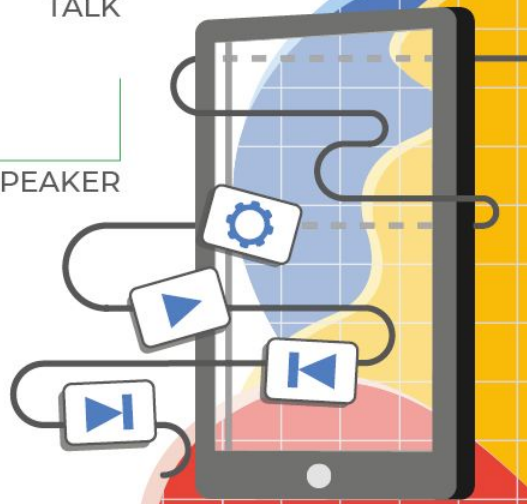
BLOCKCHAIN
Smart Contract from Scratch

TALK

Alessandro Berti
Luca Corbucci
Eugenio Paluello

SPEAKER

DEVPARTY
TOGETHER 2020



Who are we?

Alessandro Berti

ICT Solutions Architect

Computer Science Student
@University of Pisa 🇮🇹

Luca Corbucci

Computer Science Student
@University of Pisa 🇮🇹

👨‍💻🎤🎧📷⚽

Eugenio Paluello

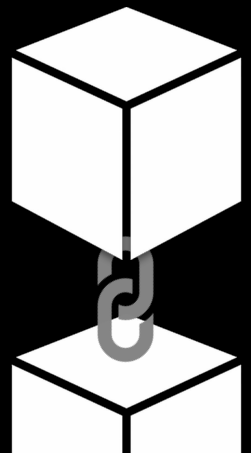
ICT Solutions Architect

Computer Science Student
@University of Pisa 🇮🇹

What are we gonna do?

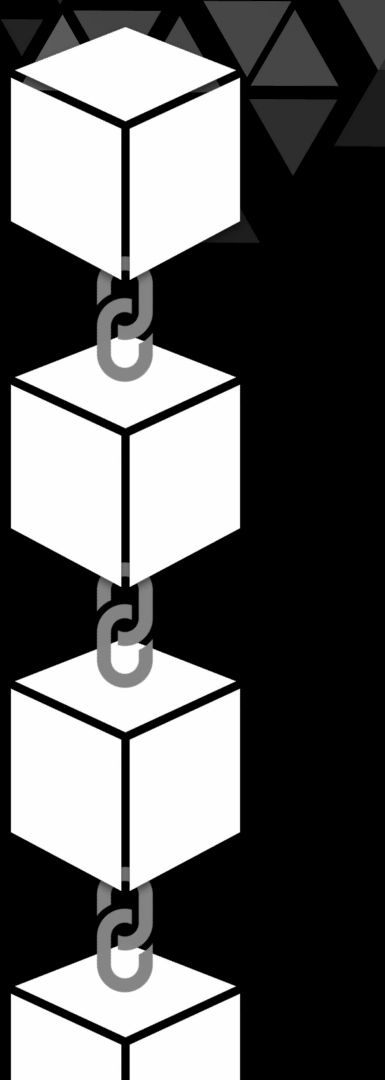
- **Let’s Grasp the Idea!** (Theory)
- **Smart Contracts**
- **Deploy your Contract!**

Let’s Grasp the Idea!



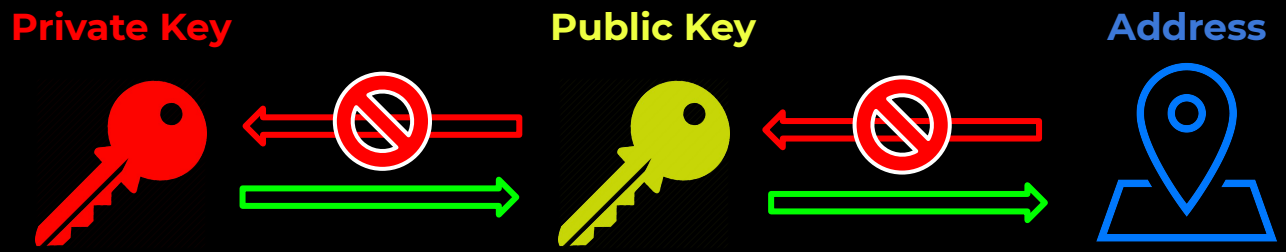
What is ?

*“The Blockchain is a **shared**, **trusted**, **public** ledger of **transactions** grouped into **blocks**”*



