



Laurea Triennale in Informatica - Università di Salerno -
Sistema di autenticazione sulla rete Blockchain Ethereum



KRYPTOAUTH

Manuale delle Istruzioni KryptoAuth

Riferimento	
Versione	1.0
Data	29/07/2022
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 Contracts	4
2.2 Configurazione rete Metamask - Ganache	7
2.3 Installazione Web DApp	10



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 e, infine, la traduzione dello Smart Contract scritto in Solidity in una classe Java mediante l'uso di solc.js e Web3j.

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](#));
- **Solc**, per generare l'abi e il bin dello Smart Contract (**LINK:** [solc.js](#));
- **Truffle**, per effettuare il deploy dello Smart Contract su Ganache (**LINK:** [Truffle](#)).

2.1 Deploy dello Smart Contract

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".

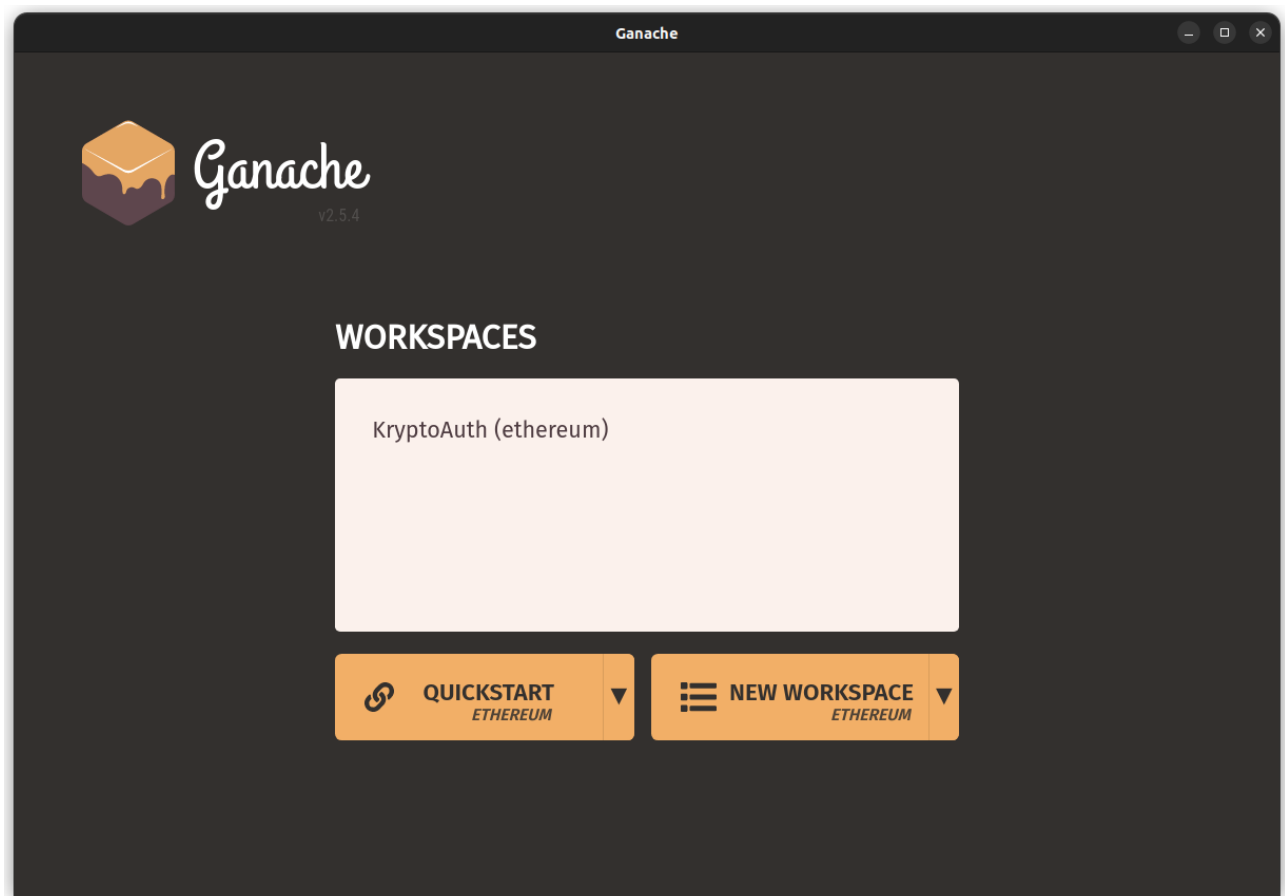


Figura 1. Homepage Ganache

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
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: 6721975000000 (0x61d14ee9bc0)

1_initial_migration.js
=====
> Replacing 'Migrations'
> -----
> transaction hash: 0xf090de631337ba176ad0cfefba38d42e009d971b0678eae6ba6f885053870d8
> Blocks: 0 Seconds: 0
> contract address: 0x0c7914165f7a520ba935448CcdF95adf259C928C
> 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: 0x02453848206b5b4c0c0bd69719f7eef10dbc566b36dbcbf8721b9c20cf71e831

```

Figura 2. Compilazione Smart Contract

```

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

> transaction hash: 0xf090de631337ba176ad0cfefba38d42e009d971b0678eae6ba6f885053870d8
> Blocks: 0 Seconds: 0
> contract address: 0x0c7914165f7a520ba935448CcdF95adf259C928C
> 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: 0x02453848206b5b4c0c0bd69719f7eef10dbc566b36dbcbf8721b9c20cf71e831
> Blocks: 0 Seconds: 0
> contract address: 0x74af11Ea891617Aa00B1084e5Ba0De1ba3081E5
> block number: 3
> block timestamp: 1659372669
> account: 0xb680bc2E7CD6c003b680A818c9A47230111b6
> balance: 99.9598238
