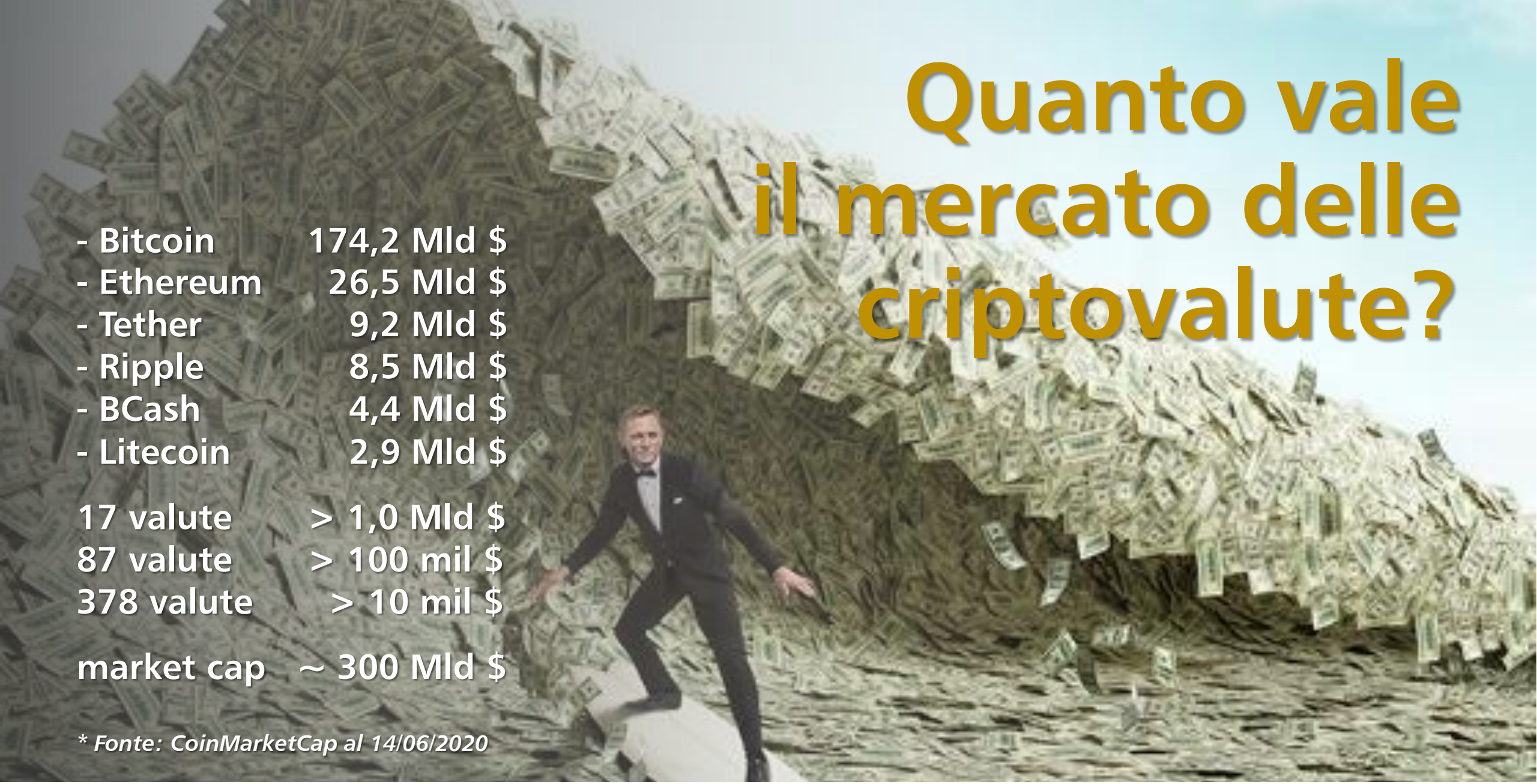
Da Bitcoin alle Blockchain 2.0:
le tecnologie che rivoluzioneranno i servizi finanziari, legali e assicurativi

Quanto vale il mercato delle criptovalute?



