



ALGOCAPITAL.IT



ING.EMANUELE.COLACCHI@GMAIL.COM

- Attualmente sono un Trader Istituzionale attivo sui mercati delle commodities.
- Laureato in Ingegneria Gestionale presso la Sapienza Università di Roma.
- Presidente della Commissione Ingegneria Gestionale presso l'Ordine degli Ingegneri della Provincia di Roma.
- Ho maturato una specializzazione in strumenti derivati su indici azionari ed obbligazionari in ottica di medio-lungo periodo.
- Prediligo il trading algoritmico, basato sia su metodi tradizionali che innovativi.
- Docente per FinecoBank SpA, una delle principali banche dirette in Europa
- Coautore del libro «*Python per il Trading*» il primo libro in Italia sul trading algoritmico, pubblicato su Amazon.
- Dal 2012 seguo valute digitali e blockchain e sono coautore del libro «*Bitcoin Revolution*», edito da Hoepli.



Indice della **Lezione**

FONDAMENTALI

1. La nascita del Bitcoin
2. Cos'è il Bitcoin?
3. Il protocollo Bitcoin
4. Cos'è la Blockchain?
5. Cos'è un Blocco?
6. Transazioni





Indice della **Lezione**

FONDAMENTALI

1. La nascita del Bitcoin

2. Cos'è il Bitcoin?
3. Il protocollo Bitcoin
4. Cos'è la Blockchain?
5. Cos'è un Blocco?
6. Transazioni





Satoshi **Nakamoto**



Chi è Satoshi Nakamoto (中本哲史)?



Nascita del **Bitcoin**

Cronistoria

- 18 Agosto 2008: viene registrato il dominio www.bitcoin.org, sembra che sia stato registrato da Satoshi Nakamoto attraverso il sito www.anonymousspeech.com che permette registrazioni anonime di domini internet.
- 31 Ottobre 2008: viene pubblicato il “Bitcoin design paper”.
- 9 Novembre 2008: il progetto “Bitcoin” viene registrato sul sito www.sourceforge.net che fornisce gli strumenti per sviluppare software in modo collaborativo.
- 3 Gennaio 2009: nasce il “Genesis Block” alle 18:15:05 GMT.



Dow Jones





Indice della **Lezione**

FONDAMENTALI

1. La nascita del Bitcoin
- 2. Cos'è il Bitcoin?**
3. Il protocollo Bitcoin
4. Cos'è la Blockchain?
5. Cos'è un Blocco?
6. Transazioni





Bitcoin Design **Paper**

Abstract

“Una versione puramente peer-to-peer di denaro elettronico consentirebbe ai pagamenti online di essere inviati da una persona all'altra senza passare attraverso un'istituzione finanziaria. Le firme digitali forniscono parte della soluzione, ma i principali benefici si perdono se, per impedire la doppia spesa (double-spending), è ancora necessario un terzo soggetto di fiducia. Noi proponiamo una soluzione al problema della doppia spesa usando un network peer-to-peer. Il network marca in maniera temporale le transazioni attraverso un codice Hash e le posiziona in una catena continua di prove di lavoro (proof-of-work) basate su funzioni Hash, formando un registro che non può essere modificato senza rifare la prova di lavoro stessa. La catena più lunga serve non soltanto come prova della sequenza di eventi di cui è testimone, ma anche come prova che proviene dal più grande pool di potenza CPU. Fintanto che la maggioranza della potenza CPU è controllata dai nodi che non cooperano ad attaccare il network, questi genereranno la catena più lunga e distanzieranno eventuali aggressori. Lo stesso network richiede una struttura minima. I messaggi vengono trasmessi nel miglior modo possibile ed i nodi possono sganciarsi e ricollegarsi al network a propria volontà, accettando la catena di lavoro più lunga come prova di quanto successo, mentre erano assenti.”



Bitcoin Design **Paper**

Abstract

“Una versione puramente peer-to-peer di denaro elettronico consentirebbe ai pagamenti online di essere inviati da una persona all'altra senza passare attraverso un'istituzione finanziaria. Le firme digitali forniscono parte della soluzione, ma i principali benefici si perdono se, per impedire la doppia spesa (double-spending), è ancora necessario un terzo soggetto di fiducia. Noi proponiamo una soluzione al problema della doppia spesa usando un network peer-to-peer. Il network marca in maniera temporale le transazioni attraverso un codice Hash e le posiziona in una catena continua di prove di lavoro (proof-of-work) basate su funzioni Hash, formando un registro che non può essere modificato senza rifare la prova di lavoro stessa. La catena più lunga serve non soltanto come prova della sequenza di eventi di cui è testimone, ma anche come prova che proviene dal più grande pool di potenza CPU. Fintanto che la maggioranza della potenza CPU è controllata dai nodi che non cooperano ad attaccare il network, questi genereranno la catena più lunga e distanzieranno eventuali aggressori. Lo stesso network richiede una struttura minima. I messaggi vengono trasmessi nel miglior modo possibile ed i nodi possono sganciarsi e ricollegarsi al network a propria volontà, accettando la catena di lavoro più lunga come prova di quanto successo, mentre erano assenti.”



Bitcoin Design **Paper**

Abstract

*“Una versione puramente peer-to-peer di denaro elettronico consentirebbe ai pagamenti online di essere inviati da una persona all'altra senza passare attraverso un'istituzione finanziaria. Le firme digitali forniscono parte della soluzione, ma i principali benefici si perdono se, per impedire la doppia spesa (double-spending), è ancora necessario un terzo soggetto di fiducia. Noi proponiamo una soluzione al problema della doppia spesa usando un network peer-to-peer. **Il network marca in maniera temporale le transazioni attraverso un codice Hash e le posiziona in una catena continua di prove di lavoro (proof-of-work) basate su funzioni Hash, formando un registro che non può essere modificato senza rifare la prova di lavoro stessa.** La catena più lunga serve non soltanto come prova della sequenza di eventi di cui è testimone, ma anche come prova che proviene dal più grande pool di potenza CPU. Fintanto che la maggioranza della potenza CPU è controllata dai nodi che non cooperano ad attaccare il network, questi genereranno la catena più lunga e distanzieranno eventuali aggressori. Lo stesso network richiede una struttura minima. I messaggi vengono trasmessi nel miglior modo possibile ed i nodi possono sganciarsi e ricollegarsi al network a propria volontà, accettando la catena di lavoro più lunga come prova di quanto successo, mentre erano assenti.”*