Transaction

***Atomic transfer** of "some-kind-of-value" between **two or more** entities.*

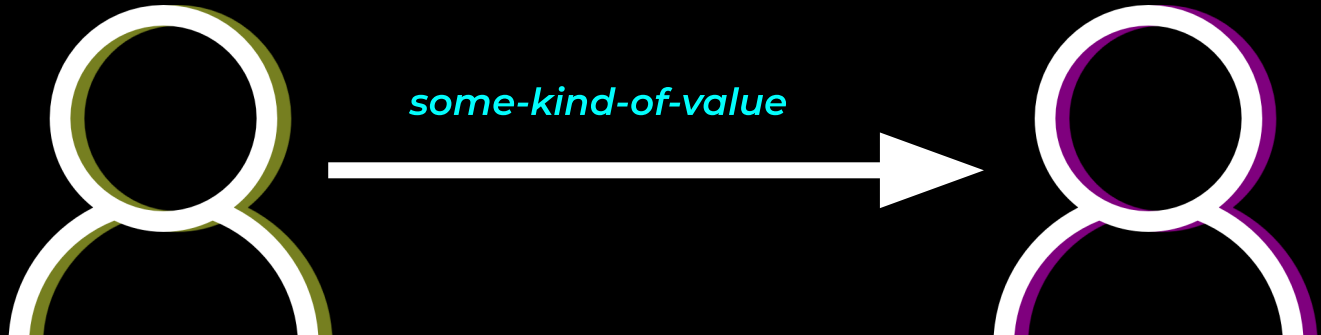


ADDRESS_1

36mdwq3JZHjpJMhokn4rVeeuzHTXGukX1L

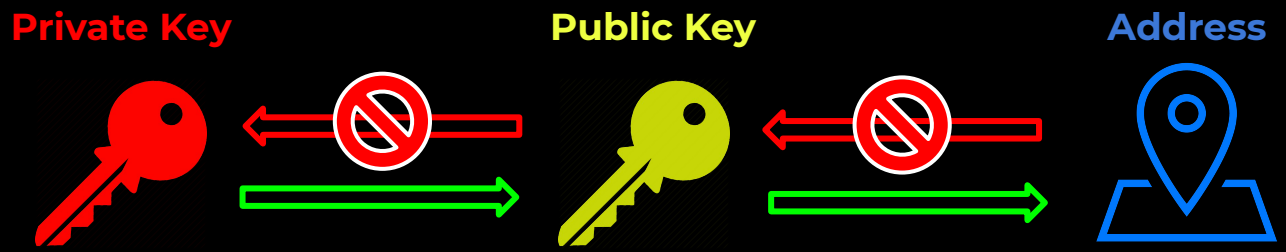
ADDRESS_2

14TDxS9NQhiu1tX4qeFwRkisXn1oDmTuKB



Transaction

***Atomic transfer** of "some-kind-of-value" between **two or more** entities.*

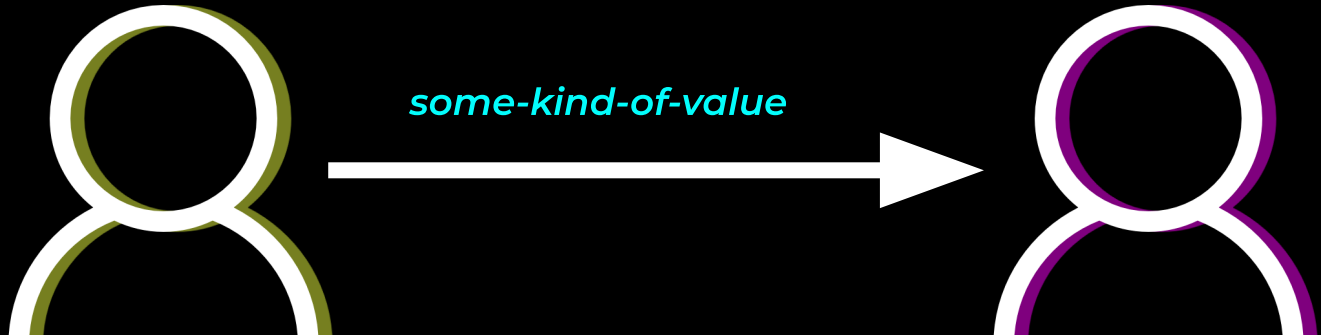


ADDRESS_1

36mdwq3JZHjpJMhokn4rVeeuzHTXGukX1L

ADDRESS_2

14TDxS9NQhiu1tX4qeFwRkisXn1oDmTuKB



Mining

Transaction_3

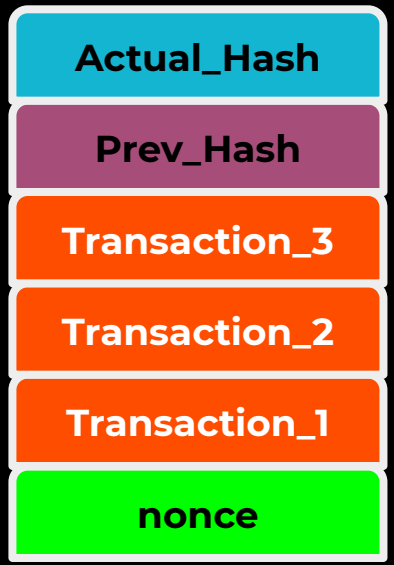
Transaction_2

Transaction_1

Transaction

ADDRESS_1
ADDRESS_2
some-kind-of-value

Mining (PoW)



Which is that value "nonce" such that:

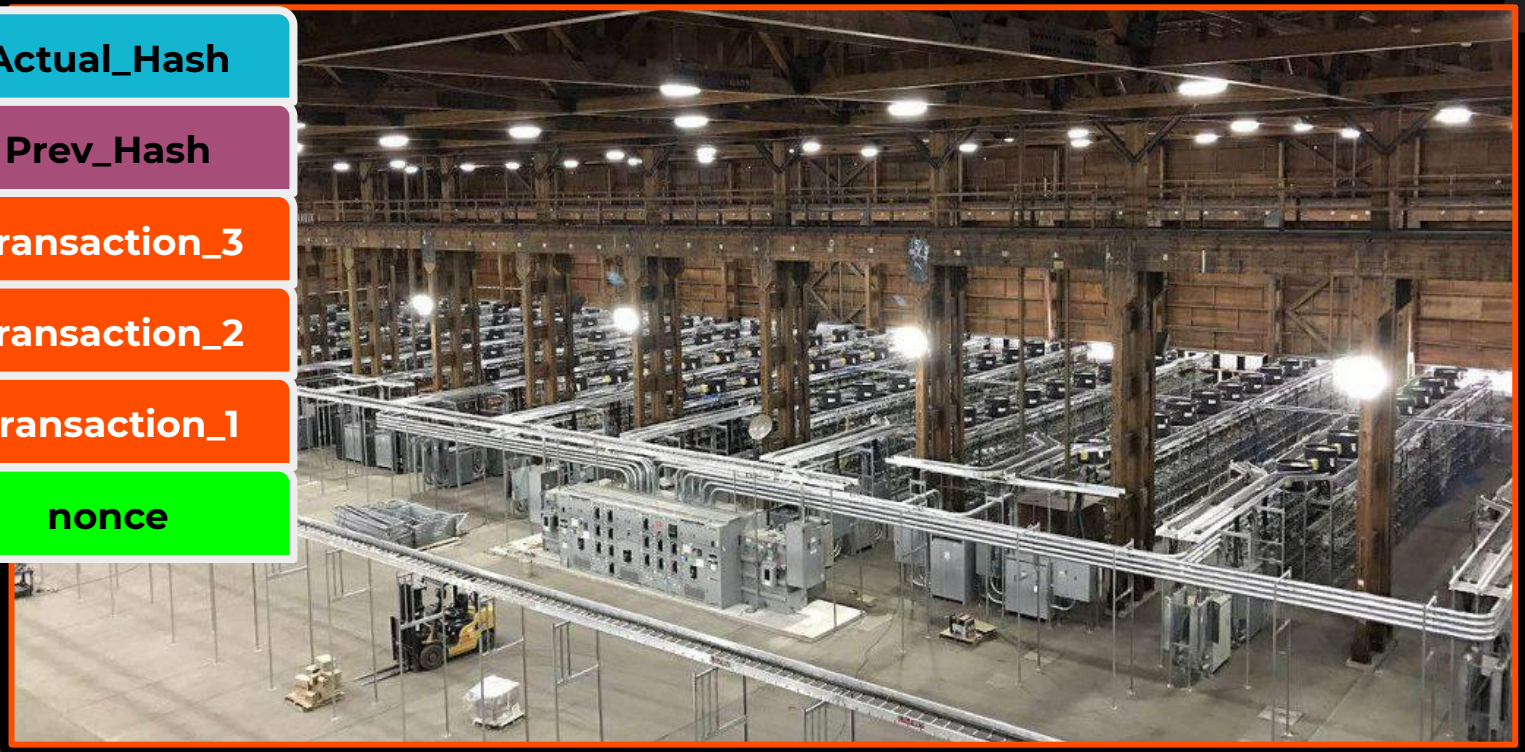
Hash(Tx_1, Tx_2, Tx_3, **Prev_Hash**, **nonce**) < Difficulty

If **found** *then*

Hash_ActBlock = **Hash**(Tx_1, Tx_2, Tx_3, **Prev_Hash**, **nonce**)

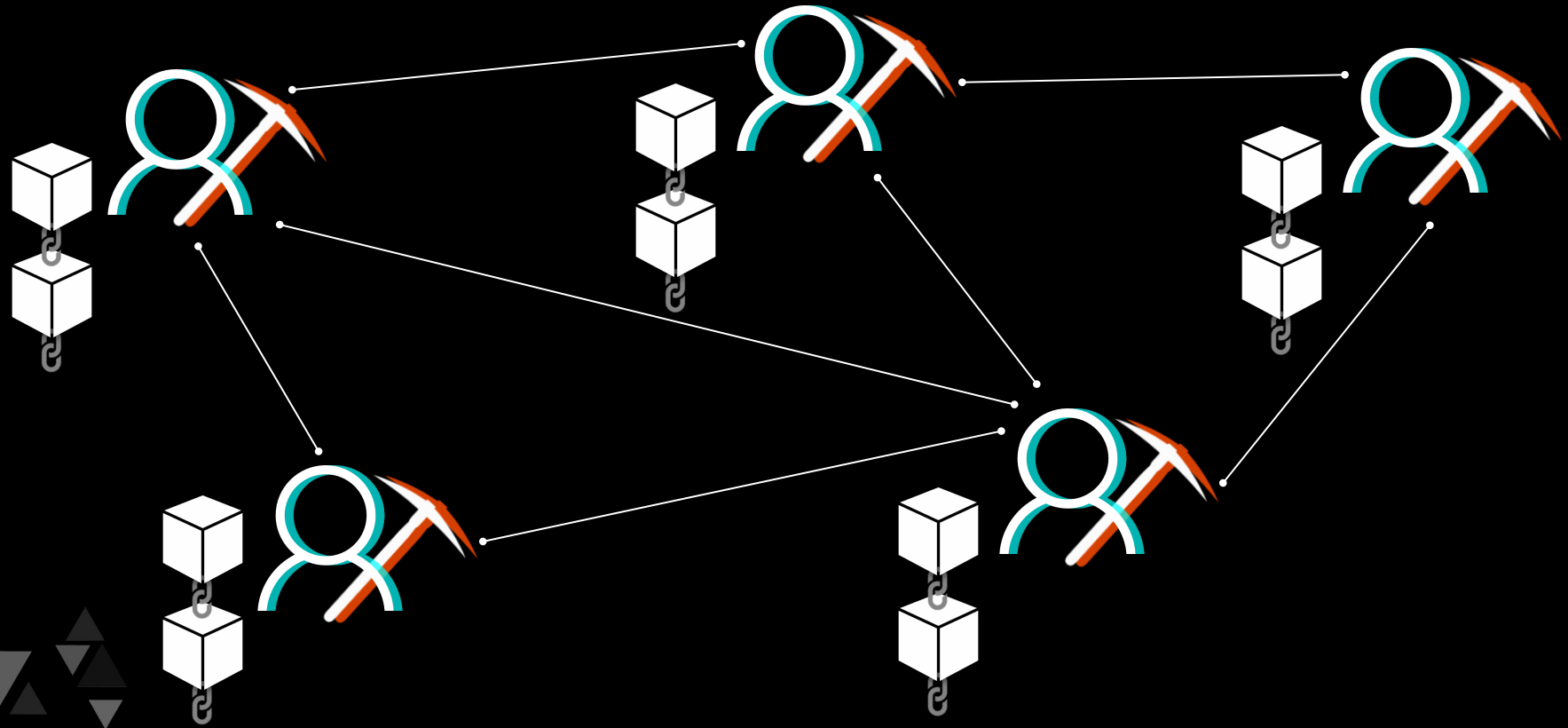
Mining (PoW)

