Hello World

Maxim Gaina

Informatico, Blockchain & dApps,
Startupper

linkedin.com/in/maximgaina
maximgaina@yandex.ru

Blockchain
e principi della
Decentralizzazione

Bitcoin?

Res Gestae Divi Augusti

Roma 25 - 20 a.C.

Contabilità Immobili

Nottingham 1722

“ It’s all about Ledgers. ”

BANCA

risolve
DOUBLE SPENDING

ordina
TRANSAZIONI

registro
CENTRALIZZATO

CENTRALIZZAZIONE

CENTRALIZZAZIONE

DECENTRALIZZAZIONE

Paul Baran.
On Distributed Communications: I. Introduction to Distributed Communications Networks.
August 1964.

CENTRALIZED (A) DECENTRALIZED (B) DISTRIBUTED (C)

CAP Theorem

“ A distributed database has three very desirable properties: partition tolerance, **consistency**, availability. The CAP theorem states: You can have at most two of these properties for any shared-data system. ”

Algoritmo di Consenso

1. costruzione & verifica **transazioni**
2. costruzione **blocco** e Proof of Work
3. **concatenazione** blocco candidato
4. selezione **fork** più lunga

CAP Theorem

“ A distributed database has three very desirable properties: partition tolerance, **consistency**, availability. The CAP theorem states: You can have at most two of these properties for any shared-data system. ”

✔ tolleranza partizioni ✔ disponibilità ✔ **T - consistenza**

Proof of Work

algoritmo di consenso

Blockchain

struttura dati

una
VALUTA DIGITALE
decentralizzata

un
PROTOCOLLO
per ordinare transazioni finanziarie in maniera **decentralizzata**, usando la valuta come **incentivo** per i nodi

Bitcoin è

tipo di

STRUTTURA DATI

pubblica, immutabile, distribuita

tipo di

PROTOCOLLO

definisce il modo in cui opera una rete decentralizzata

Blockchain è

Your Company Name

Source: Coinmetrics, Statista, nacha.org, digitaltransactions.net
mastercard, visa transaction value of 2016 (rest 2017), bitcoin 2018 numbers annualized

Smartcontracts?

ethereum

Registro Distribuito
Algoritmo di Consenso
Rete P2P
TCP/IP
Strato Blockchain
Internet

Logica Decentralizzata
Registro Distribuito
Algoritmo di Consenso
Rete P2P
TCP/IP
Strato Applicativo
Strato Blockchain
Internet

app
app
....
app

dapp
dapp
dapp
dapp

dApp1
Front-End
dApp0
Front-End
web3.js
Back-End
nodejs web3.js
Logica
Decentralizzata

dApp1
Front-End
dApp0
Front-End
web3.js
ipfs.js
Back-End
nodejs web3.js
ipfs.js
Logica
Decentralizzata
Storage
Decentralizzato
swarm
IPFS

dApp1
Front-End
dApp0
Front-End
web3.js
ipfs.js
Back-End
nodejs web3.js
ipfs.js
Storage
Decentralizzato
Logica
Decentralizzata
Messaging
Decentralizzato
swarm
IPFS
whisper
NKN

- porzione di codice che **risiede sulla blockchain**
- interpretabile ed **eseguibile dai nodi**
- la sua esecuzione è

1. **automatica**, ogni volta che tx al suo indirizzo vengono fatte
2. **vincolante**, senza garante e come specificato nel codice
3. **inarrestabile**, anche in condizioni avverse

Smartcontract è

app che istanzia almeno una parte della sua business logic sotto forma di un insieme di smartcontracts che comunicano fra loro

dApp è

Una dApp istanzia la sua business logic su un registro decentralizzato e la esegue secondo il suo protocollo blockchain, permettendo all’utente finale di interagirvi fornendo un front-end. La logica decentralizzata è composta da un insieme di sc in grado di comunicare fra loro

dApp è

TRAGUARDI protocolli BLOCKCHAIN

transazioni **veloci**
commissioni **piccole**

SFIDE ATTUALI

più **scalabilità**
mantenendo
decentralizzazione

richiedente emittente web3.js ethereum

richiedente
emittente
web3.js
ethereum
Request
Perform e_j
Estimate Fee
Simulate
Decide Fee
Deploy $cert(-)$
Propagate tx
View txHash
Send c_i txHash
Wait
x
Consensus
Receipt
No
Yes
Receive
Send $cert(-)$
address to c_i

```
import "./Certificate.sol";

contract Issuer {
    event LogNewCertificate(address certificate);

    address public owner;
    address[] public certificates;

    modifier onlyOwner {
        if (msg.sender != owner)
            revert();
        _;
    }

    ...
    function issueCertificate(uint c_i, string info, uint e_j)
        public onlyOwner returns (address certificate)
    {
        Certificate newCert = new Certificate(c_i, info, e_j);

        LogNewCertificate(newCert);
        certificates.push(newCert);

        return newCert;
    }
}
```

Issuer.sol

index.js

```
1  issuerInstance.methods.issueCertificate(args)
2    .send({ from: account, gas: gasLimit, gasPrice: wei })
3    .once('transactionHash', function(txHash) { ... })
4    .on('confirmation', function(confNumber, receipt) { ... })
5    .on('error', function(error) { this.handleError(tx); })
6    .then(function(receipt) {
7      return receipt.
8          events.LogNewCertificate.returnValues.certificate;
9    });
```

Ethereum - Transactions
1M
500k
0
ETH
Apr 2017
Jul 2017
Oct 2017
Jan 2018

Ethereum - Transactions
1M
500k
0
ETH
Apr 2017
Jul 2017
Oct 2017
Jan 2018

Ethereum - Avg. Transaction Fee
4
3
2
1
0
Apr 2017
Jul 2017
Oct 2017
Jan 2018

Teorema DCS

“ I sistemi decentralizzati, centralizzano all’aumentare di richiesta di transazioni, quando i membri del consenso mantengono localmente lo stato completo del sistema. ”

potenziali utenti
consenso
utenti

Teorema DCS

“ I sistemi decentralizzati, centralizzano all’aumentare di richiesta di transazioni, quando i membri del consenso mantengono localmente lo stato completo del sistema. ”

NEO
smart economy

Proof of Stake

Scalabilità

Internet of Things

WEB ed EVOLUZIONE

web 1.0 read

1991 pagine statiche

social networks,
contenuto
generato da utenti

2004

read & write **web 2.0**

web 3.0

read & write,
decentralize

adesso

contenuto mirato,
web semantico,
internet of things,
responsabilizzazione
dell’utente

futuro

HEALTHCARE
FOOD
TRADING
TELEFONIA
PUBBLICA AMMINISTRAZIONE
CAR SHARING
CLOUD COMPUTING & STORAGE
EDUCAZIONE
...

DECENTRALIZE EVERYTHING