Bitcoin Design **Paper**

Abstract

*“Una versione puramente peer-to-peer di denaro elettronico consentirebbe ai pagamenti online di essere inviati da una persona all'altra senza passare attraverso un'istituzione finanziaria. Le firme digitali forniscono parte della soluzione, ma i principali benefici si perdono se, per impedire la doppia spesa (double-spending), è ancora necessario un terzo soggetto di fiducia. Noi proponiamo una soluzione al problema della doppia spesa usando un network peer-to-peer. Il network marca in maniera temporale le transazioni attraverso un codice Hash e le posiziona in una catena continua di prove di lavoro (proof-of-work) basate su funzioni Hash, formando un registro che non può essere modificato senza rifare la prova di lavoro stessa. La catena più lunga serve non soltanto come prova della sequenza di eventi di cui è testimone, ma anche come prova che proviene dal più grande pool di potenza CPU. Fintanto che la maggioranza della potenza CPU è controllata dai nodi che non cooperano ad attaccare il network, questi genereranno la catena più lunga e distanzieranno eventuali aggressori. **Lo stesso network richiede una struttura minima. I messaggi vengono trasmessi nel miglior modo possibile ed i nodi possono sganciarsi e ricollegarsi al network a propria volontà, accettando la catena di lavoro più lunga come prova di quanto successo, mentre erano assenti.**”*



Cos'è il **Bitcoin**?

Bitcoin è un sistema di pagamento peer-to-peer ed una moneta digitale, sviluppata nel 2009 come software open source. Si tratta di una crypto valuta, poiché utilizza la crittografia per controllare la creazione e il trasferimento della moneta.

Wikipedia

**SISTEMA DI PAGAMENTO
P2P**

**MONETA
DIGITALE**

**CRYPTO
VALUTA**

CREATO E TRASFERITO



Cos'è il **Bitcoin**?





Indice della **Lezione**

FONDAMENTALI

1. La nascita del Bitcoin
2. Cos'è il Bitcoin?
- 3. Il protocollo Bitcoin**
4. Cos'è la Blockchain?
5. Cos'è un Blocco?
6. Transazioni





3 in **1**

La parola Bitcoin raccoglie 3 cose in 1:



1. PROTOCOLLO



2. OPEN SOURCE



3. NETWORK



Protocollo **Bitcoin**

Bitcoin è un protocollo ovvero un insieme di regole che servono a definire il funzionamento del software utilizzato da un network di computer collegati tra loro, con lo scopo di creare e gestire la valuta Bitcoin.





Open **Source**

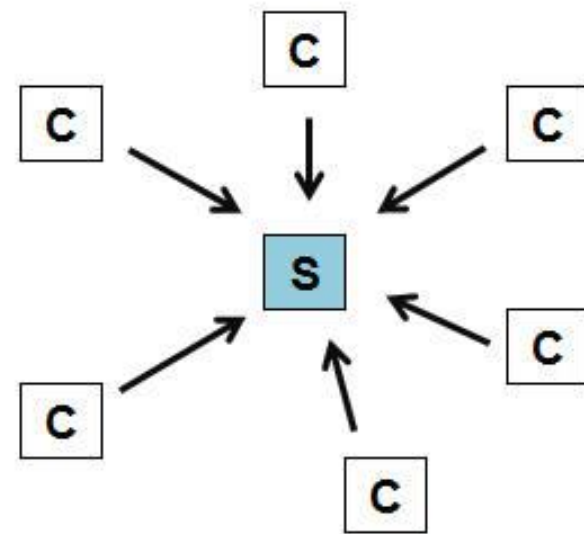
Il protocollo e il software Bitcoin sono di tipo open source e qualsiasi sviluppatore può revisionare il codice o creare la propria versione modificata del software Bitcoin.

- Gli sviluppatori non possono forzare un cambiamento nel protocollo Bitcoin, perché tutti gli utenti sono liberi di scegliere quale software e versione usare.
- Per restare compatibili con gli altri, tutti gli utenti devono però usare software conformi alle stesse regole. Bitcoin funziona solo con un consenso completo tra tutti gli utenti.



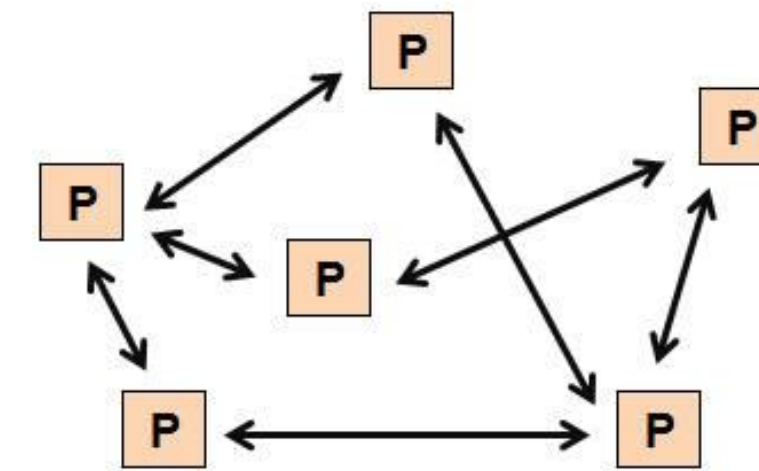
Bitcoin **Network**

La rete Bitcoin si compone di computer collegati tra loro, secondo un'architettura peer to peer (P2P).