- Actual_Hash
- Prev_Hash
- Transaction_3
- Transaction_2
- Transaction_1
- nonce

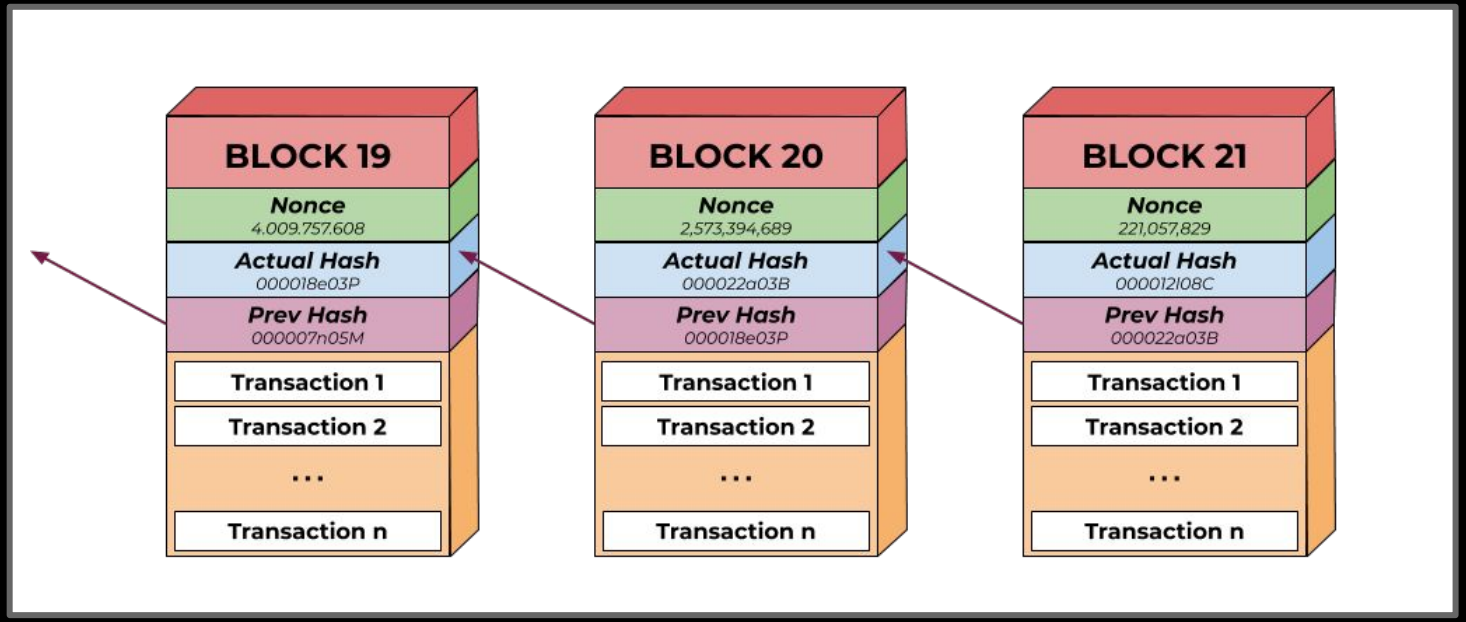


Shared

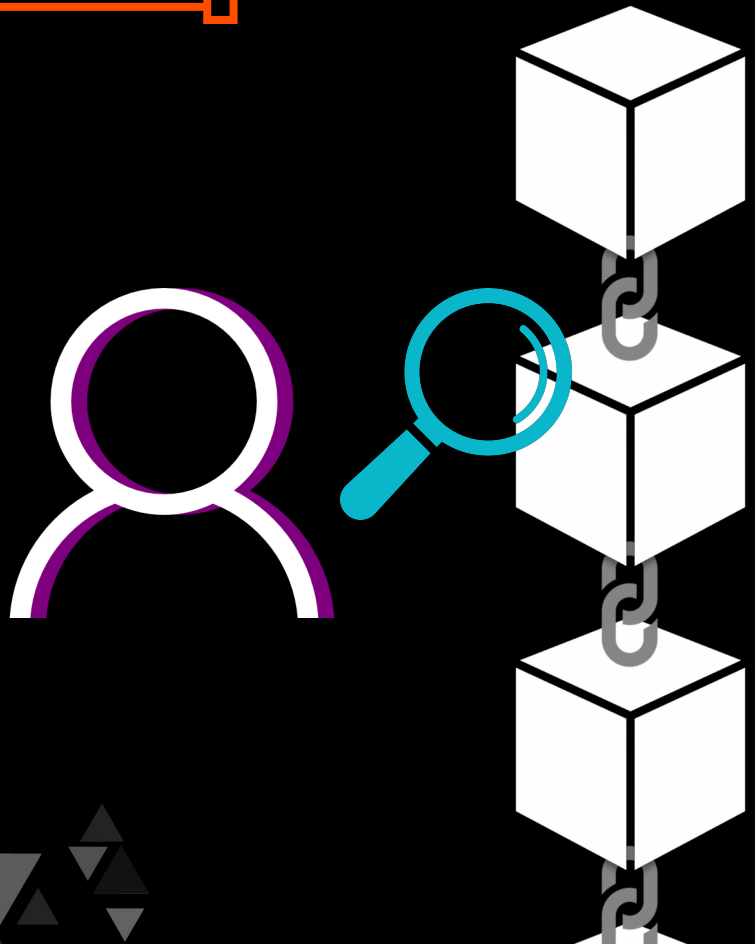
The blockchain is shared across the miners.
Namely: each miner has a consistent ***replica*** of the blockchain