> gas used: 1695884 (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 3. 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.



Laurea Triennale in Informatica - Università di Salerno - Sistema di autenticazione sulla rete Blockchain Ethereum

Ganache

ACCOUNTS

BLOCKS

TRANSACTIONS

CONTRACTS

EVENTS

LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK

4

GAS PRICE

20000000000

GAS LIMIT

6721975000000

HARDFORK

MUIRGLACIER

NETWORK ID

5777

RPC SERVER

HTTP://127.0.0.1:7545

MINING STATUS

AUTOMINING

WORKSPACE

QUICKSTART

SAVE

UNDO

MNEMONIC

dirt derive patient artist yellow smoke south deputy truly enjoy chest neck

HD PATH

m/44'/60'/0'/0'/account_index

ADDRESS

0xbb68DbC2E7cDb6C003b680A81Bc9A47230111b6

BALANCE

99.96 ETH

TX COUNT

4

INDEX

0

ADDRESS

0xB7a95e695F053922cb70824CfC2EF8a2F78c2573

BALANCE

100.00 ETH

TX COUNT

0

INDEX

1

ADDRESS

0x2CFB9721ca83BeaADa30A2e32e407a17E55C7b6D

BALANCE

100.00 ETH

TX COUNT

0

INDEX

2

ADDRESS

0xAFAd2b4798C4b3c80c4A48459E476116C8fdeA9A

BALANCE

100.00 ETH

TX COUNT

0

INDEX

3

ADDRESS

0x38517e96E449b088E3406812e839bEfde93613C3

BALANCE

100.00 ETH

TX COUNT

0

INDEX

4

ADDRESS

0x5bEF3ae25115C569DDf6b27eF0b7E699908E5eD3

BALANCE

100.00 ETH

TX COUNT

0

INDEX

5

ADDRESS

0xe6F00954178e53f12C65D62E78063fcc78acD882

BALANCE

100.00 ETH

TX COUNT

0

INDEX

6

ADDRESS

BALANCE

TX COUNT

INDEX

Figura 5. Accounts Ganache

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

Ganache

ACCOUNTS

BLOCKS

TRANSACTIONS

CONTRACTS

EVENTS

LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK125

GAS PRICE20000000000

GAS LIMIT6721975000000

HARDFORKMUIRGLACIER

NETWORK ID5777

RPC SERVERHTTP://127.0.0.1:7545

MINING STATUSAUTOMINING

WORKSPACEKRYPTOAUTH

SWITCH

smart contract

/home/alberto/Documents/Github/Blockchain-Authentication/KryptoAuth/src/main/smart contract

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

Figura 5. Contracts Address Ganache

2.2 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.