- Bitcoin	174,2 Mld $
- Ethereum	26,5 Mld $
- Tether	9,2 Mld $
- Ripple	8,5 Mld $
- BCash	4,4 Mld $
- Litecoin	2,9 Mld $
17 valute	> 1,0 Mld $
87 valute	> 100 mil $
378 valute	> 10 mil $
market cap	~ 300 Mld $

** Fonte: CoinMarketCap al 14/06/2020*

Cosa è una moneta?

- strumento di pagamento (mezzo di scambio nelle transazioni commerciali, es. per la compravendita di beni e servizi)

- unità di conto (misura del valore)

- riserva di valore (fondo di valore)

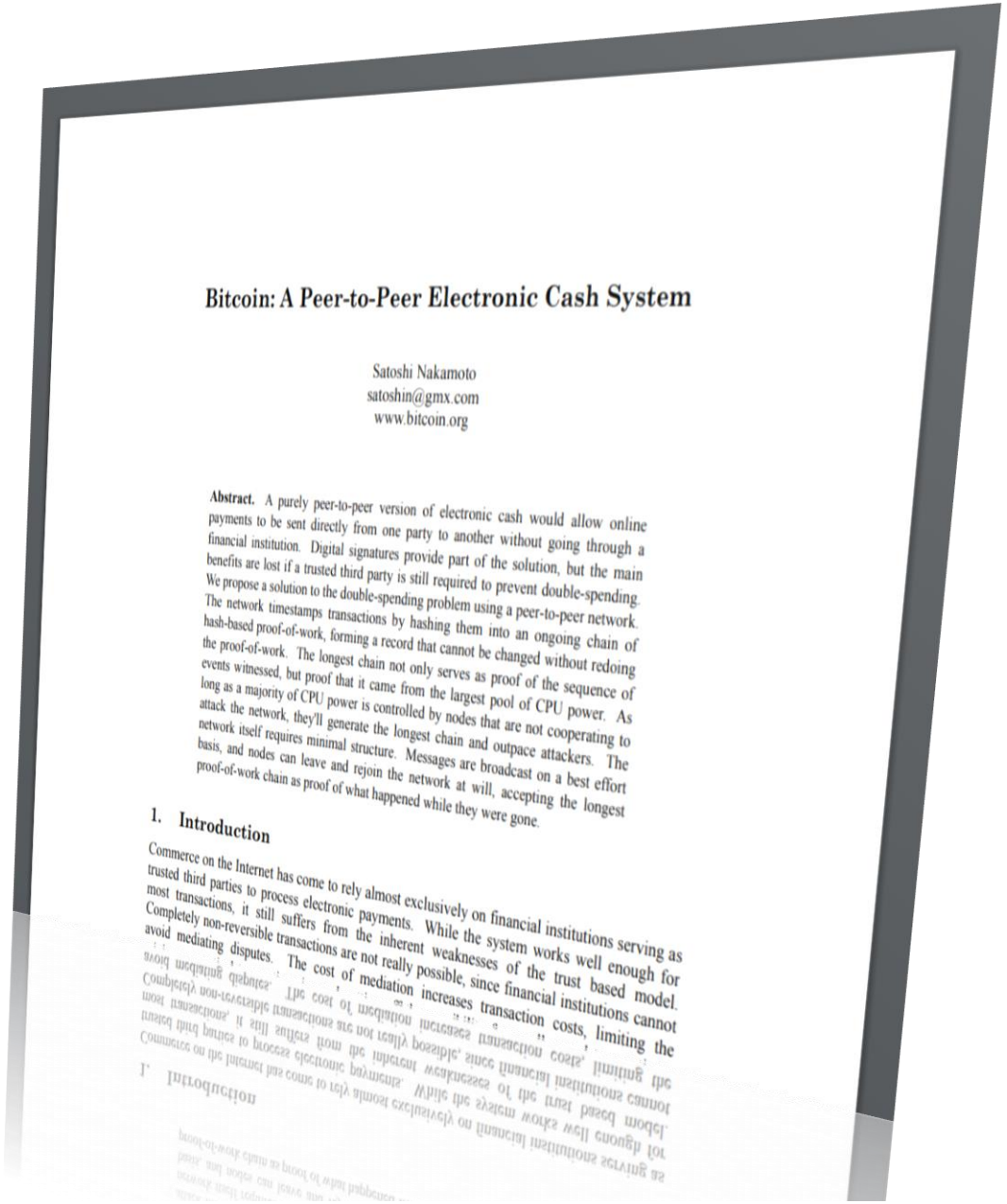
FIDUCIA

Bitcoin e Blockchain

- ottobre 2008
  Pubblicazione Bitcoin

- gennaio 2009
  Rilascio versione 0.1

- Criptovaluta
  + Protocollo
  + Rete P2P



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the

Cosa è una criptovaluta?

È uno strumento per il trasferimento di valore

Crittografia a chiave pubblica/privata

UNA FAVOLA MEDIEVALE

- La Regina mette un messaggio nel suo scrigno
- Chiude tutto col suo lucchetto e manda ad Artù
- Artù aggiunge il suo lucchetto e manda indietro
- La Regina toglie il suo lucchetto e rimanda ad Artù
- Artù apre il suo lucchetto

Crittografia a chiave pubblica/privata

UNA FAVOLA MATEMATICA

Messaggio: 71
Coppia di chiavi di La Regina: 2 | 3
Coppia di chiavi di Artù: 5 | 7