Trusted


BLOCK 19
Nonce
4.009.757.608
Actual Hash
000018e03P
Prev Hash
000007n05M
Transaction 1
Transaction 2
...
Transaction n
BLOCK 20
Nonce
2,573,394,689
Actual Hash
000022a03B
Prev Hash
000018e03P
Transaction 1
Transaction 2
...
Transaction n
BLOCK 21
Nonce
221,057,829
Actual Hash
000012108C
Prev Hash
000022a03B
Transaction 1
Transaction 2
...
Transaction n

Public



BLOCKCHAIN.COM Prodotti Dati Esploratore Accesso Iscriviti

Le transazioni

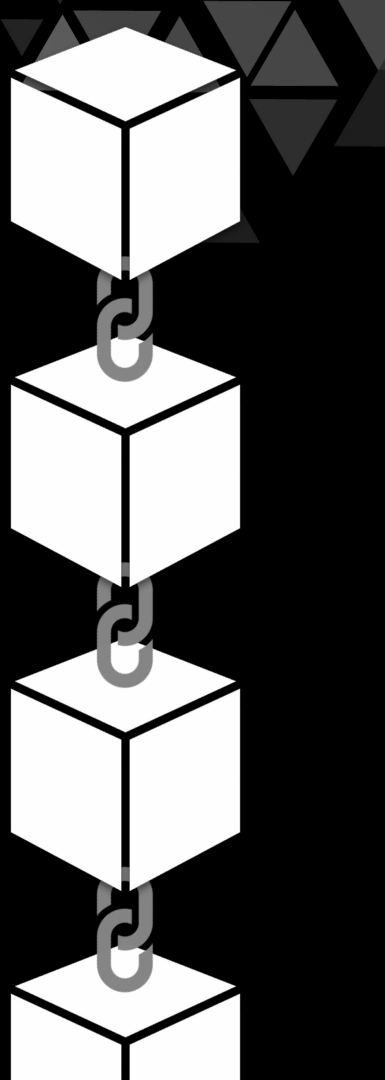
Standard Interno

1 2 3 4 5 Il prossimo +10

hash	0×03411439f603b54f4cca767019fa89f645e2682f362591bc77913...		2020-04-12 23:12
	0xd0808da05cc71a9f308d330bc9c5c81bbc26fc59	→	0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48
tassa	0.000129075 ETH (43025 GAS - 3000000000 WEI)		1 Conferme 0.00000000 ETH
hash	0×06f8a4225b61f7575ae9f03109539daf4c5624641d6406b21b42...		2020-04-12 23:12
	0xff1b9745f68f84f036e5e92c920038d895fb701a	→	0×693c188e40f760ecf00d2946ef45260b84fbc43e
tassa	0.00015503 ETH (31006 GAS - 5000000000 WEI)		1 Conferme 0.00000000 ETH
hash	0×0c215222b2237ce2cb03263065753c131341322e95c334d8b7a...		2020-04-12 23:12
	0×38caa9a43c911a5bd745c5ba8d40dbaad26f90e1	→	0×794e6e91555438afc3ccf1c5076a74f42133d08d
tassa	0.00141332026 ETH (242422 GAS - 5830000000 WEI)		1 Conferme 0.00000000 ETH

What is ?

*“The Blockchain is a **shared**, **trusted**, **public** ledger of **transactions** grouped into **blocks**”*



Examples

	bitcoin	ethereum
Transaction Scheme Model	UTXO	Account Based
Consensus Algorithm	PoW	PoW[1]
Block Validation Time	10 mins	15 secs
Turing Complete	No	Yes[2] 

[1]Moving to PoS
[2]Actually, “Rich-Statefulness”

Smart Contracts

ethereum

What is ?

A *smartcontract* is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a *contract*.

Smart contracts help you exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman.

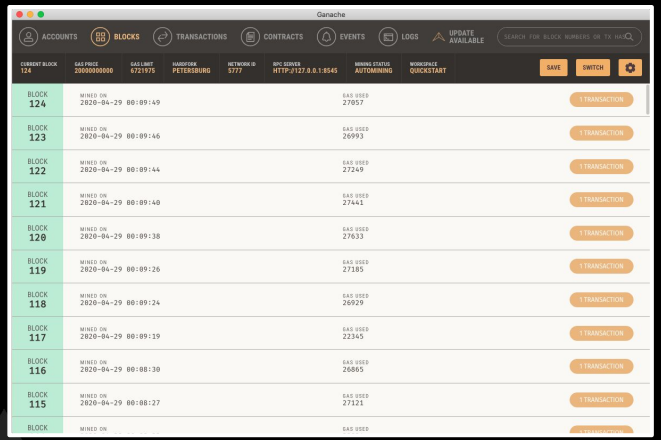
Deploy Your Contract!

ethereum

Test Net vs Ganache

Ganache

Ganache creates a **fake blockchain** that runs on your machine. All the **transactions are immediately mined**.