CLIENT/SERVER

Architettura centralizzata

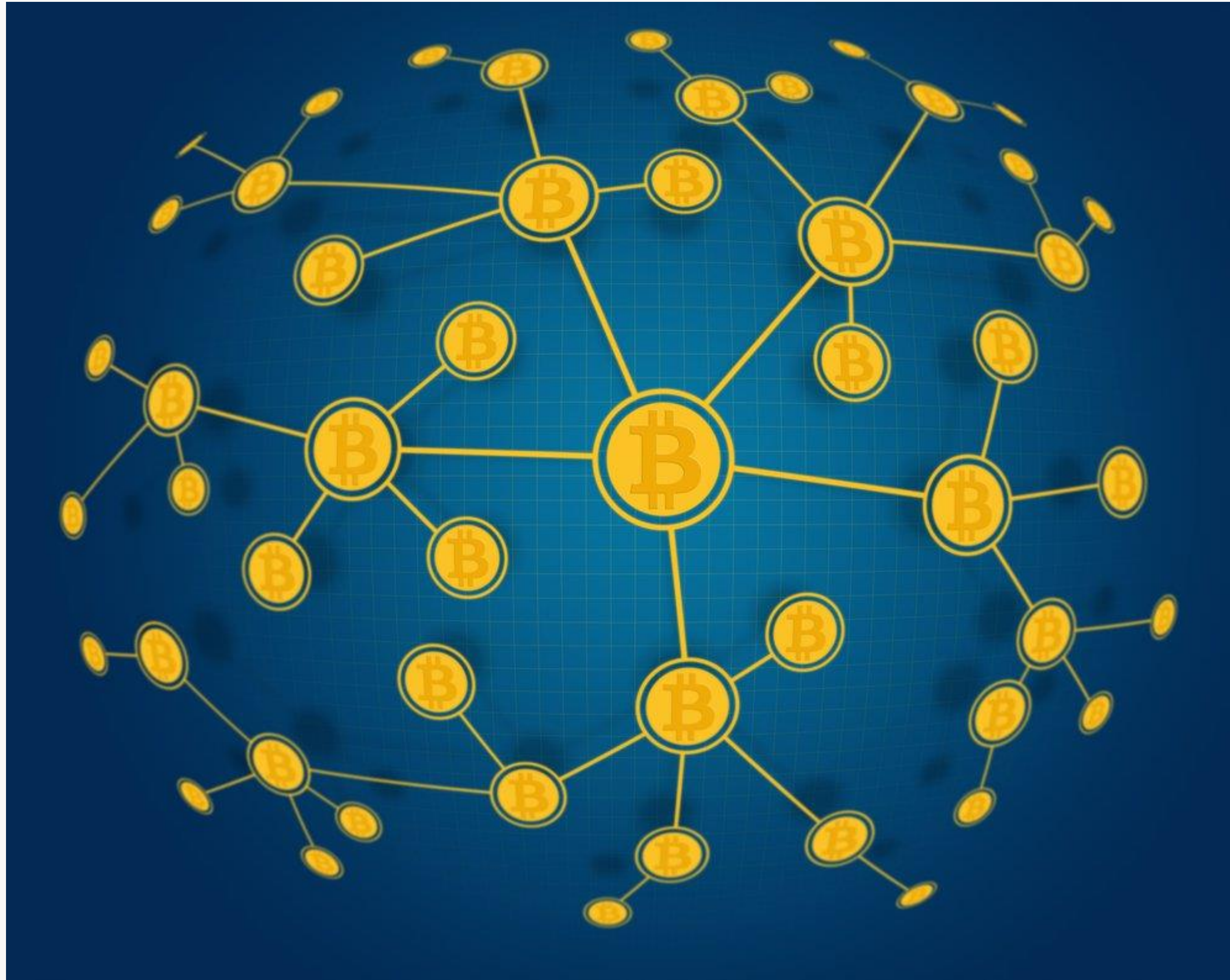


PEER TO PEER (P2P)

Architettura decentralizzata



Bitcoin **Network**



NODI

Ogni nodo è in grado di comunicare direttamente con gli altri nodi senza dover passare da un server centrale



Bitcoin Nodes

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Wed Jun 07 2017
22:25:57 GMT+0200 (CEST).

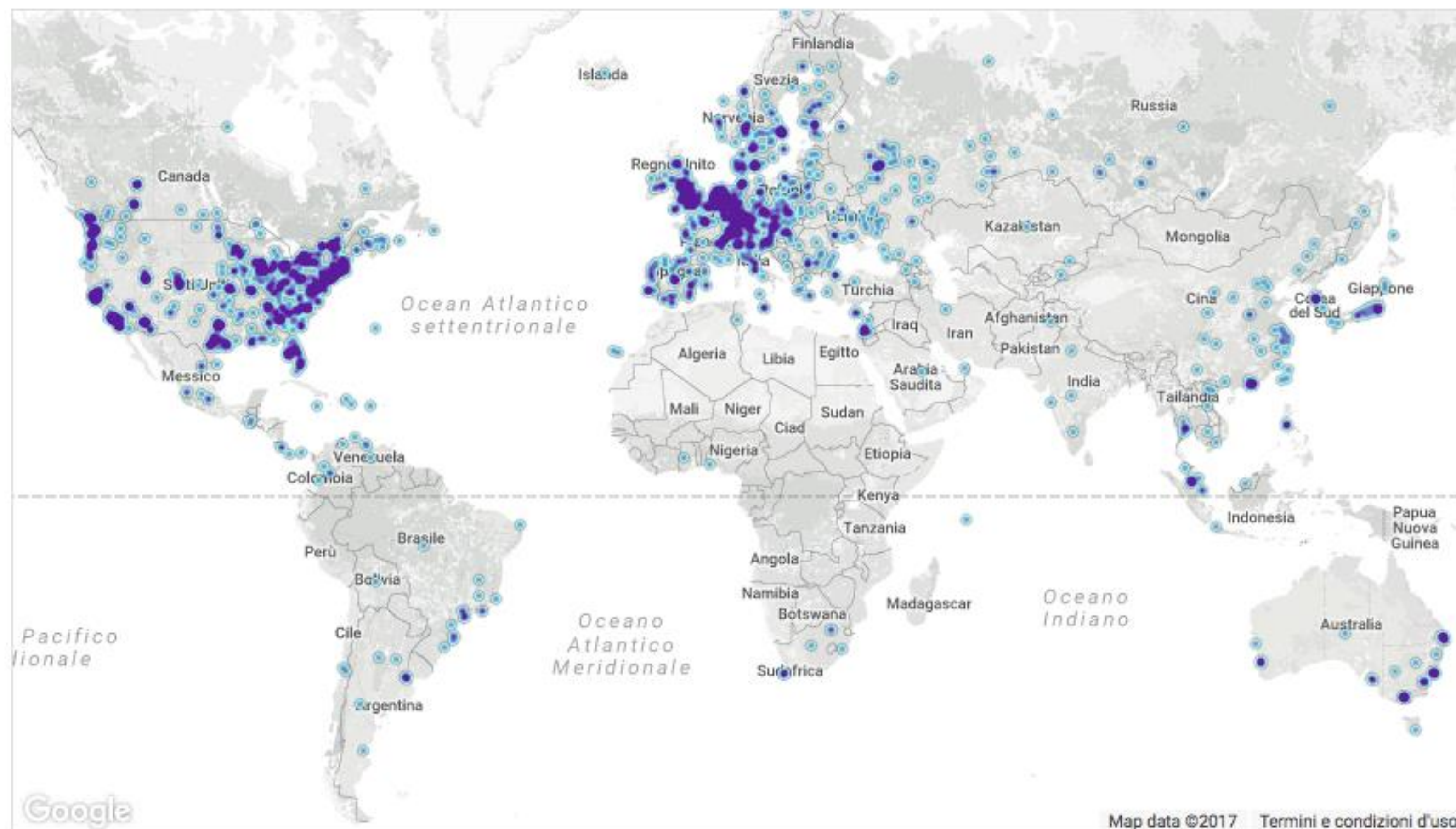
10365 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2935 (28.32%)
2	Germany	1454 (14.03%)
3	United Kingdom	548 (5.29%)
4	France	538 (5.19%)
5	Canada	534 (5.15%)
6	Netherlands	427 (4.12%)
7	Singapore	359 (3.46%)
8	Japan	334 (3.22%)
9	Korea, Republic of	302 (2.91%)
10	Australia	286 (2.76%)

More (93) »



www.bitnodes.21.co



Cos'è la **Crittografia**?