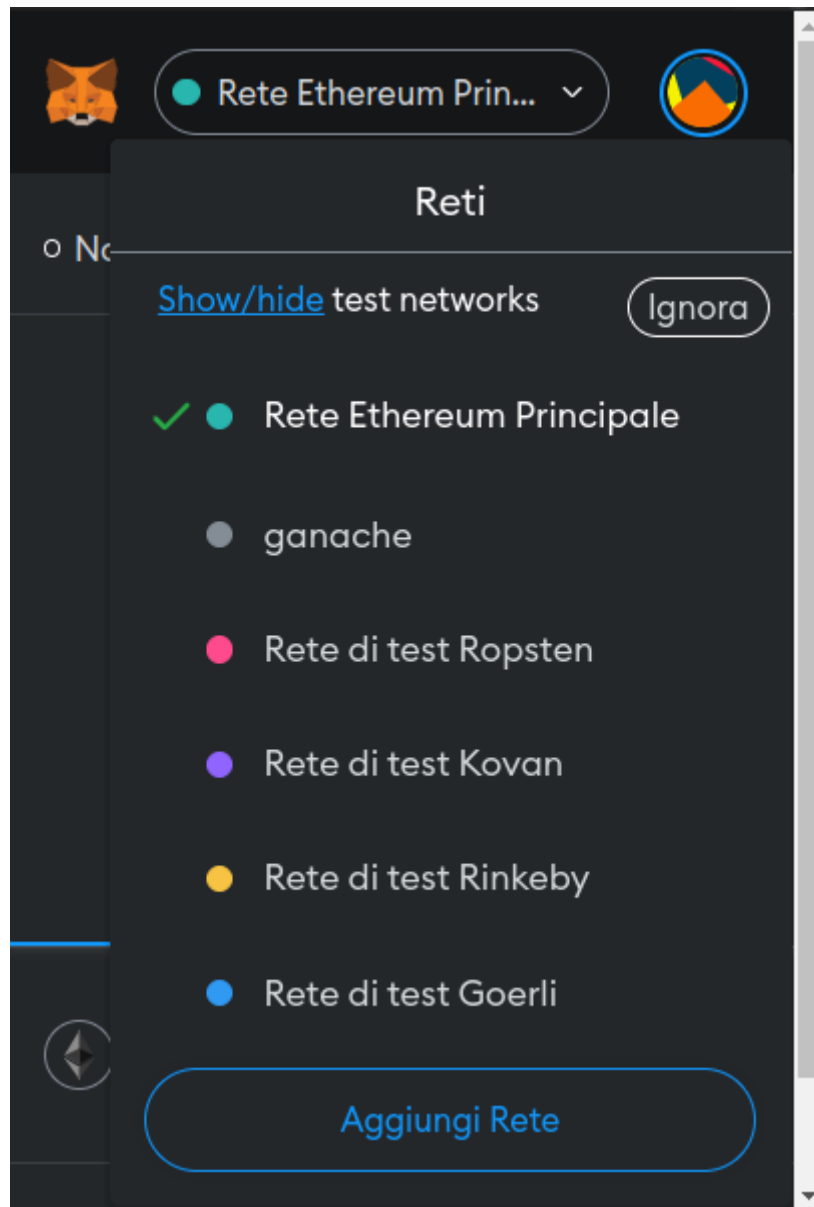


Figura 6. Aggiungi Rete

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);
- Chain ID: si deve inserire 1337 che corrisponde all'id di Ethereum;
- Currency Symbol: si deve inserire "ETH" se abbiamo una Blockchain Ethereum.