Test Net

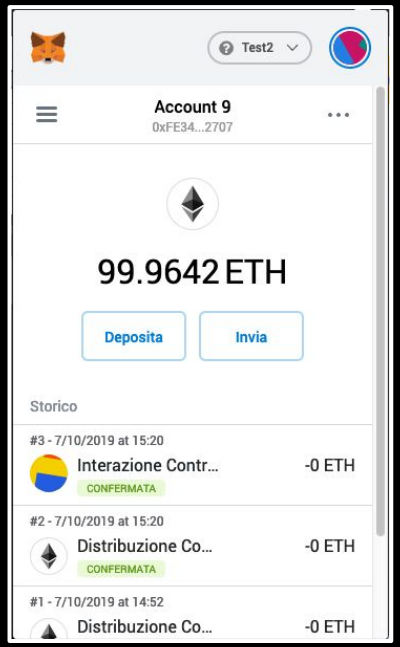
If you want to try your contract in a **“real” world** you can use the Ethereum Test Net.
The **transactions are mined after a few seconds**.

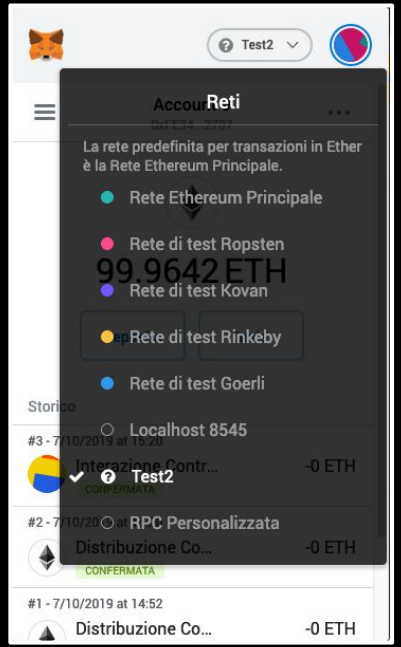
<u>There exists several Test net:</u>

- Ropsten
- Kovan
- Rinkeby
- Gorli

Metamask

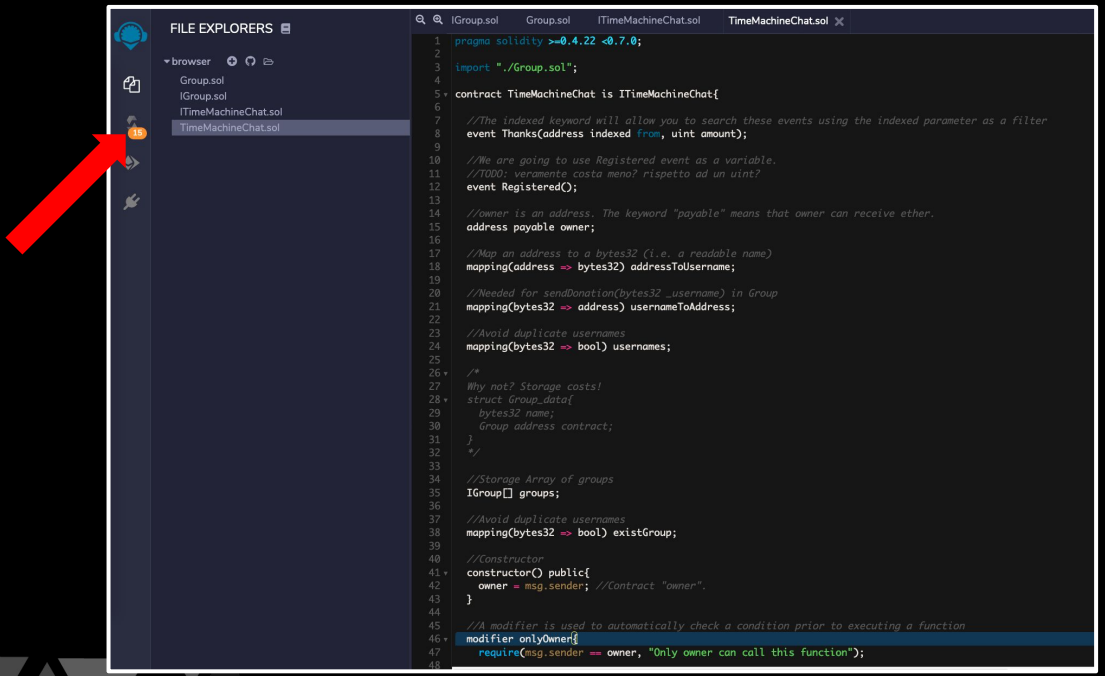
MetaMask is an **extension** for **accessing Ethereum enabled distributed applications,** in your **browser**.