La crittografia è un insieme di tecniche che consentono di trasmettere un messaggio mantenendolo segreto a tutti, tranne alle persone che possiedono le chiavi per decifrarlo.

KRYPTÒS

+

GRAPHIA

Nascosto

Scrittura

OBIETTIVO: NASCONDERE IL CONTENUTO DI UN MESSAGGIO



Cifratura **Simmetrica**

Cifrario di Cesare

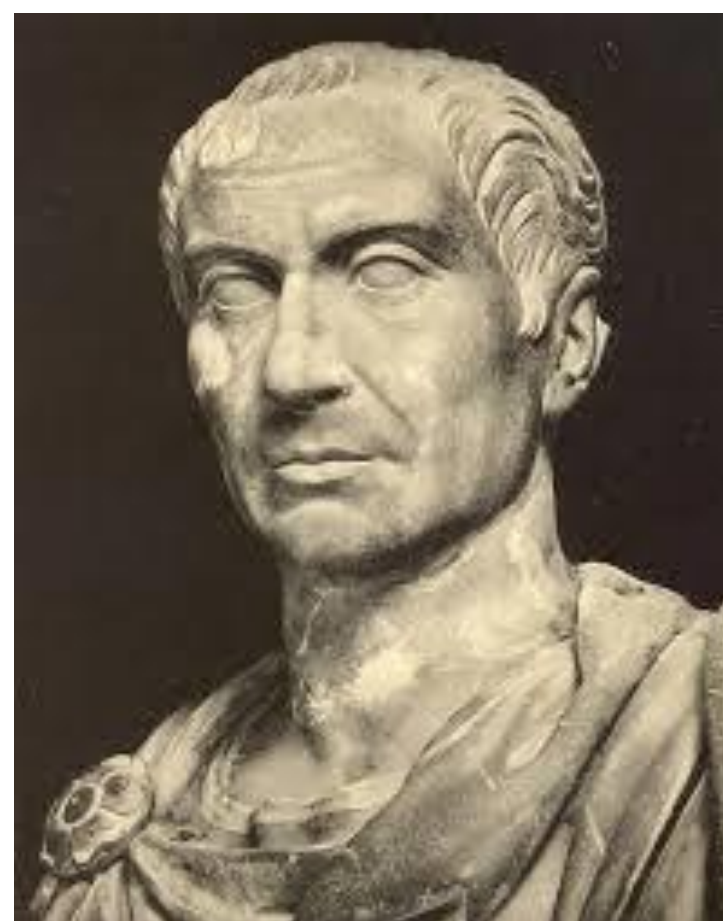
- È un metodo semplice e facilmente scardinabile.
- Tuttavia contiene già i due elementi caratteristici di un codice di cifratura:

ALGORITMO	CHIAVE
È la regola con cui si modifica il messaggio originale, rendendolo criptato (o cifrato)	È il parametro che permette di decodificare (o decifrare) il messaggio

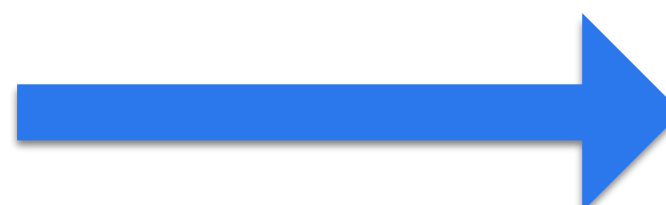
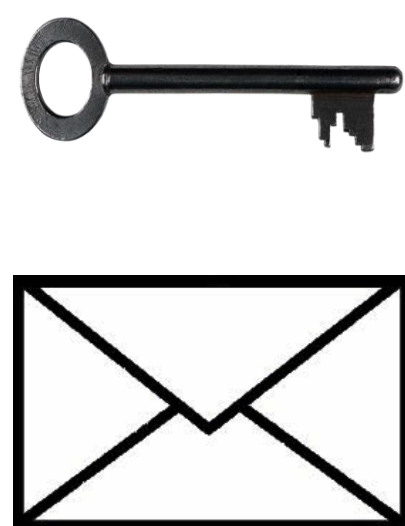
- È un metodo di cifratura simmetrica, in cui la chiave per codificare e decodificare il messaggio è la stessa.



Cifratura **Simmetrica**



Giulio Cesare



Tito Labieno



Evoluzione della **Crittografia**

La vera evoluzione della crittografia si è però avuta solo nel XX secolo, sulla scia dell'arrivo di nuovi mezzi di trasmissione dell'informazione e della sempre più pressante richiesta di sistemi di sicurezza per lo scambio di informazioni.

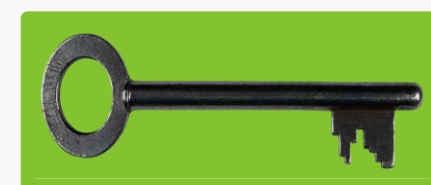
La novità si è avuta con l'introduzione di due chiavi:

CHIAVE PUBBLICA
(O CHIAVE DI CIFRATURA)



È nota a tutti coloro che vogliono inviare un messaggio cifrato

CHIAVE PRIVATA
(O CHIAVE DI DECIFRATURA)



È nota solo al destinatario ed è indispensabile per decifrare il messaggio ricevuto



Cifratura **Asimmetrica**

- In questo modo è facile passare dal testo in chiaro a quello cifrato, ma non si è in grado di passare dal testo cifrato a quello in chiaro.
- Decade così una delle principali caratteristiche dei tradizionali sistemi di cifratura, la simmetria.
- Cifrare e decifrare non sono più la stessa cosa.

CIFRATURA
SIMMETRICA



CIFRATURA
ASIMMETRICA





Funzione **Hash**

La funzione Hash è una funzione che trasforma un messaggio di lunghezza arbitraria in un codice alfanumerico di lunghezza prefissata, che prende il nome di Hash, Digest o impronta del messaggio.

Se ipotizziamo che:

- Σ è un alfabeto.
- Σ^* è l'insieme delle stringhe di qualsiasi lunghezza, composte dai simboli dell'alfabeto.
- Σ^n è l'insieme delle stringhe di lunghezza n .

