



Laurea Magistrale in Sicurezza Informatica - Università di Salerno
Corso di *Sicurezza dei Dati* – Prof. C. Esposito, A. De Santis



KRYPTOAUTH

Manuale delle Istruzioni KryptoAuth

Riferimento	
Versione	1.0
Data	12/02/2023
Destinatario	Prof. C. Esposito Prof. A. De Santis
Presentato da	Montefusco Alberto



Sommario

Sommario	2
1. Introduzione	3
1.1 Scopo del Sistema	3
1.2 Scopo del Documento	3
2. Requisiti per l'installazione	3
2.1 Deploy Smart Contract su Ganache	4
2.2 Conversione Smart Contract in classe Java	7
2.3 Configurazione rete Metamask - Ganache	8
2.4 Avvio Web DApp	11
2.5 Esempio generazione NFT in Pinata	11



1. Introduzione

1.1 Scopo del Sistema

La realizzazione di KryptoAuth ha l'obiettivo di offrire maggiore sicurezza durante l'operazione di autenticazione sfruttando la tecnologia Blockchain Ethereum.

1.2 Scopo del Documento

Lo scopo di questo documento è di aiutare l'utente nell'installazione del sistema e, qualora mancanti, di tutte le componenti necessarie al suo funzionamento. In particolare, sarà mostrata la procedura di deploy dello Smart Contract sulla Blockchain di test Ganache, la creazione e la configurazione della rete per l'interfacciamento tra Metamask e Ganache, la traduzione dello Smart Contract scritto in Solidity in una classe Java mediante l'uso di solc.js e Web3j e, infine, un esempio di creazione di un NFT con Pinata.

2. Requisiti per l'installazione

Requisiti lato client:

- web Browser;
- estensione Metamask;
- connessione ad Internet.

Requisiti lato server, necessari per l'uso di KryptoAuth:

- **Ganache**, requisito base per il funzionamento del sistema (**LINK:** [Ganache](#));
- **Web3j**, con il quale si potrà convertire lo Smart Contract in linguaggio Java ed interfacciare la Web DApp con Ganache (**LINK:** [Web3j](#));
- Pacchetti npm (usare la versione di node v16.17.0):
 - `npm install -g solc`
 - `npm install -g truffle`
 - `npm install -g @openzeppelin/contracts`
 - `npm install -g browserify`

- inserire manualmente nella cartella globale `node_modules`
`@BokkyPooBahsDateTimeLibrary/contracts` scaricabile da [GitHub](https://github.com/BokkyPooBahsDateTimeLibrary/contracts)

Se in `KryptoAuth/src/main/resources/static/js/pinata_IPFS` non è presente la cartella **`node_modules`**, allora installare `npm install @pinata/sdk`.

2.1 Deploy Smart Contract su Ganache

Per effettuare il deploy dello Smart Contract bisogna dapprima aprire l'applicazione Ganache: all'avvio possiamo creare un workspace personalizzato oppure avviarne uno di default tramite la sezione "Quickstart".

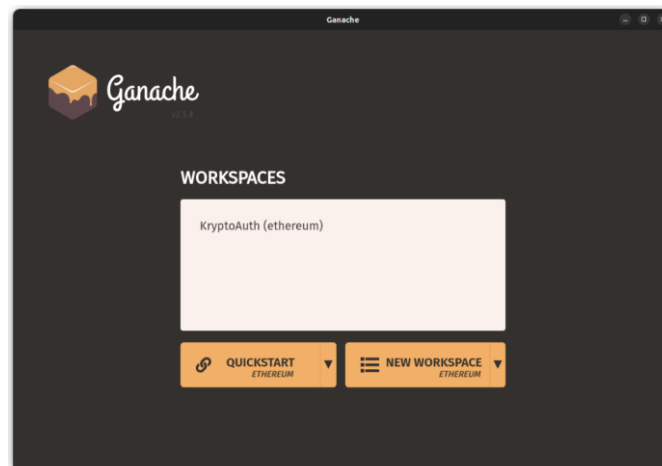


Figura 1. Homepage Ganache

Successivamente, importiamo la configurazione dello Smart Contract all'interno di Ganache andando a specificare il path di **`truffle-config.js`**:

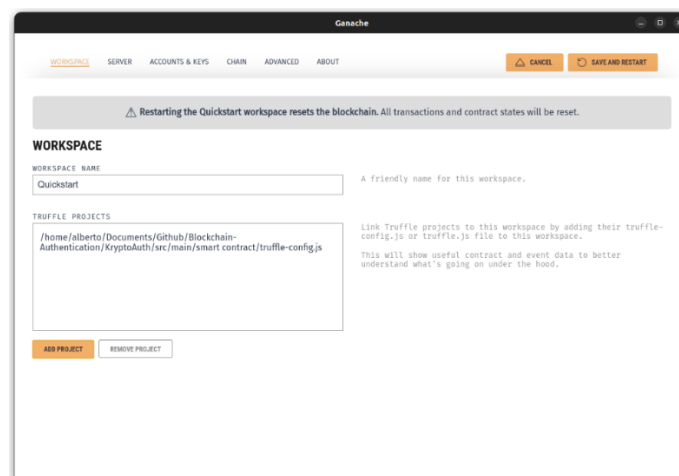
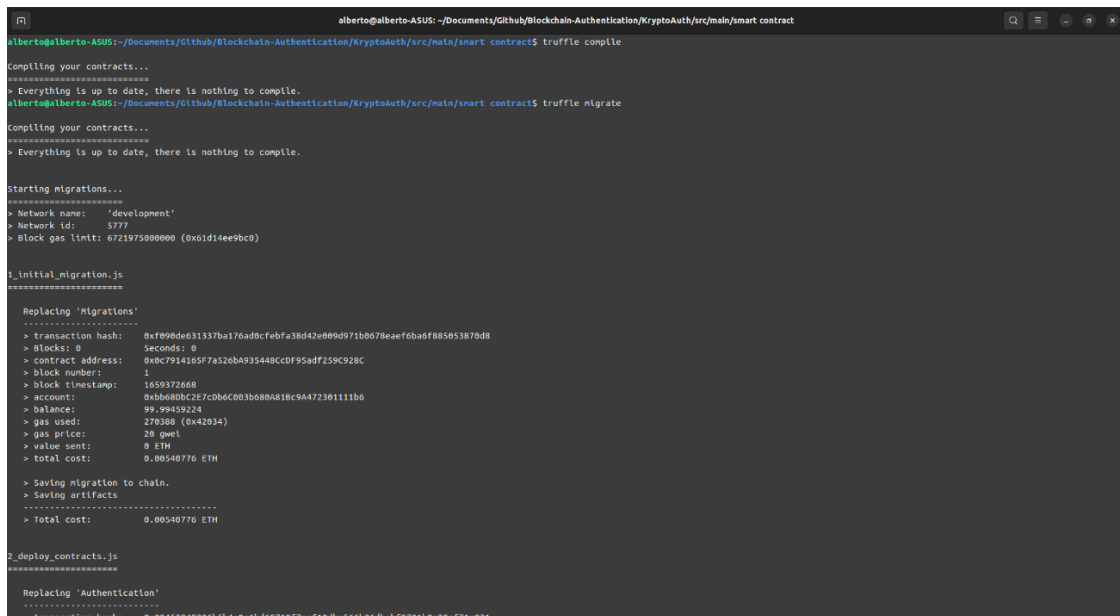


Figura 2. Aggiunta Smart Contract

Dopodiché, apriamo il nostro terminale e ci rechiamo nel package “**smart contract**” all’interno del progetto KryptoAuth. All’interno del terminale digitiamo:

- `truffle compile`, per verificare se ci sono errori sintattici all’interno dello Smart Contract;
- `truffle migrate`, per deployare lo Smart Contract (per effettuare un reset delle connessioni eseguiamo `truffle migrate --reset`).



```

alberto@alberto-ASUS: ~/Documents/Github/Blockchain-Authentication/KryptoAuth/src/main/smart contract
alberto@alberto-ASUS:~/Documents/Github/Blockchain-Authentication/KryptoAuth/src/main/smart contract$ truffle compile
Compiling your contracts...
> Everything is up to date, there is nothing to compile.
alberto@alberto-ASUS:~/Documents/Github/Blockchain-Authentication/KryptoAuth/src/main/smart contract$ truffle migrate
Compiling your contracts...
> Everything is up to date, there is nothing to compile.

Starting migrations...
> Network name: 'development'
> Network id: 5777
> Block gas limit: 0721975000000 (0x5d14ee9bc0)

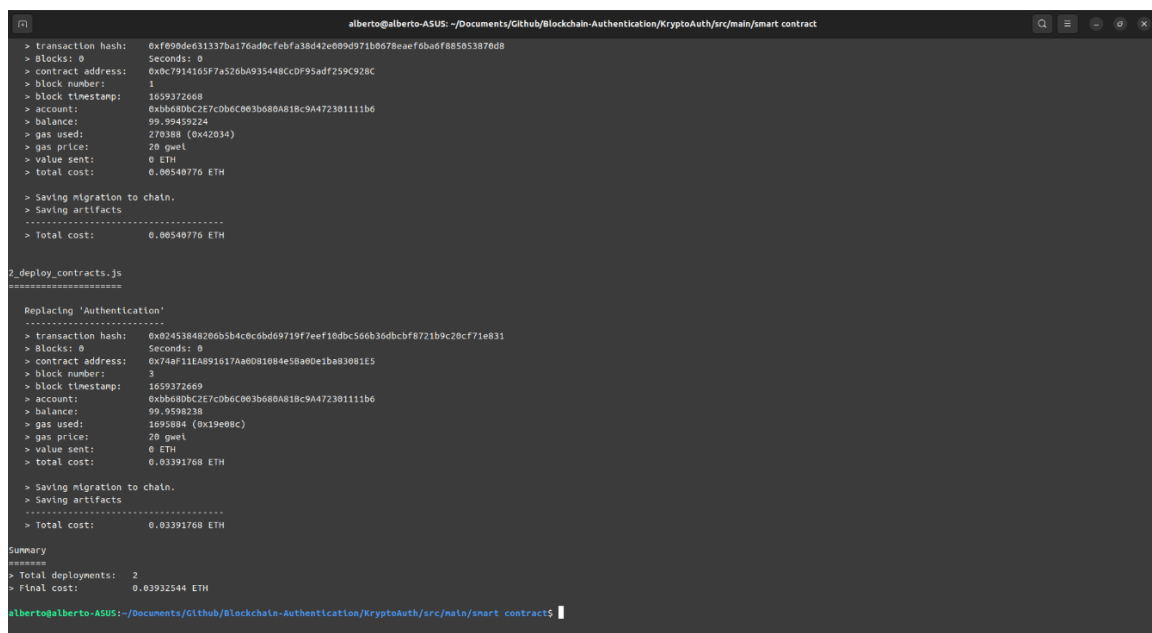
1_initial_migration.js
=====
> Replacing 'Migrations'
> -----
> transaction hash: 0xf090de631337ba176ad8cfebf38d42e009d971b0678eae6ba6f885053870d8
> blocks: 0
> seconds: 0
> contract address: 0x0c7914165f7a526ba935448ccdf95adf259c928c
> block number: 1
> block timestamp: 1659372668
> account: 0xb680bc2e7cd6c003b680a818c9a47230111b6
> balance: 99.99459224
> gas used: 270388 (0x42034)
> gas price: 20 gwei
> value sent: 0 ETH
> total cost: 0.00540776 ETH

> Saving migration to chain.
> Saving artifacts
> -----
> Total cost: 0.00540776 ETH

2_deploy_contracts.js
=====
> Replacing 'Authentication'
> -----
> transaction hash: 0x02453848206b5b4cc0bd69719f7eef10dbc566b36dbcbf8721b9c20cf71e831

