8zzSF3Jh_fULWnFHgJxCLBNYmopnvVAv_erJR0wjX9imMpMsBh3w
8O6RyN8ghhlkJ0q4JKyaauF-xk8nLwIAvdWiPWNpzJ57oXfHUXesbLCfLIuM3f_suh_RaZn7uC0jEO1uG23htOqMb1M0TW5uk8
pAxdhVKYbKsPR8CMOUc1je8wDo2w4y4gY_1koST3xnA6IRhBQ",
      "use" : "sig",
      "x5c" : [
"MIICuDCCAaCgAwIBAQIQMcWR+VPwTieC06b3Fn6XbzANBgkqhkiG9w0BAQsFADAYMRYwFAYDVQQDEw1mdXNpb25hdXRoLmlvM
B4XDTIxMDUyNDE5NDU1OVoXDTMxMDUyNDE5NDU1OVowGDEWMBQGA1UEAxMNZnVzaW9uYXV0aC5pbzCCASIwDQYJKoZIhvcNAQE
BBQADggEPADCCAQoCggEBANsc01BjUqSHjXLyAkpRZYb3q+NnUfQlmHjxKC5Op3LpNZyi88Dq/oct1tq5pBvsfw2lTFQU+Y4pg
pS/5OxbucZbHHsaZjU6N5Sv36lr/6oZzjjUml9BE6lkq0vTF1pyXD02ZAN+2QMIRims/M80hdyYf31C1pxR4CcQiwTWJqKZ71Q
L/3qyUdMI1/YpjKTLAYd8PDukcjfIIYZZCdKuCSsmmrhfsZPJy8CAL3Voj1jacyee6F3x1F3rGywnyyLjN3/7Lof0WmZ+7gtIx
Dtbhtt4bTqjG9TNE1ubpPKQMXYVSmGyrD0fAjDlHNY3vMA6NsOMuIGP9ZKEk98ZwOiEYQUCAwEAATANBgkqhkiG9w0BAQsFAAO
CAQEAcj/NIIltfhyP9zsleVn7N/QRavfKA1SBTwtlPMVezuRIX+S3jzxJb/ot47TBD5WFNY5y5AOkWHQFNkVtuPjUYmKTAqJd0
+kVur77tLKzour6wjOp2QgKzG3IGxQnK903JkFlyWF4vSJuOpH8WymJ1jq1gD5zJjz2NXqch+gBIp5Kscr2tj2hg2BGmq5v7+5
pz2jYHosarj4sJwGsLqk1j479wK1iaMjdBVCMuq/QS9yF0sG0STsjbceyGzFWbknmZdfNup6C4a0m8paeb9mlgFfIx9qljuNIn
pc9QZWeRymNJ5spX0WYVRLu7ULrLDXr8xUupjCSMV95yI1XF6tMkw=="
      ],
      "x5t" : "uk0PWf8KkTKiJqWwrNjn16QoKKI",
      "x5t#S256" : "UW-4zdFS6YR9g4Vhl3T3xLwfQ_S1aLFh2x4VBvK1sbY"
    }
  ]
}
```

```
{
      "alg" : "RS256",
      "kid" : "uk0PWf8KkTKiJqWwrNjn16QoKKI",
      "x5c" : [
"MIICuDCCAaCgAwIBAQIQMcWR+VPwTieC06b3Fn6XbzA
NBgkqhkiG9w0BAQsFADAYMRYwFAYDVQQDEw1mdXNpb25
hdX..."
      ]
      // ...
  }
```

JWT Header

```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "uk0PWf8KkTKiJqWwrNjn16QoKKI"
}
```

Invalid Signature


GO TO
JAIL

Validating Claims

Validating Claims

```
{
  "iss": "fusionauth.io",
  "exp": 1619555018,
  "aud":
"238d4793-70de-4183-9707-48ed8ecd19d9",
  "sub":
"19016b73-3ffa-4b26-80d8-aa9287738677",
  "name": "Dan Moore",
  "roles": ["RETRIEVE_TODOS", "ADMIN"]
}
```

Validating Claims

