

Bitcoin: Fidarsi o non Fidarsi?

Luca Grilli, DI UniPG



UNIVERSITÀ DEGLI STUDI
DI PERUGIA

Sommario

- Prologo
- Perché il BTC?
- Come funziona il BTC?
- Conclusioni



Prologo

Una storiella per iniziare ...

- nel **2009**
 - studente norvegese
 - acquistò **5600 BTC** con **19 €** (150 corone)

Kristoffer Koch



Una storiella per iniziare ...

- nel **2009**
 - studente norvegese
 - acquistò **5600 BTC** con **19 €** (150 corone)
- ... poi **dimenticò** ...

Kristoffer Koch



Una storiella per iniziare ...

- nel **2009**
 - studente norvegese
 - acquistò **5600 BTC** con **19 €** (150 corone)
- ... poi **dimenticò** ...
- nel **2013**
 - **1 BTC = 205 €**
 - Koch era **MILIONARIO!!!**

Kristoffer Koch



... ma che cos'è il Bitcoin?

- Possibile definizione
 - il bitcoin è una **critto-valuta digitale** introdotta nel 2009 da **Satoshi Nakamoto**

... ma che cos'è il Bitcoin?

- Possibile definizione
 - il bitcoin è una **critto-valuta digitale** introdotta nel 2009 da **Satoshi Nakamoto**
- Perché il Bitcoin? Come funziona?
 - speriamo di chiarirlo oggi
 - ... ma molti **misteri** rimangono

... ma che cos'è il Bitcoin?

- Possibile definizione
 - il bitcoin è una **critto-valuta digitale** introdotta nel 2009 da **Satoshi Nakamoto**
- Perché il Bitcoin? Come funziona?
 - speriamo di chiarirlo oggi
 - ... ma molti **misteri** rimangono
- **Primo mistero**
 - chi è Satoshi Nakamoto?

Chi è Satoshi Nakamoto?



è Dorian Satoshi Nakamoto?

Chi è Satoshi Nakamoto?

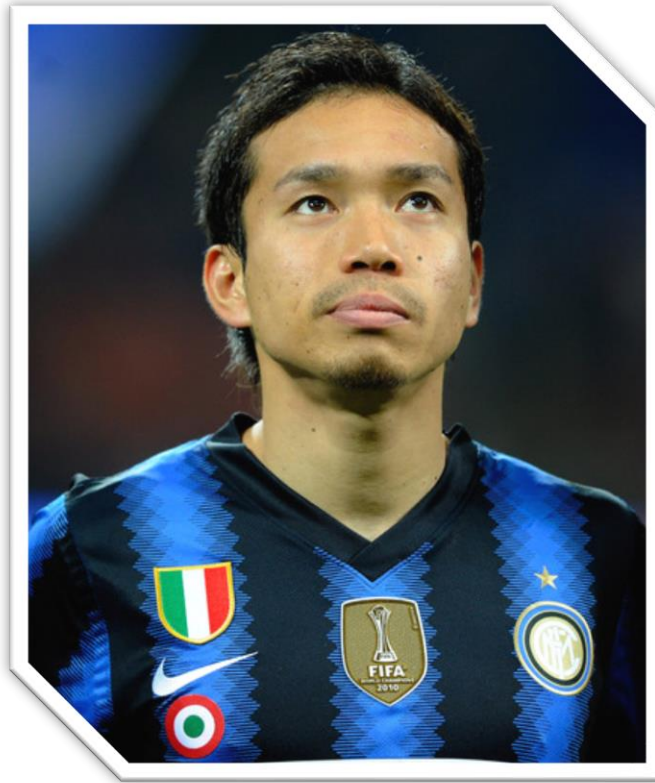


Dorian S. Nakamoto NEGA

Chi è Satoshi Nakamoto?



è Tatsuaki Okamoto, NSA?



Chi è Satoshi Nakamoto?

è Yuto Nagatomo, ex FC Inter?

Chi è Satoshi Nakamoto?



per chi vuole fare un regalo!

Chi è Satoshi Nakamoto?



è ancora un mistero!

... BTC e anonimato ...



Deposit Address:

Account Balance:

Pending:

0.00000

BTC

0.00000

BTC

Home

Your Account

Your Purchases

Forum

Logout

Help

Categories

Drugs (2814)

Services (1177)

Data (676)

Weapons (148)

Collectables (29)

Metals/Stones (19)

Other (244)

Software (144)

Movies (32)

Tobacco (165)

Counterfeits (82)

Alcohol (16)

eBooks (771)

Exchange

Exchange

User Menu

Home

Inbox (0/0)

Account

Purchases

Favorites

Deposit Addresses

Forum

There's no account admin or similar here, if anyone other than backopy (user id 1) addresses you by PM **that person has nothing to do with BMR** and is most likely just a scammer trying to impersonate the BMR staff!