```

Figura 3. Compilazione Smart Contract



```

> transaction hash: 0xf090de631337ba176ad8cfebf38d42e009d971b0678eae6ba6f885053870d8
> blocks: 0
> seconds: 0
> contract address: 0x0c7914165f7a526ba935448ccdf95adf259c928c
> block number: 1
> block timestamp: 1659372668
> account: 0xb680bc2e7cd6c003b680a818c9a47230111b6
> balance: 99.99459224
> gas used: 270388 (0x42034)
> gas price: 20 gwei
> value sent: 0 ETH
> total cost: 0.00540776 ETH

> Saving migration to chain.
> Saving artifacts
> -----
> Total cost: 0.00540776 ETH

2_deploy_contracts.js
=====
> Replacing 'Authentication'
> -----
> transaction hash: 0x02453848206b5b4cc0bd69719f7eef10dbc566b36dbcbf8721b9c20cf71e831
> blocks: 0
> seconds: 0
> contract address: 0x74af11EAB91617Aa0D81084e58a0e1ba83081E5
> block number: 3
> block timestamp: 1659372669
> account: 0xb680bc2e7cd6c003b680a818c9a47230111b6
> balance: 99.9598238
> gas used: 1695804 (0x19e08c)
> gas price: 20 gwei
> value sent: 0 ETH
> total cost: 0.03391768 ETH

> Saving migration to chain.
> Saving artifacts
> -----
> Total cost: 0.03391768 ETH

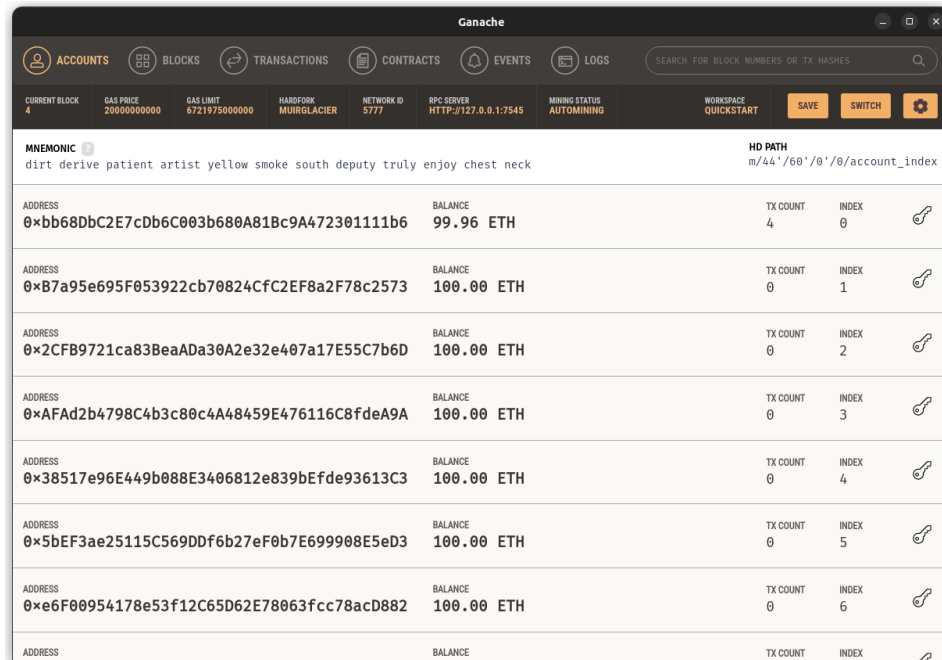
Summary
=====
> Total deployments: 2
> Final cost: 0.03932544 ETH

alberto@alberto-ASUS:~/Documents/Github/Blockchain-Authentication/KryptoAuth/src/main/smart contract$

```

Figura 4. Deploy Smart Contract

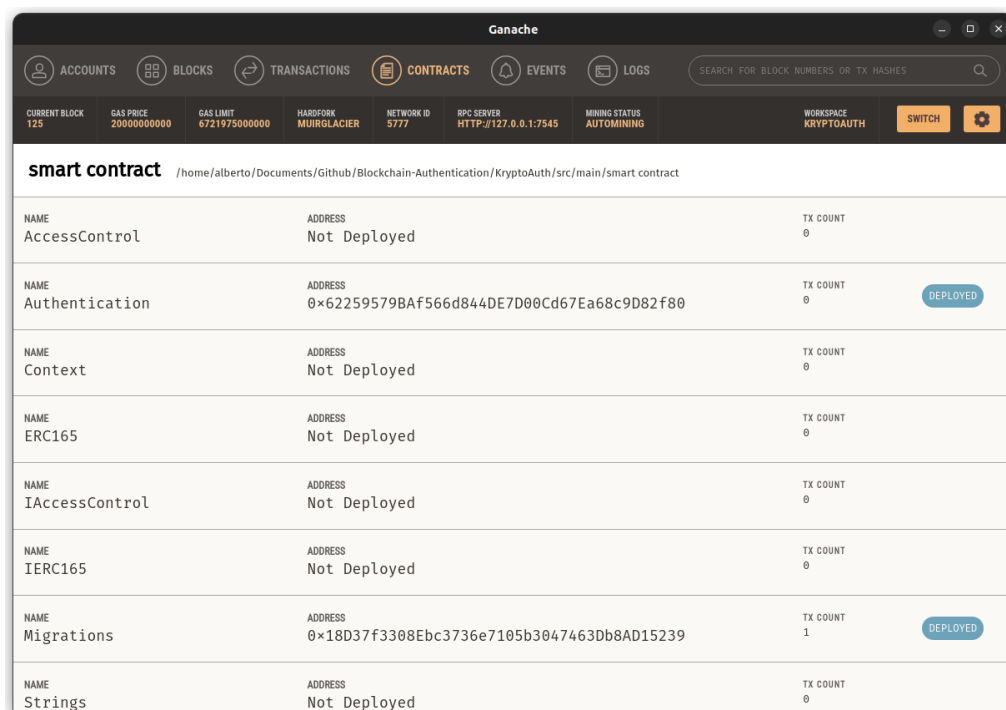
Una volta completata la procedura il nostro contratto sarà deployato sulla Blockchain Ganache. Infatti, nella Figura 3., possiamo notare che il primo address ha speso 0.03932544 ETH per effettuare la seguente transazione.