- **La Regina calcola 71 x 2 x 3 = 426 e lo invia**
- **Artù calcola 426 x 7 = 2982 e lo manda indietro**
- **La Regina calcola 2982 / 3 = 994 e lo invia**
- **Artù risolve 994 / 7 = 142 / 2 = 71**

Perché le criptovalute sono rivoluzionarie?

Perché sono un asset digitale non duplicabile

Perché una criptovaluta non è duplicabile? Perché viene iscritta in un Ledger

Ledger e Blockchain

- Nel caso base il Ledger contiene un bilancio ossia una lista di coppie Indirizzo / Ammontare e le transazioni avvenute fra Indirizzi

- Il Ledger è archiviato in una Blockchain ossia una catena di blocchi di dati composti da:
  - un content (gli ultimi aggiornamenti al Ledger)
  - un header (i metadati e l'hash del blocco precedente a cui è indissolubilmente legato)

Funzioni HASH

- Output a lunghezza fissa
  per Bitcoin si usa SHA-256 con output di 2^{256} bit
- Facile da calcolare
- Resistente alle collisioni
- Irreversibile (a differenza della crittografia)
  se y = H(x) allora non esiste H^{-1} tale che $H^{-1}(y)=x$

ESEMPIO

H("Gatto") = "Go" H("Cane") = "Ce"

Perché il Ledger non è falsificabile?

Perché è condiviso sulla Blockchain e ogni aggiunta (fork) è convalidata tramite Consensus

PoW (proof-of-work)

