Two ways to validate a token

- Keys are fetched dynamically from the JWKS endpoint

- Local (/keys endpoint)

- Remote (/introspect endpoint)

- Up-to-date info

- the token is sent to the authorization server for validation

- App performs the validation itself

HTTPBearer scheme

```python
async def verify_token(credentials: HTTPAuthorizationCredentials = Depends(bearer_scheme)) -> User:
    """Verifies the incoming access token using FastAPI's HTTPBearer."""
    token = credentials.credentials  # Extract the token from the Authorization header
    # print(f"Extracted token: {token}")
```