ADDRESS	BALANCE	TX COUNT	INDEX
0xbb68DbC2E7cDb6C003b680A81Bc9A47230111b6	99.96 ETH	4	0
0xB7a95e695F053922cb70824CfC2EF8a2F78c2573	100.00 ETH	0	1
0x2CFB9721ca83BeaADa30A2e32e407a17E55C7b6D	100.00 ETH	0	2
0xAFAd2b4798C4b3c80c4A48459E476116C8fdeA9A	100.00 ETH	0	3
0x38517e96E449b088E3406812e839bFde93613C3	100.00 ETH	0	4
0x5bEF3ae25115C569DDf6b27eF0b7E699908E5eD3	100.00 ETH	0	5
0xe6F00954178e53f12C65D62E78063fcc78acD882	100.00 ETH	0	6

Figura 5. Accounts Ganache

Nella sezione “Contracts” ci sono gli indirizzi dei contratti deployati.



NAME	ADDRESS	TX COUNT	STATUS
AccessControl	Not Deployed	0	
Authentication	0x62259579BAf566d844DE7D00Cd67Ea68c9D82f80	0	DEPLOYED
Context	Not Deployed	0	
ERC165	Not Deployed	0	
IAccessControl	Not Deployed	0	
IERC165	Not Deployed	0	
Migrations	0x18D37f3308Ebc3736e7105b3047463Db8AD15239	1	DEPLOYED
Strings	Not Deployed	0	

Figura 6. Contracts Address Ganache

Una volta che il contratto sarà deployato, copiamo il contract address dello Smart Contract KryptoNFT di Ganache e lo andremo ad inserire nel progetto nella classe **BlockchainServiceImpl** assegnandolo alla costante **CONTRACT_ADDRESS**, poiché quest'ultima avrà l'indirizzo del deploy precedente:

```
@Service
public class BlockchainServiceImpl implements BlockchainService {

    2 usages
    private final static Web3j web3j = Web3j.build(new HttpService( url: "HTTP://127.0.0.1:7545"));
    1 usage
    private final static String CONTRACT_ADDRESS = "0x62259579BAf566d8440E7D00Cd67Ea68c9D82f80";
```

Figura 7. Contracts Address Ganache in Java

Inoltre, assicuriamoci che il **GAS LIMIT** in Ganache sia impostato su **41000000000**.

2.2 Conversione Smart Contract in classe Java

Per tradurre lo Smart Contract scritto in Solidity in una classe Java, nel terminale digitiamo:

```
solcjs /home/alberto/Documents/GitHub/Kryptoauth-
NFT/KryptoAuth/src/main/'smart contract'/contracts/KryptoNFT.sol --bin --
include-path /home/alberto/.nvm/versions/node/v16.17.0/lib/node_modules/
--base-path . --abi --optimize -o /home/alberto/Documents/GitHub/
Kryptoauth-NFT/KryptoAuth/src/main/resources/solidity
```

In questo modo nella cartella solidity verranno generati diversi file; noi andremo a conservare solo i file **KryptoNFT.abi** e **KryptoNFT.bin** rinominandoli.

Infine, utilizzeremo web3j per creare la classe Java a partire dai due file appena generati:

```
web3j generate solidity -b ./src/main/resources/solidity/KryptoNFT.bin -a
./src/main/resources/solidity/KryptoNFT.abi -o ./src/main/java -p
it.unisa.KryptoAuth.contracts
```

2.3 Configurazione rete Metamask - Ganache

Per collegare l'estensione browser Metamask alla Blockchain Ganache i passaggi iniziali da seguire sono di installare e di registrarsi a Metamask; successivamente dalle impostazioni dell'estensione andiamo nella sezione “Aggiungi Rete” per creare una nuova rete.