Allora h è detta funzione Hash se:

- $h: \Sigma^* \rightarrow \Sigma^n$
- $x \rightarrow h(x)$



Funzione **Hash**

Proprietà

- Semplicità: deve essere agevole calcolare il codice Hash da qualunque tipo di messaggio di qualunque dimensione.
- Univocità: deve essere praticamente nulla la probabilità che due messaggi generino lo stesso codice Hash.
- Non invertibilità: deve essere praticamente impossibile poter risalire dal codice Hash al messaggio.
- “Effetto valanga”: la minima modifica del messaggio deve generare un’alterazione radicale dell’Hash.

L’Hash è una specie d’impronta digitale, che identifica in modo univoco ed irreversibile un certo messaggio, conferendogli integrità e autenticità.



Funzione **Hash**



MESSAGGIO

Il messaggio può essere di lunghezza arbitraria



FUNZIONE HASH

La funzione Hash comprime il messaggio



HASH

Si ottiene un codice alfanumerico di lunghezza prefissata



Funzione **Hash**

Esempio di Hash

compra cento bitcoin → 5335C303E0981E00317EC53582DE99D9495DF45CF7F2916D0E6931EEE666849A

Effetto valanga

Compra cento bitcoin → 9B5CA3809B136416B0EB94AB18A1B148344C026B50C151797477974877936629

compra cento **B**itcoin → 4CCFEF1B5D1864B219BB233F518724DAF07E571C3DF5C5C7C118F04572BF072E

compr**o** cento bitcoin → AE6DBD264B706DDCF3E98052E65C417DB080DDA18D2457EDE55409CE88D1BE37



- www.hashemall.com

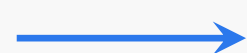


Funzione **Hash**

Tipologie

Le funzioni Hash più utilizzate sono:

- MD4 (Message Digest 4)
- MD5 (Message Digest 5)
- SHA (Secure Hash Algorithm)



L'algoritmo SHA è stato sviluppato dalla NSA (National Security Agency) e le specifiche sono state pubblicate dal NIST (National Institute of Standards and Technology) nel 1993. Questa versione è nota come SHA-0.

- Nel 1995 è stata pubblicata una nuova versione, nota come SHA-1.
- Nel 2001 sono state pubblicate quattro funzioni: SHA-224, SHA-256, SHA-384 e SHA-512. Queste funzioni sono spesso indicate come SHA-2.
- Nel sistema Bitcoin viene utilizzato l'algoritmo SHA-256 che è in grado di processare messaggi con dimensione inferiore a 264 bit, in blocchi da 512 bit, ognuno formato da 16 parole da 32 bit. Questo algoritmo restituisce un hash a 256 bit.



Firma **Digitale**

La firma digitale è uno schema matematico per dimostrare l'autenticità di un messaggio o di un documento digitale inviato attraverso un canale non sicuro.

CRITTOGRAFIA + FUNZIONE HASH

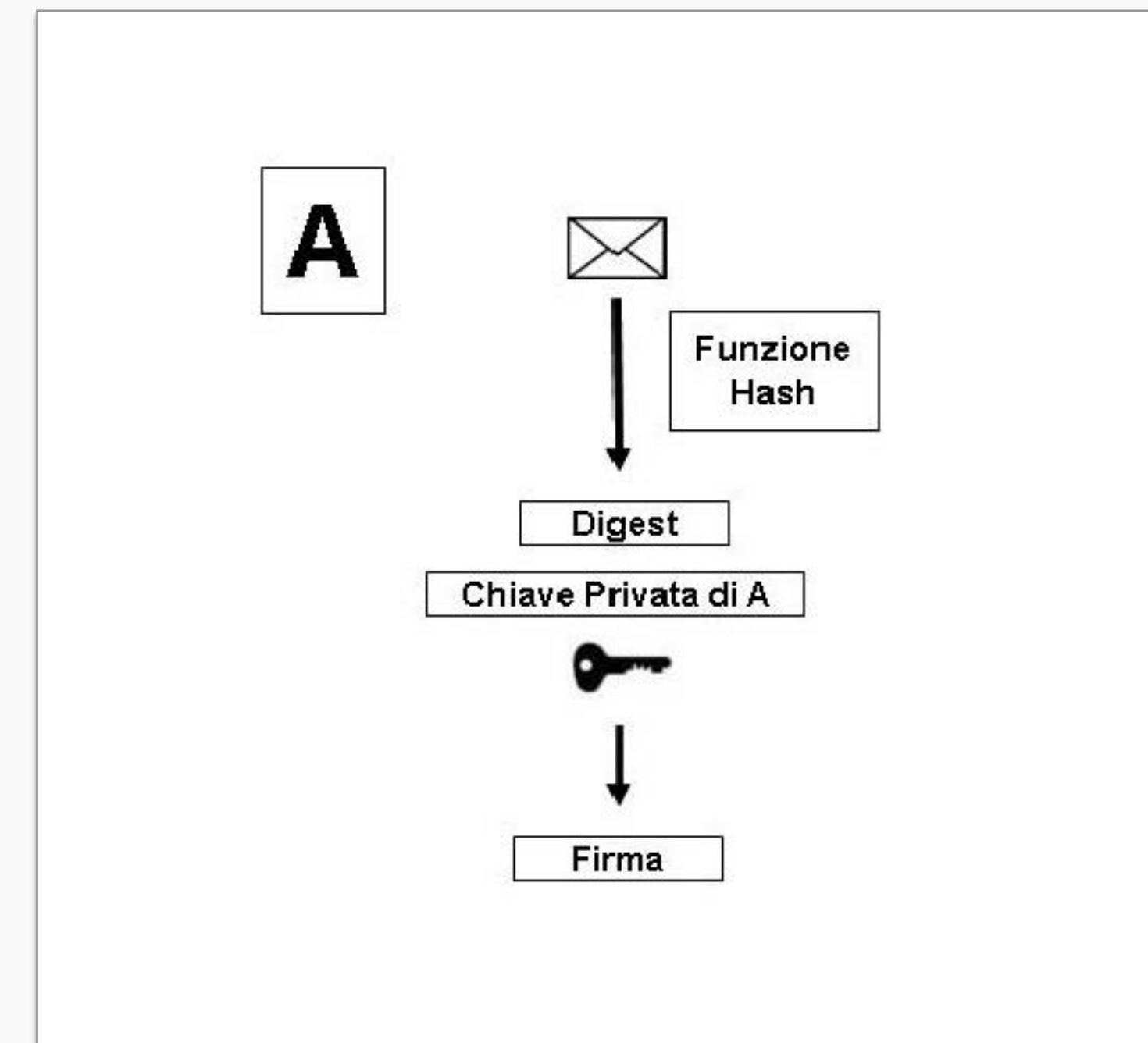
Una firma digitale valida garantisce al destinatario che il mittente del messaggio sia chi dice di essere (autenticazione), che il mittente non possa negare di averlo inviato (non ripudio), e che il messaggio non sia stato alterato lungo il percorso dal mittente al destinatario (integrità).