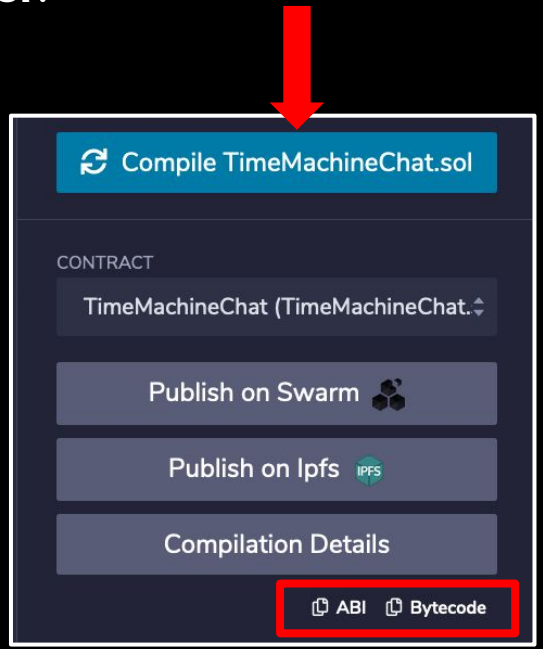




Remix

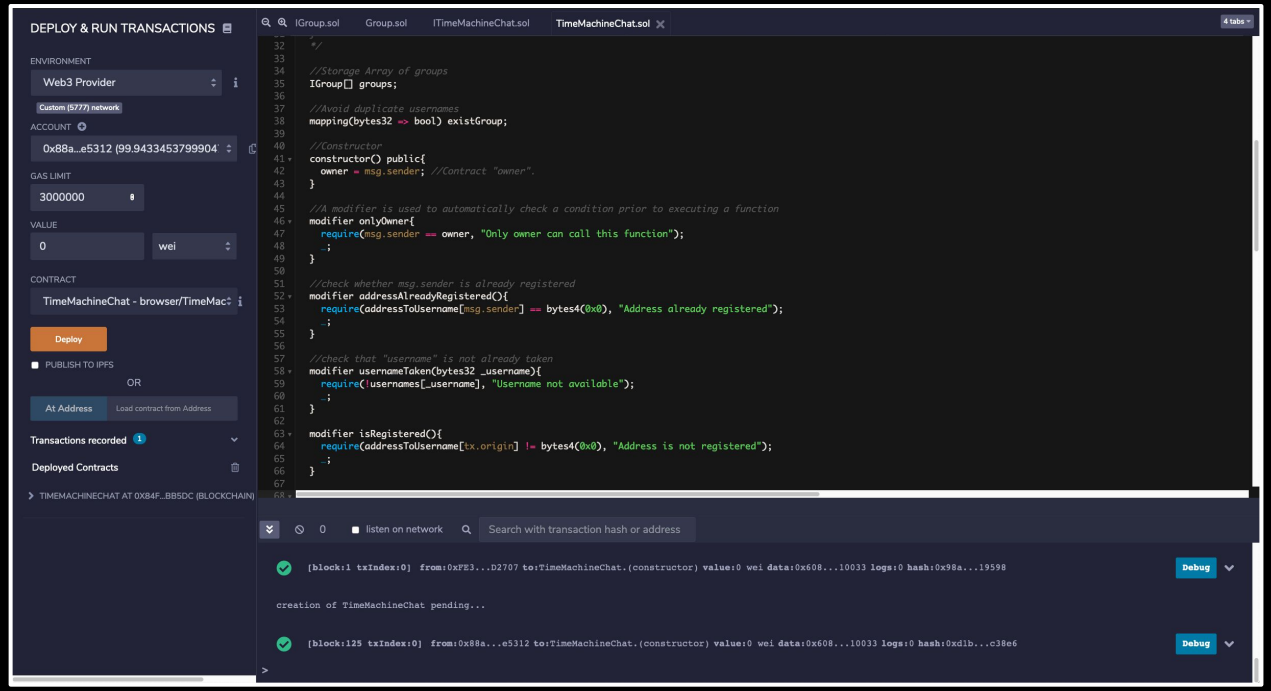
Remix is an **open source tool** that helps you **write Solidity contracts** from the **browser**.





Remix

Remix also supports **testing**, **debugging** and **deploying** of smart contracts.



Configure the frontend

To interact with your contract from the **frontend** you need two informations:

- **The address of your contract**
- **The ABI of your contract**

```
web3.current = new Web3(new Web3.providers.WebsocketProvider('ws://localhost:8545'))
accounts = await web3.current.eth.getAccounts()
contratto = new web3.current.eth.Contract(
            TIME_MACHINE_ABI,
            TIME_MACHINE_ADDRESS
           )
```

```
    },
    ..........
  ]
```

Let’s make some calls

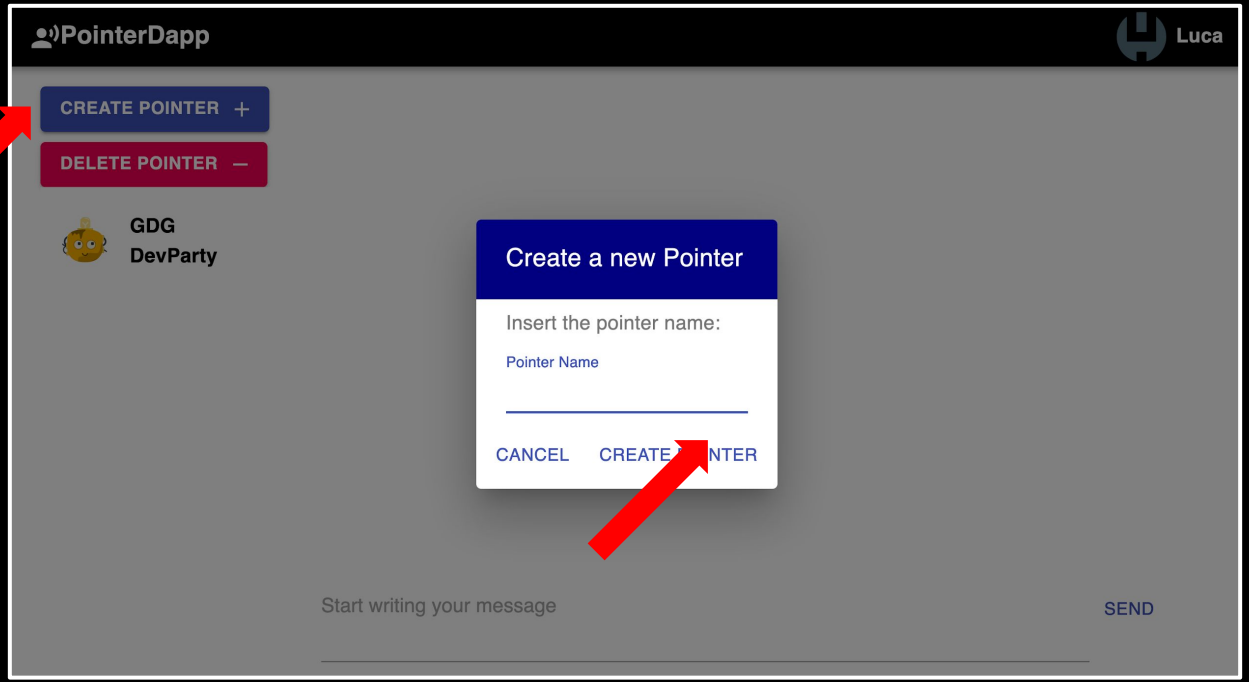
Get Data from the Blockchain

How to invoke a call to the contract?