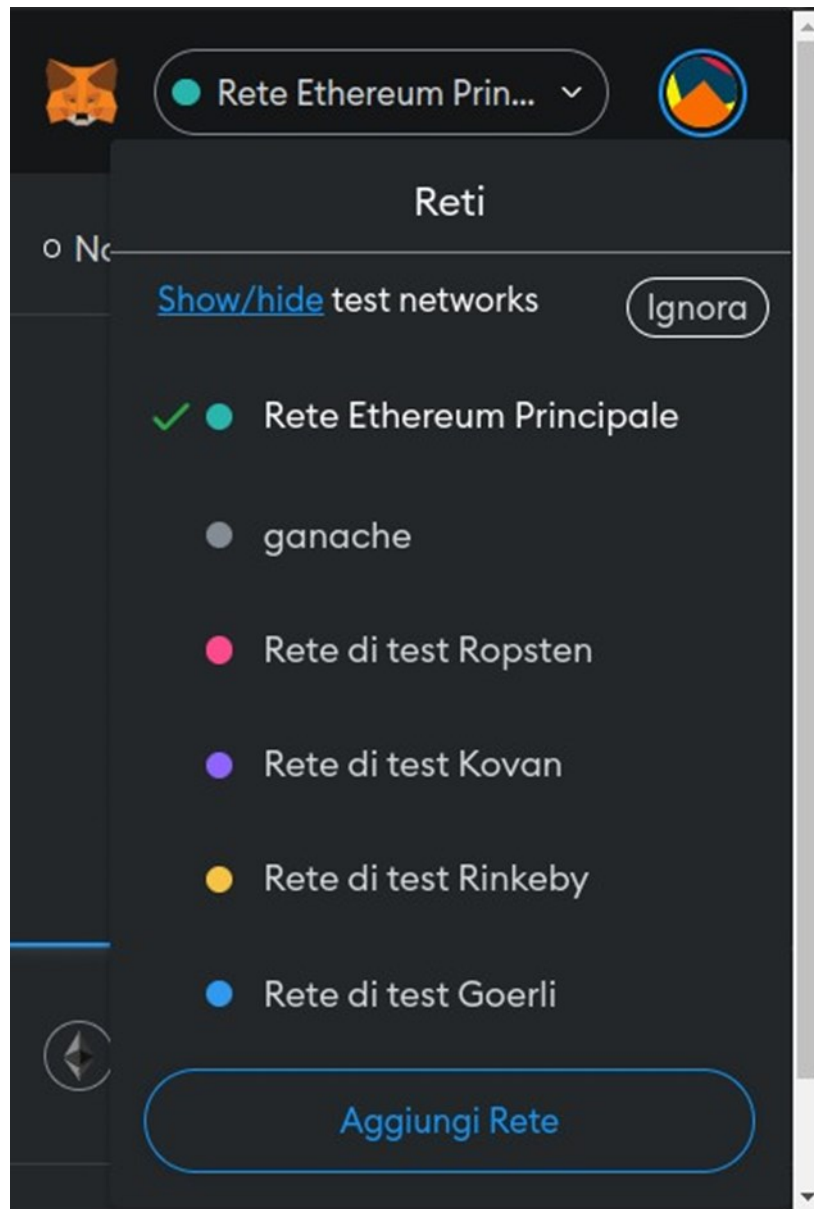


Figura 8. Aggiungi Rete

Le informazioni che devono essere inserite devono essere reperite da Ganache, in particolare:

- **Nome rete:** assegniamo il nome che vorremmo che abbia la nuova rete;
- **Nuovo URL RPC:** è l'indirizzo http di Ganache (default [HTTP://127.0.0.1:7545](http://127.0.0.1:7545));
- **Chain ID:** si deve inserire 1337 che corrisponde all'id di Ethereum;
- **Currency Symbol:** si deve inserire “ETH” se abbiamo una Blockchain Ethereum.

Figura 9. Configurazione Rete

Salviamo la nuova rete ed importiamo gli account da Ganache andando nella sezione “Importa Account” di Metamask.