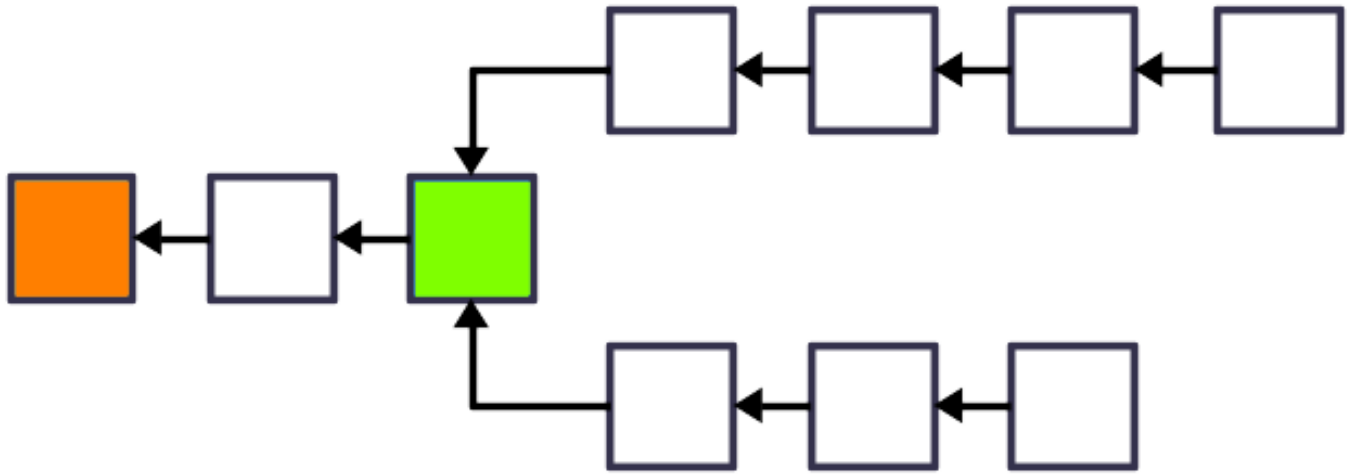
- Nel caso base la validità di un blocco è data da $H(B_x, H(B_{x-1}), rnd) > diff$

- Il calcolo viene effettuato dai Miner
  diff dipende dal numero di miner attivi
  0000000000007fb7db930261856af693cd7e2f1

- Il primo Miner che trova la soluzione distribuisce il nuovo blocco, tutti gli altri Nodi verificano

Fork, Soft Fork, Hard Fork

- Soft Fork: nuove regole più restrittive "retro-compatibile", non invalida i nuovi blocchi
- Hard Fork: nuove regole meno restrittive necessita consenso sulla validazione



Nuove regole

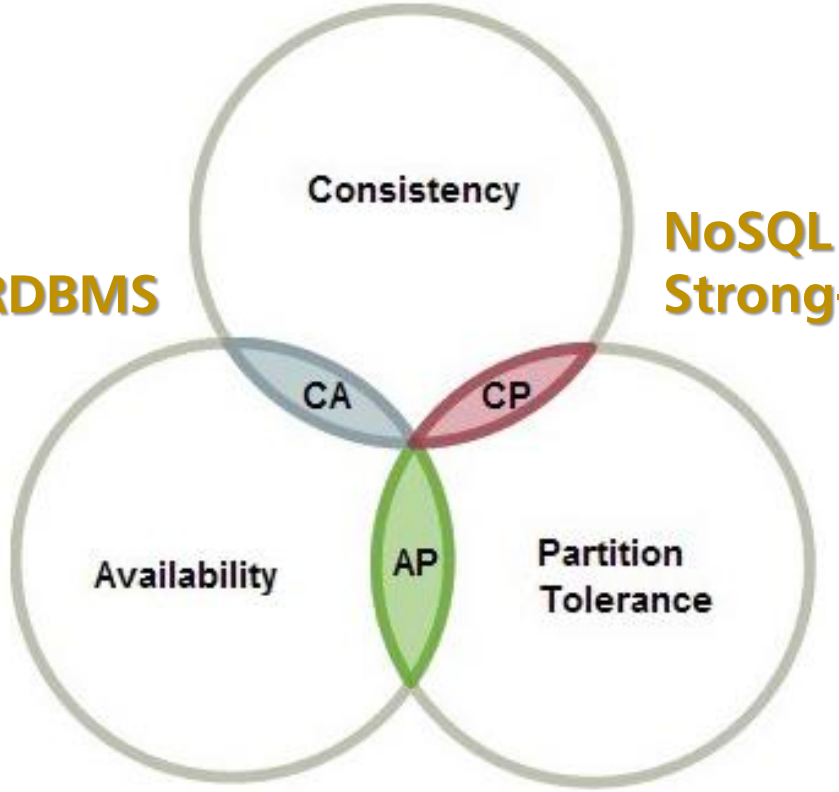
Vecchie regole

Teorema CAP

È impossibile per un sistema informatico distribuito fornire simultaneamente le tre seguenti garanzie:

- **Coerenza [consistency] (tutti i nodi vedono gli stessi dati nello stesso momento)**
- **Disponibilità [availability] (ogni richiesta riceve una risposta su ciò che è riuscito o fallito)**
- **Tolleranza alla partizione [partition tolerance] (il sistema continua a funzionare nonostante arbitrarie perdite di messaggi o malfunzionamenti)**

Teorema CAP



RDBMS

NoSQL (es. biglietteria online)
Strong-Consensus Blockchain

NoSQL (es. social network)
Weak-Consensus Blockchain

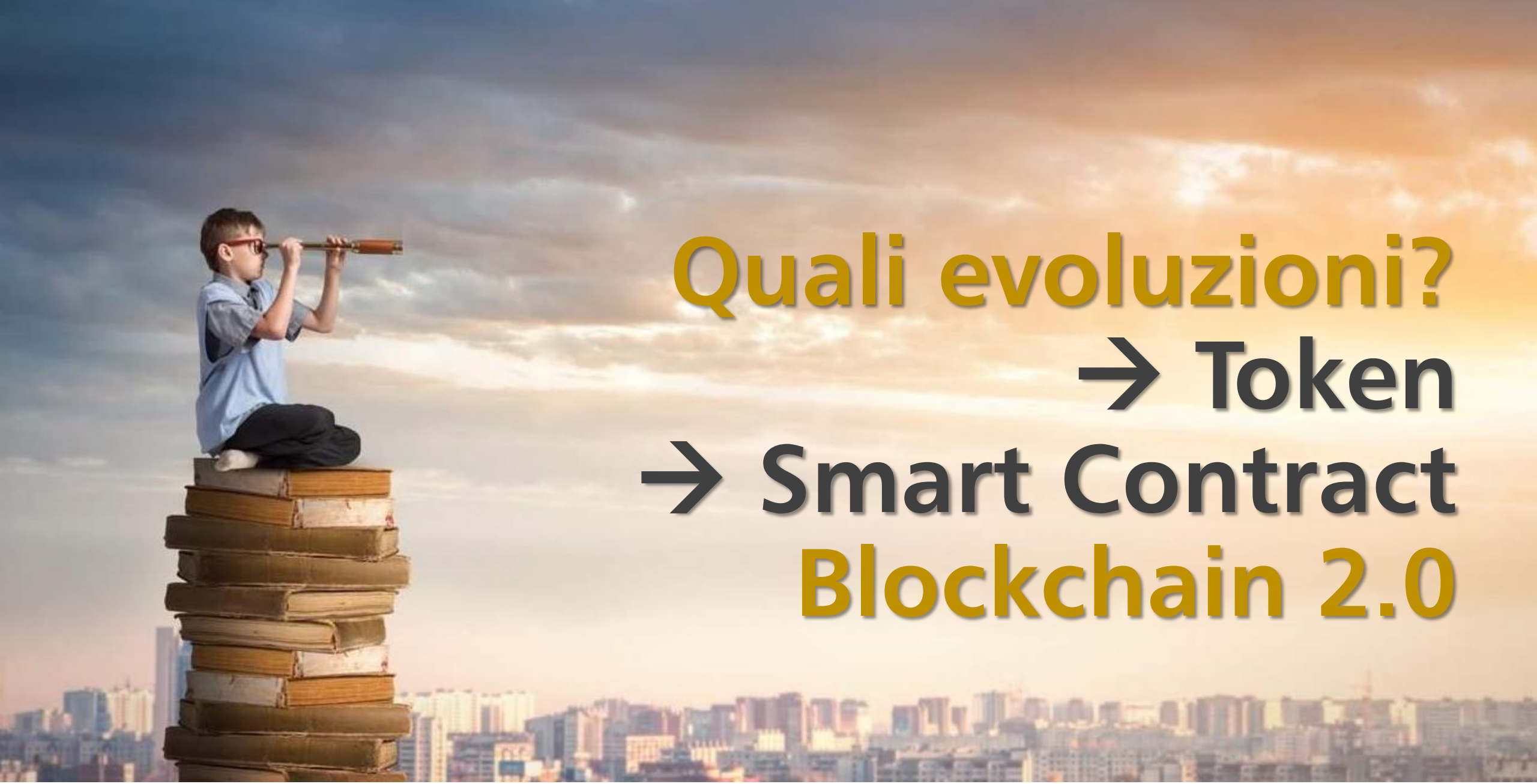
Un sistema distribuito è in grado di soddisfare al massimo due di queste garanzie allo stesso tempo, ma non tutte e tre.