Firma **Digitale**

Invio

- Il mittente (A) applica una funzione Hash sul messaggio da inviare, ottenendo un Digest che cifra usando la propria chiave privata.
- Si ottiene in questo modo la firma, che è in sostanza il Digest crittografato. Il documento e la firma vengono inviati al destinatario (B).

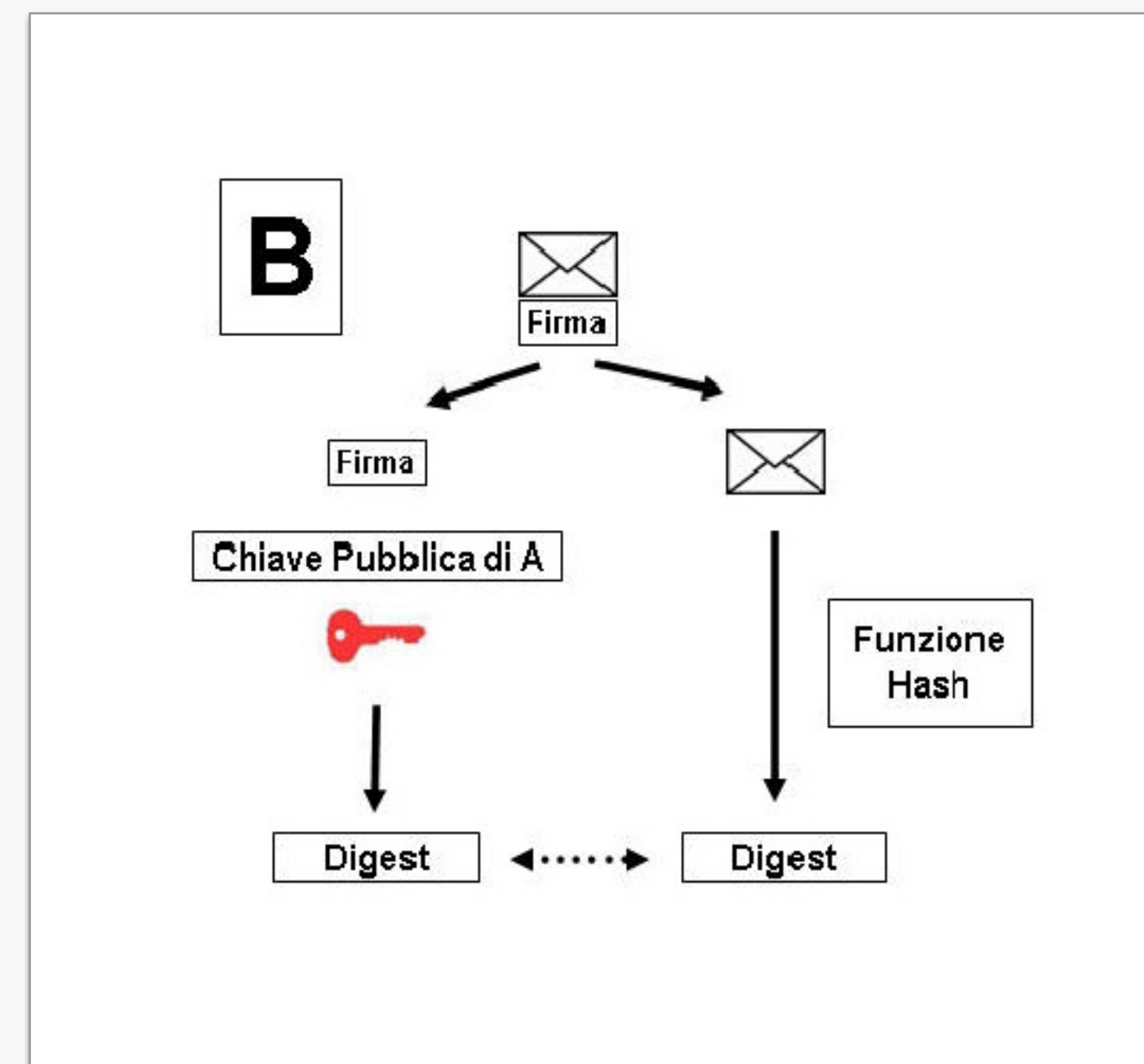




Firma **Digitale**

Ricezione

- Quando il destinatario riceve il messaggio, lo separa in documento originale e firma digitale.
- Essendo in possesso della chiave pubblica del mittente è in grado di decifrare la firma digitale ottenendo il Digest, applica poi al documento originale la medesima funzione Hash, utilizzata dal mittente, e se questa produce un Digest uguale a quello che ha appena decifrato allora ha la garanzia che il messaggio è integro e autentico.





Indice della **Lezione**

FONDAMENTALI

1. La nascita del Bitcoin
2. Cos'è il Bitcoin?
3. Il protocollo Bitcoin
- 4. Cos'è la Blockchain?**
5. Cos'è un Blocco?
6. Transazioni





Cos'è la **Blockchain**?

Blockchain è un registro pubblico di tutte le transazioni in Bitcoin. Tali transazioni sono contenute in blocchi ordinati cronologicamente.

Dal punto di vista informatico, la Blockchain si definisce come un database memorizzato e distribuito su ogni macchina che fa parte del network Bitcoin.



Catena di **Blocchi**

- La traduzione di Blockchain è “catena di blocchi”, questo perché ogni blocco, che la compone, è per costruzione collegato con il precedente.
- Partendo dall’ultimo blocco generato si può risalire la catena fino ad arrivare al blocco 0.





Catena di **Blocchi**

- La traduzione di Blockchain è “catena di blocchi”, questo perché ogni blocco, che la compone, è per costruzione collegato con il precedente.
- Partendo dall’ultimo blocco generato si può risalire la catena fino ad arrivare al blocco 0.



LAST BLOCK

Ultimo blocco n creato
al tempo t



Catena di **Blocchi**

- La traduzione di Blockchain è “catena di blocchi”, questo perché ogni blocco, che la compone, è per costruzione collegato con il precedente.
- Partendo dall’ultimo blocco generato si può risalire la catena fino ad arrivare al blocco 0.



BLOCK $n-1$



Catena di **Blocchi**

- La traduzione di Blockchain è “catena di blocchi”, questo perché ogni blocco, che la compone, è per costruzione collegato con il precedente.
- Partendo dall’ultimo blocco generato si può risalire la catena fino ad arrivare al blocco 0.