Figura 7. Configurazione Rete

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

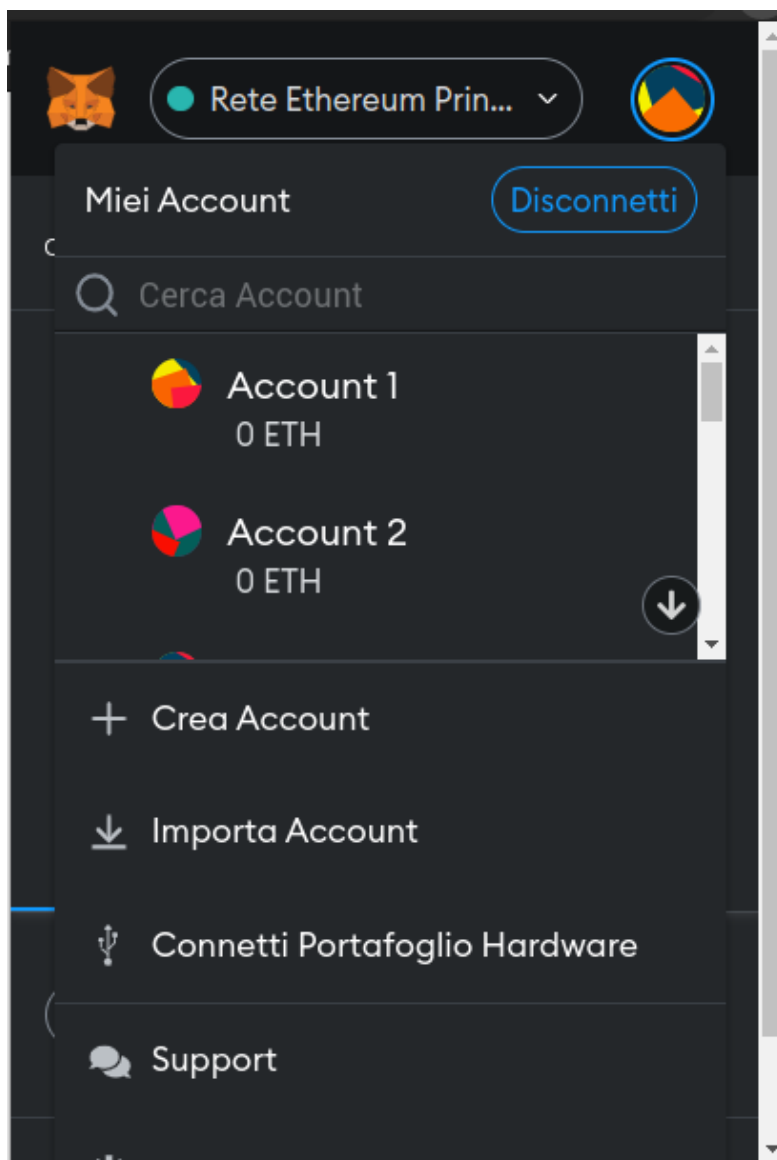


Figura 8. Importa Account

2.3 Installazione 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>.

Nel caso in cui si volesse tradurre nuovamente lo Smart Contract scritto in Solidity in una classe Java, nel terminale digitiamo:

```
alberto@alberto-ASUS: ~  
alberto@alberto-ASUS:~$ solcjs /home/alberto/Documents/Github/Blockchain-Authentication/KryptoAuth  
/src/main/'smart contract'/contracts/Authentication.sol --bin --include-path node_modules/ --base-  
path . --abi --optimize -o /home/alberto/Documents/Github/Blockchain-Authentication/KryptoAuth/src  
/main/resources/solidity
```

Figura 9. Generazione .abi e .bin



```
alberto@alberto-ASUS: ~  
alberto@alberto-ASUS:~$ web3j generate solidity -b ./src/main/resources/solidity/Authentication.bin -a ./src/main/resources/solidity/Authentication.abi -o ./src/main/java -p it.unisa.KryptoAuth.contracts
```

Figura 10. Generazione classe Java