PoS (proof-of-stake)

La probabilità che un miner aggiunga un nuovo blocco è dipendente da un parametro diverso dalla potenza di calcolo (es. da quantità di coin)

Strategie e tecniche alternative

- acyclic graphs
- oracoli
- zero-knowledge proof


Quali evoluzioni?
→ Token
→ Smart Contract
Blockchain 2.0

Cosa è un token?

Coin (criptomoneta)
- non nativo
- con funzionalità avanzate

Esiste uno standard?

ERC20 e ERC223 ad oggi riconosciuti dagli Exchange

Quali funzionalità avanzate?

Per usi monetari più complessi dello scambio (dal contante al bonifico)

Quali funzionalità avanzate?

Per usi non monetari (ticket, votazioni, ecc…)

Blockchain 2.0

- Lightning Network (secondo layer di Bitcoin, scalabile e programmabile)

- Hyperledger (permissioned, programmabile)

- Ethereum (pubblica, Turing equivalente)

- Algorand (pubblica, Pure Proof-of-Stake)

La soluzione Ethereum: Solidity

Un linguaggio di programmazione Turing-completo

www.ethereum.org

MINIMUM VIABLE TOKEN

The standard token contract can be quite complex. But in essence a very basic token boils down to this:

```
pragma solidity >=0.4.22 <0.6.0;

contract MyToken {
    /* This creates an array with all balances */
    mapping (address => uint256) public balanceOf;

    /* Initializes contract with initial supply tokens to the creator of the contract */
    constructor(
        uint256 initialSupply
        ) public {
        balanceOf[msg.sender] = initialSupply;              // Give the creator all initial tokens
    }

    /* Send coins */
    function transfer(address _to, uint256 _value) public returns (bool success) {
        require(balanceOf[msg.sender] >= _value);           // Check if the sender has enough
```

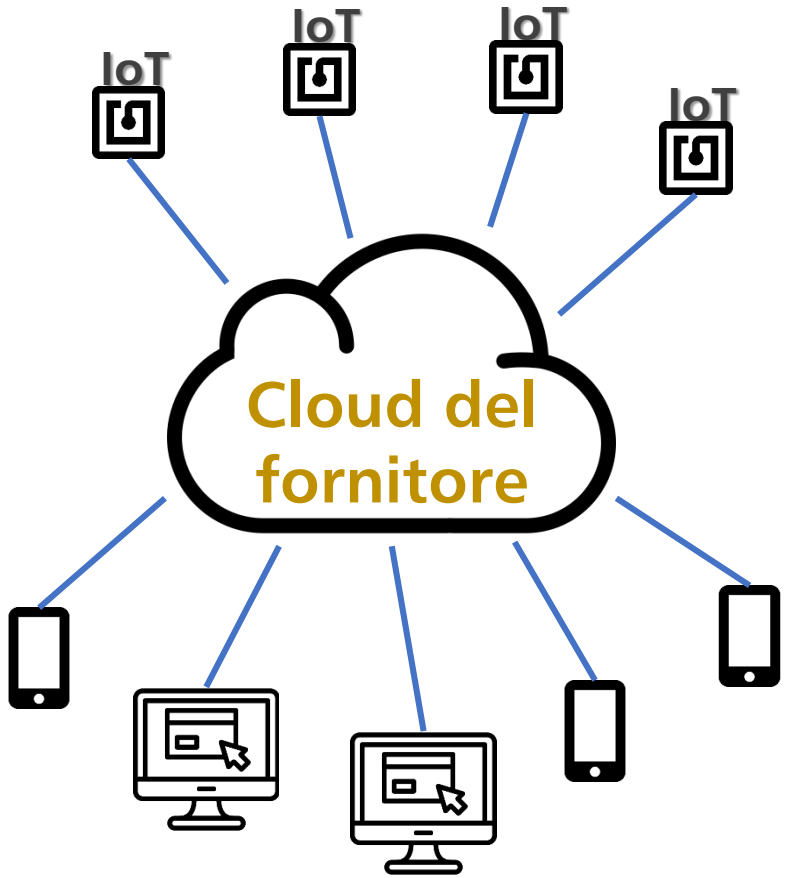
Chi esegue e verifica gli Smart Contract?