BLOCK $n-2$



Catena di **Blocchi**

- La traduzione di Blockchain è “catena di blocchi”, questo perché ogni blocco, che la compone, è per costruzione collegato con il precedente.
- Partendo dall’ultimo blocco generato si può risalire la catena fino ad arrivare al blocco 0.



BLOCK $n-3$



Catena di **Blocchi**

- La traduzione di Blockchain è “catena di blocchi”, questo perché ogni blocco, che la compone, è per costruzione collegato con il precedente.
- Partendo dall’ultimo blocco generato si può risalire la catena fino ad arrivare al blocco 0.

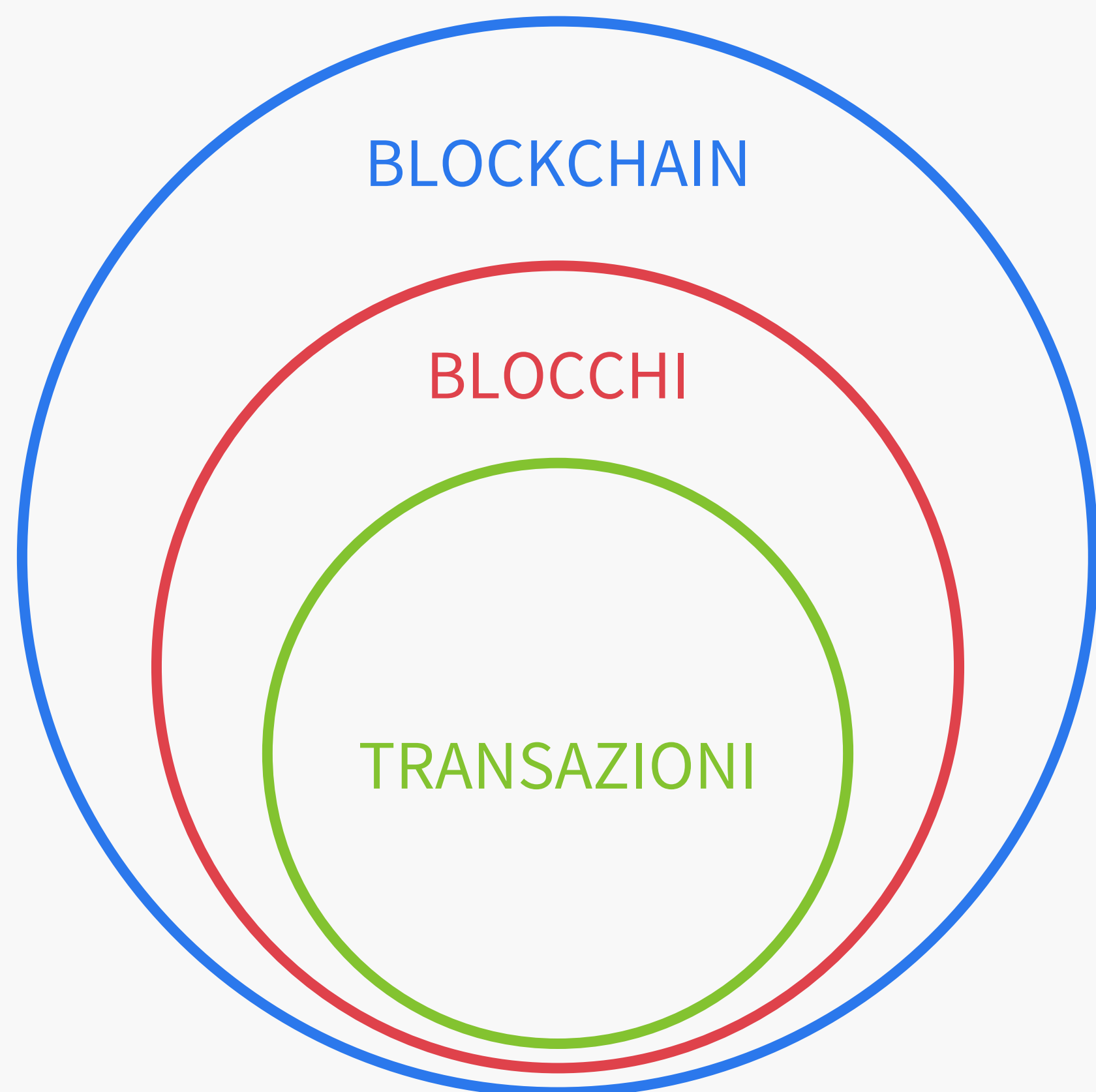


GENESIS BLOCK

Il blocco 0 nasce il 3 Gennaio
2009 alle ore 18:15:05 GMT



Componenti della **Blockchain**



- La Blockchain contiene i blocchi.
- Un blocco è una parte della Blockchain che contiene e conferma le transazioni. In media ogni 10 minuti viene creato un nuovo blocco ed è aggiunto alla Blockchain attraverso il processo di mining.
- Per conferma si intende la verifica della transazione. Una sola conferma può talvolta essere sufficiente, ma per grandi somme è possibile aspettare più conferme, solitamente sei. Ogni nuova conferma riduce esponenzialmente il rischio d'annullamento della transazione.



Indice della **Lezione**

FONDAMENTALI

1. La nascita del Bitcoin
2. Cos'è il Bitcoin?
3. Il protocollo Bitcoin
4. Cos'è la Blockchain?
- 5. Cos'è un Blocco?**
6. Transazioni





Cos'è un **Blocco**?

Un blocco è un file in cui sono contenute una serie di informazioni, tra cui:

- Numero del blocco: i blocchi sono numerati in modo crescente, a partire dal blocco 0.
- Codice Hash: ogni blocco è identificato in maniera univoca da un certo codice alfanumerico.
- Data e ora in cui il blocco è stato creato.
- Tutte le transazioni confermate nel blocco.
- Totale dei Bitcoin movimentati all'interno del blocco.
- Dimensioni in kiloByte del blocco.