- We use the function “**call**”
- This is a **free interaction** with the contract

```
contratto.current.methods
                  .getGroups()
                  .call({ from: address })
                  .then((result) => {
                    // Do something
                  });
```

Let’s make some calls



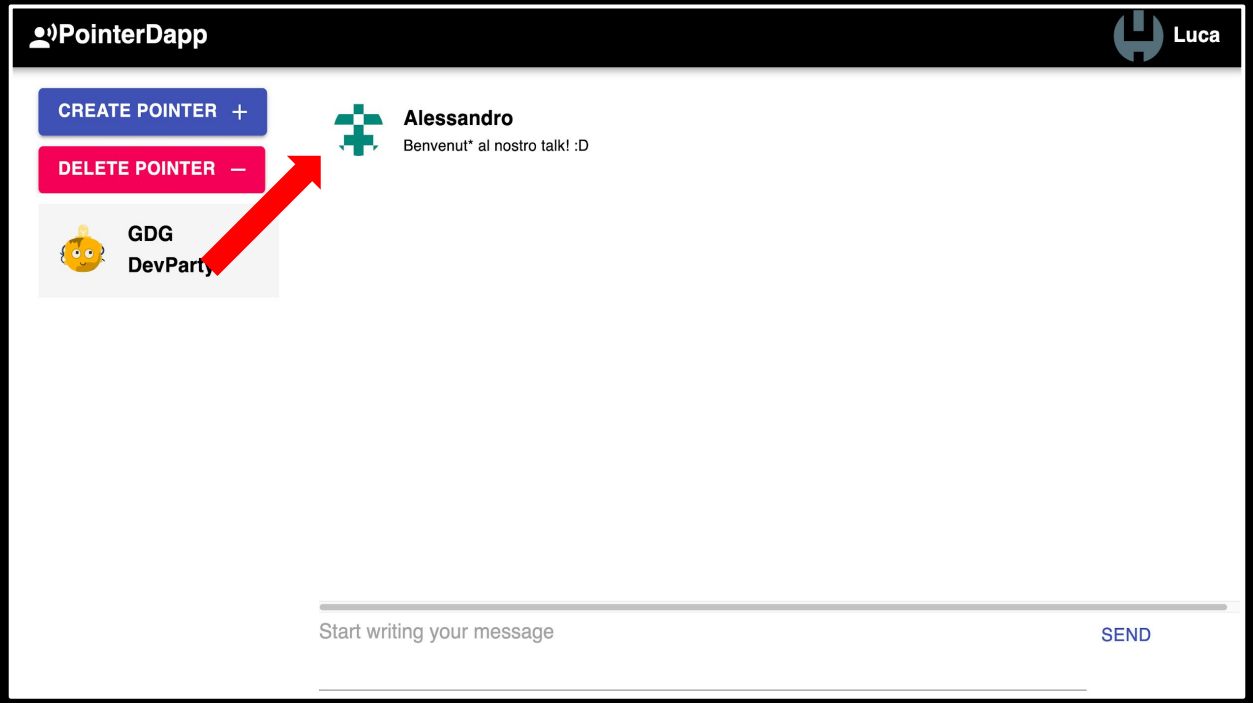
Send data to the Blockchain

How to send a transaction to the contract?

- We use the function “**send**”
- This is a **paid interaction** with the contract.
- We use the function createGroup and we could specify:
  - **Gas**
  - **GasPrice**

```
contratto.current.methods
                .createGroup(web3.current.utils.fromAscii(groupName))
                .send({
                    from: address,
                    gas: 1000000,
                    gasPrice: '1'
                })
                .on("confirmation", (confirmationNumber, receipt) => {
                    // Do something
                })
                .on("error", (error) => {
                    // Do something else
                });
```

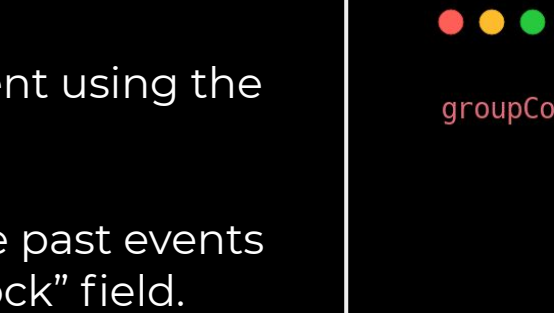
Let’s make some calls



Handle Events

How to listen for events's contract?

- We can listen for an event using the name of the event.
- We can also retrieve the past events specifying the "fromBlock" field.



```
groupContract.events.Message({
                fromBlock: 0
            }, function (error, event) {
                // Do something
            })
```

Pro/Cons

PRO

- Pseudo-anonymity
  - No personal data, only address
- Transparency
- Decentralized
- Tampering-Free
- User owns his data
- Has Legal Value
  - It's more important than you think

CONS

- High Response Time
- Transactions cost
- Scalability issues

Warning

Blockchain is not applicable in any context.
You have to carefully analyze your problem.

Mantra
"If it fits then I use it"

Don't follow the hype.

Thanks!

github.com/PointerPodcast/PointerDapp

PointerDapp.it

Alessandro Berti

Luca Corbucci

Eugenio Paluello

PointerPodcast.it