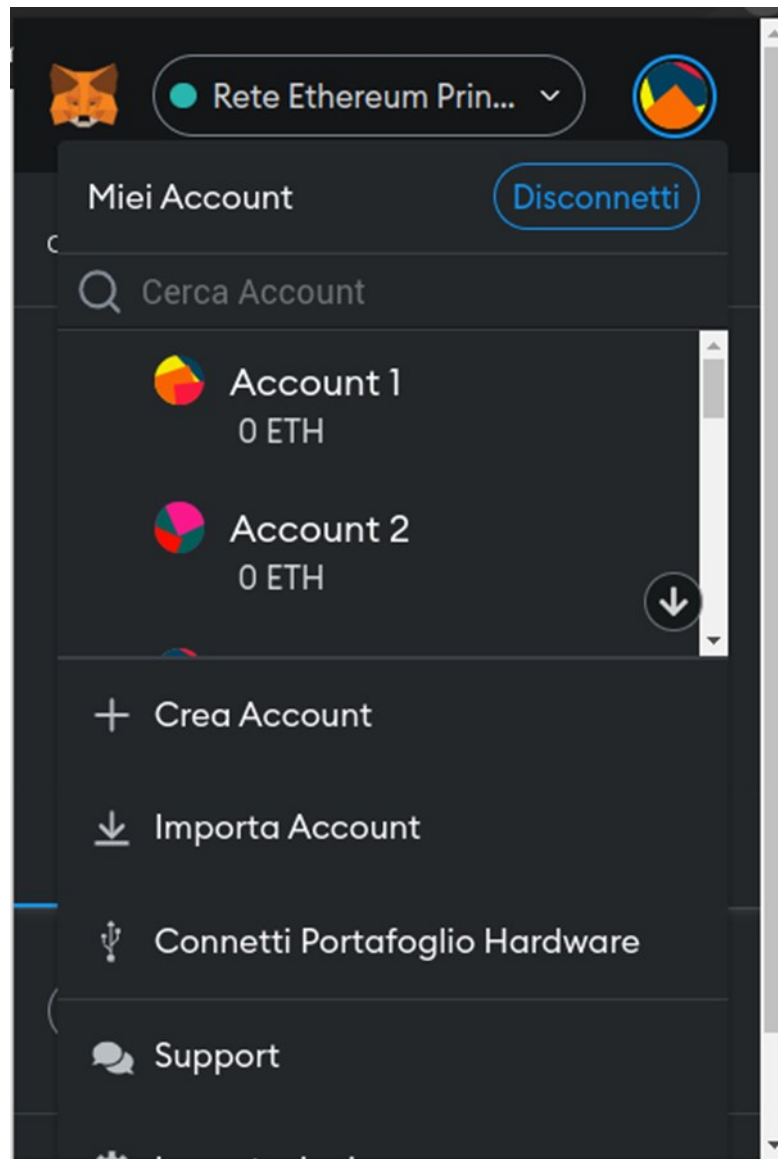


Figura 10. Importa Account



2.4 Avvio Web DApp

Per poter utilizzare la Web DApp KryptoAuth bisogna accedere dall'IDE JetBrains IntelliJ e avviare la classe main “KryptoAuth”. Avviato il server Tomcat grazie a Spring Boot, accediamo al nostro Web Browser alla pagina <http://localhost:8080/kryptoauth>.

Ps. controllare che nella cartella `resources/static/txt` i due file json siano vuoti (devono contenere solo ‘[]’).

2.5 Esempio generazione NFT in Pinata

Quando un amministratore vuole creare per la prima volta un nuovo NFT, prima di inserire i dati all'interno dell'applicazione KryptoAuth deve effettuare una prima configurazione dell'NFT su Pinata. Se tutto va a buon fine, l'amministratore vedrà nella pagina “Aggiungi NFT” i nomi degli NFT creati su Pinata e che potrà generare e salvare sulla Blockchain.

1. Effettuiamo il Login su [Pinata](#);
2. Clicchiamo sul bottone “Upload +” e poi scegliamo “File”;
3. Clicchiamo su “Select File” e dal nostro computer scegliamo la foto di un NFT da caricare;
4. Clicchiamo su “Upload”;
5. Dopodichè facciamo il reload della pagina e quando ci verrà mostrato la foto caricata su Pinata andremo a selezionare la casella “More” e poi “Edit Details”;
6. Inseriamo due coppie chiave - valore:
 - Key: created • Value: 1
 - Key: seller • Value: 0x4a70bef29d6fb.... (l'indirizzo dell'amministratore che vuole creare l'NFT).