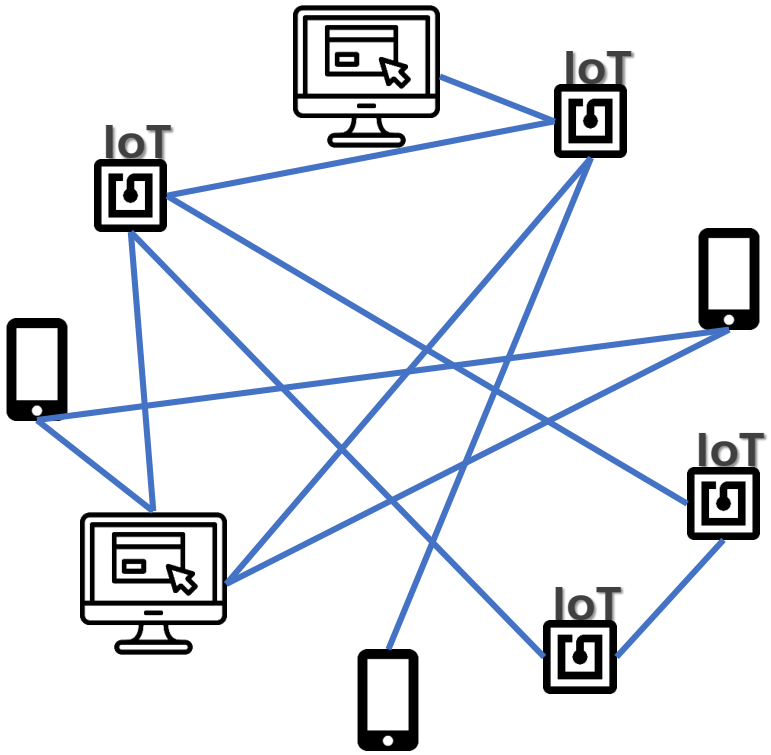
Gli Smart Contract sulla blockchain esistono solo come istanze eseguite dai nodi (miner)

All'atto pratico, una DLT per cosa può essere utile?

Nei problemi di fiducia, ma è una soluzione costosa

Dal Cloud agli Untrusted Services





Timestamping e Notarizzazione

Per un documento è possibile ottenere:

- Confidenzialità e Non Ripudio (chiave pubblica/privata)

- Integrità (funzioni hash)

- Disponibilità e Data Certa (archiviazione su blockchain)

Comunità fra pari (Community P2P)

In una comunità i rapporti fra i membri sono organizzati tramite il rispetto di regole, siano esse formali o informali.

- C'è un intermediario o un arbitro?

- Può essere sostituito da un processo automatico?

Sistemi di tracking e/o di voto (?)

Blockchain consente di archiviare in modalità disintermediata e in modo non modificabile dei dati

- Quale modalità di verifica dei dati prima della scrittura?

- I dati possono essere pubblici?

Francesco La Regina

francesco@studiolaregina.com