```
{
  "iss": "fusionauth.io",
  "exp": 1619555018,
  "aud":
"238d4793-70de-4183-9707-48ed8ecd19d9",
  "sub":
"19016b73-3ffa-4b26-80d8-aa9287738677",
  "name": "Dan Moore",
  "roles": ["RETRIEVE_TODOS", "ADMIN"]
}
```

Validating Claims

```
{
  "iss": "fusionauth.io",
  "exp": 1619555018,
  "aud":
"238d4793-70de-4183-9707-48ed8ecd19d9",
  "sub":
"19016b73-3ffa-4b26-80d8-aa9287738677",
  "name": "Dan Moore",
  "roles": ["RETRIEVE_TODOS", "ADMIN"]
}
```

Validating Claims

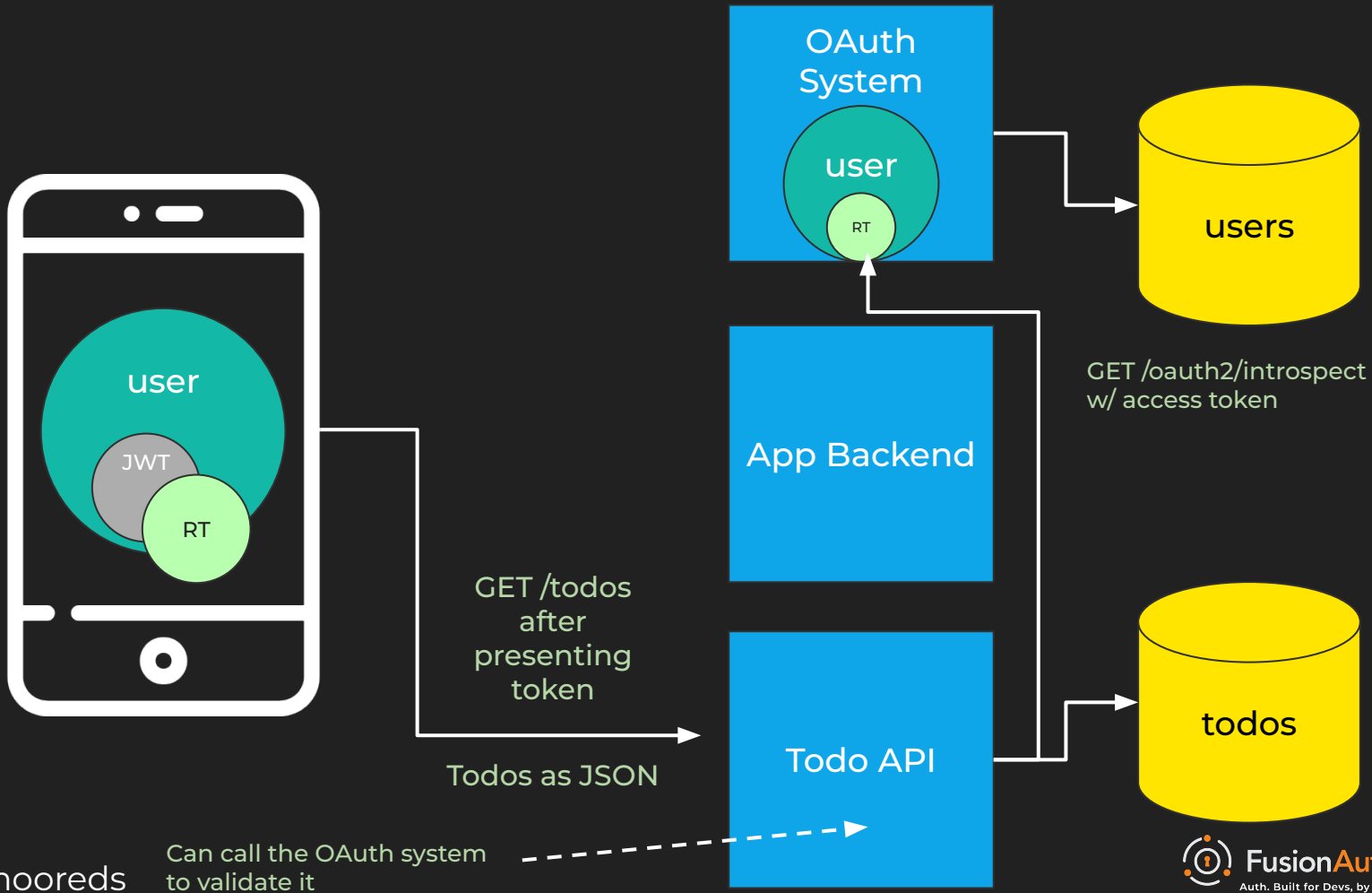
```
{
  "iss": "fusionauth.io",
  "exp": 1619555018,
  "aud":
"238d4793-70de-4183-9707-48ed8ecd19d9",
  "sub":
"19016b73-3ffa-4b26-80d8-aa9287738677",
  "name": "Dan Moore",
  "roles": ["RETRIEVE_TODOS", "ADMIN"]
}
```

Validating Claims