- <https://blockchain.info>
- <https://blockexplorer.com>



Genesis **Block**

Block #0			
BlockHash 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f			
Number of transactions	1	Difficulty	1
Height	0 (Mainchain)	Bits	1d00ffff
Block Reward	50 BTC	Size (bytes)	285
Timestamp	Jan, 3 2009 7:15:05 PM	Version	1
Mined by		Nonce	1083236893
Merkle Root	4a5e1e4baab89f3a3251 8a88c31bc87f6...	Next Block	1

<https://blockexplorer.com/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f>



Blocco

Block #469585			
BlockHash 00000000000000000000c22ef592526148e050209504fafc4af4de6f2eb5bd7590			
Number of transactions	1550	Difficulty	595921917085.416
Height	469585 (Mainchain)	Bits	1801d854
Block Reward	12.5 BTC	Size (bytes)	998076
Timestamp	Jun, 3 2017 7:39:13 PM	Version	536870912
Mined by	AntMiner	Nonce	516711018
Merkle Root	8155be532dfd2406519 ef7bdb4595...	Next Block	469586

<https://blockexplorer.com/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f>



Blocco

Block #469585			
BlockHash 00000000000000000000c22ef592526148e050209504fafc4af4de6f2eb5bd7590			
Number of transactions	1550	Difficulty	595921917085.416
Height	469585 (Mainchain)	Bits	1801d854
Block Reward	12.5 BTC	Size (bytes)	998076
Timestamp	Jun, 3 2017 7:39:13 PM	Version	536870912
Mined by	AntMiner	Nonce	516711018
Merkle Root	8155be532dfd2406519 ef7bdb4595...	Next Block	469586

<https://blockexplorer.com/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f>



Indice della **Lezione**

FONDAMENTALI

1. La nascita del Bitcoin
2. Cos'è il Bitcoin?
3. Il protocollo Bitcoin
4. Cos'è la Blockchain?
5. Cos'è un Blocco?

6. Transazioni





Transazioni nel **Blocco**

Transactions			
512c752a5e120158014cf8c47f330005740fa63b8b5f18dff5d9420d4e4651ff		mined Jun 3, 2017 7:39:13 PM	
No Inputs (Newly Generated Coins)		1L75eRMgeCwAxEjD1oWXjLgud9jxwxm34u	17.31556741 BTC (U)
		17 CONFIRMATIONS	17.31556741 BTC
96ea3a1666a10d6223b22fdadd66055d3a46cc59933eab6c9217b11e3c0f81e2		mined Jun 3, 2017 7:39:13 PM	
1eovjxspiLE4qoxxkqdxVohhB3jZSpTTD	2.8 BTC >>>	1Pznrn13wz7ekjLSVgbjdKmJrgzneEeH6s	2.71107044 BTC (U)
		13eRKEaojrjPbGH5gzmkFTH8b8BDgGt9WT	0.08879396 BTC (S)
FEE: 0.0001356 BTC		17 CONFIRMATIONS	2.7998644 BTC



Transazioni nel **Blocco**

Transactions			
512c752a5e120158014cf8c47f330005740fa63b8b5f18dff5d9420d4e4651ff		mined Jun 3, 2017 7:39:13 PM	
No Inputs (Newly Generated Coins)		1L75eRMgeCwAxEjD1oWXjLgud9jwxm34u	17.31556741 BTC (U)
		17 CONFIRMATIONS	17.31556741 BTC
<div>Coinbase Transactions: è la prima transazione che compare in ogni blocco. Si tratta della ricompensa ottenuta dai minatori per aver risolto il problema matematico contenuto nel blocco stesso.</div>		mined Jun 3, 2017 7:39:13 PM	
		1Pznrn13wz7ekjLSVgbdKmJrgzneEeH6s	2.71107044 BTC (U)
		13eRKEaojrjPbGH5gzmkFTH8b8BDgGt9WT	0.08879396 BTC (S)
		17 CONFIRMATIONS	2.7998644 BTC
FEE: 0.0001356 BTC			



Transazioni nel **Blocco**

Transactions			
512c752a5e120158014cf8c47f330005740fa63b8b5f18dff5d9420d4e4651ff		mined Jun 3, 2017 7:39:13 PM	
No Inputs (Newly Generated Coins)		1L75eRMgeCwAxEjD1oWXjLgud9jxwxm34u	17.31556741 BTC (U)
		17 CONFIRMATIONS	17.31556741 BTC
96ea3a1666a10d6223b22fdadd66055d3a46cc59933eab6c9211e3c0f81e2		7:39:13 PM	
1eovjxspiLE4qoxxkqdxVohhB3jZSpTTD	2.8 BTC >>>	neEeH6s	0.044 BTC (U)
		13eRKEaojrjPbGH5gzmkFTH8b8BDgGt9WT	0.08879396 BTC (S)
FEE: 0.0001356 BTC		17 CONFIRMATIONS	2.7998644 BTC

12.5 BTC + Tot. Fee delle transazioni contenute nel blocco.



Transazioni nel **Blocco**

Transactions			
512c752a5e120158014cf8c47f330005740fa63b8b5f18dff5d9420d4e4651ff		mined Jun 3, 2017 7:39:13 PM	
No Inputs (Newly Generated Coins)		1L75eRMgeCwAxEjD1oWXjLgud9jxwxm34u	17.31556741 BTC (U)
		17 CONFIRMATIONS	17.31556741 BTC
96ea3a1666a10d6223b22fdadd66055d3a46cc59933eab6c9217b11e3c0f81e2		mined Jun 3, 2017 7:39:13 PM	
1eovjxspiLE4qoxxkqdxVohhB3jZSpTTD	2.8 BTC >>>	1Pznrn13wz7ekjLSVgbjdKmJrgzneEeH6s	2.71107044 BTC (U)
		13eRKEaojrjPbGH5gzmkFTH8b8BDgGt9WT	0.08879396 BTC (S)
FEE: 0.0001356 BTC		17 CONFIRMATIONS	2.7998644 BTC



Bitcoin Address

Address			
1eovjxspiLE4qoxxkqdxVohhB3jZSpTTD			
Total Received	2.8 BTC		
Total Sent	2.8 BTC		
Final Balance	0 btc		
N° Transactions	2		

<https://blockexplorer.com/address/1eovjxspiLE4qoxxkqdxVohhB3jZSpTTD>



Cos'è lo **Script**?

Lo script si tratta di un linguaggio che accompagna le transazioni in modo da istruire i nodi su cosa fare dei pacchetti per realizzare operazioni più complesse del semplice trasferimento.

SCRIPT = SCRIPTSIG + SCRIPTPUBKEY

FIRMA DIGITALE

CHIAVE PUBBLICA



Componenti dello **Script**

Funzionamento

- La chiave pubblica appartiene al beneficiario dell'output della transazione, così da permettergli di riscattare il valore di moneta contenuto nell'output.
- L'altra componente è la firma dell'hash. La firma, combinata con la chiave pubblica, dimostra che la transazione è stata eseguita dal legittimo proprietario dell'indirizzo in oggetto.
- In sintesi, il sistema Bitcoin prevede di inviare una transazione con uno script che può essere risolto esclusivamente con una specifica chiave privata, cioè attraverso l'uso della chiave pubblica usata per creare lo script.



Numero di **Transazioni**

—N° transazioni giornaliere





Numero di **Transazioni**

■ N° transazioni mensili