```
{
  "iss": "fusionauth.io",
  "exp": 1619555018,
  "aud":
"238d4793-70de-4183-9707-48ed8ecd19d9",
  "sub":
"19016b73-3ffa-4b26-80d8-aa9287738677",
  "name": "Dan Moore",
  "roles": ["RETRIEVE_TODOS", "ADMIN"]
}
```

Validating Claims
Is Business Logic

Introspect


OAuth System
user
RT
users
GET /oauth2/introspect w/ access token
user
JWT
RT
App Backend
GET /todos after presenting token
Todos as JSON
Todo API
todos
Can call the OAuth system to validate it

Introspect Results


```
{
  "iss": "fusionauth.io",
  "exp": 1619555018,
  "aud":
"238d4793-70de-4183-9707-48ed8ecd19d9",
  "sub":
"19016b73-3ffa-4b26-80d8-aa9287738677",
  "name": "Dan Moore",
  "roles": ["RETRIEVE_TODOS", "ADMIN"],
  "active": true
}
```

Processing Introspect Claims

- RFC 7662

Processing Introspect Claims

- RFC 7662
- OAuth Server Docs

Introspect Results

```
{
  "iss": "fusionauth.io",
  "exp": 1619555018,
  "aud":
"238d4793-70de-4183-9707-48ed8ecd19d9",
  "sub":
"19016b73-3ffa-4b26-80d8-aa9287738677",
  "name": "Dan Moore",
  "roles": ["RETRIEVE_TODOS", "ADMIN"],
  "active": true
}
```

Validating Claims
Is Business Logic

Common Issues

JWT Footguns

- Options
  - Tons
  - Use Library

JWT Footguns

- Options
  - Tons
  - Use Library
- Arbitrary JSON
  - Custom Claims
  - No Secrets
  - Contents Encoded


WHAT DO YOU NOT UNDERSTAND
THERE ARE NO SECRETS,
ONLY DELAYED REVELATIONS
imgflip.com

JWT Footguns

- Options
  - Tons
  - Use Library
- Arbitrary JSON
  - Custom Claims
  - No Secrets
  - Contents Encoded
- “none” algorithm
  - Unsigned

Unsanitized Credentials

Simple Fix = Never “none”


NOPE
NEVER
memegenerator.net

Alternatives

API Keys

- Static
- Not Time Bound
- No Structure

Sessions

- No Refresh
- Low Scalability

Conclusion

Conclusion

- Tokens
- Client
  - Transmit
  - Store
  - Refresh
- Consumer
  - Validate
    - Signature
      - Examine
      - Introspect
    - Claims

Thanks & Questions

Contact

dan@fusionauth.io

Website

fusionauth.io

Website

@mooreds