Search

in All Categories

Search



Drugs > Cannabis > Weed
1/2oz. Cosmic OG(FREE
1/4oz. of Indoor Shake
Included)
Seller: CalBud2052 (1044)

1.17261 BTC



Alcohol > Wine
(RARE BAROLO 1964
COLLECTOR'S WINE
Seller: fake (594)

2.47974 BTC



Services > Money
(SSN/DL#/UKDOB
SEARCH: GUARANTEED G4
CCS
Seller: demonita (464)

6.14071 BTC



Drugs > Ecstasy
1 kpl 200 mg Party Flocker
ESSO
Seller: Prodig (414)

0.34716 BTC



Drugs > Cannabis > Seeds
(5) LifeSaver (B.O.G.
Seeds)
Seller: Toolleg (346)

0.42214 BTC



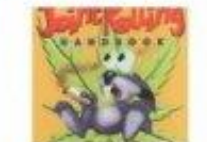
Drugs > Psychedelics > Others
2C-B 200mg
Seller: neoliberalian (307)

0.64349 BTC



Drugs > Stimulants > Speed
28.5g Speed /
Amphetamine paste (1
Ounce)
Seller: Bungee54 (400)

2.33583 BTC



eBooks > Drugs
The Joint Rolling
Handbook
Seller: captaincard (0)

0.00938 BTC



Drugs > Ecstasy
("1Gram Dutch MDMA
Crystals 82%-Promo
Seller: QualityDrug (163)

0.21078 BTC



Data > Digital Goods
[ebook] Dynamite
Mentalism by George
Anderson
Seller: sh4d3r1950 (308)

0.02814 BTC



Services > Documents
[Document] Ohio
(OH-USA) Driving License
PSD File
Seller: sh4d3r1950 (308)

0.00000 BTC

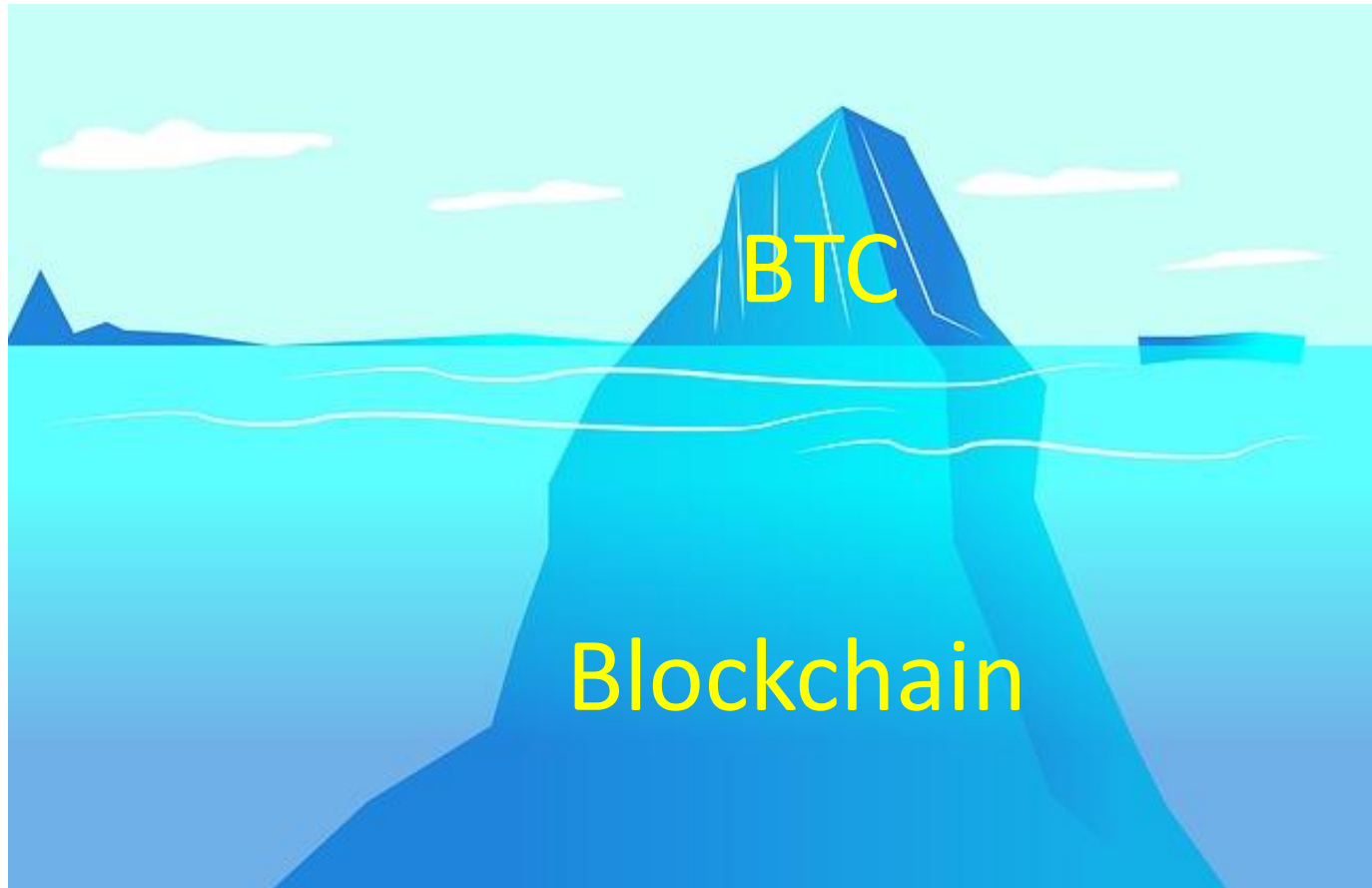


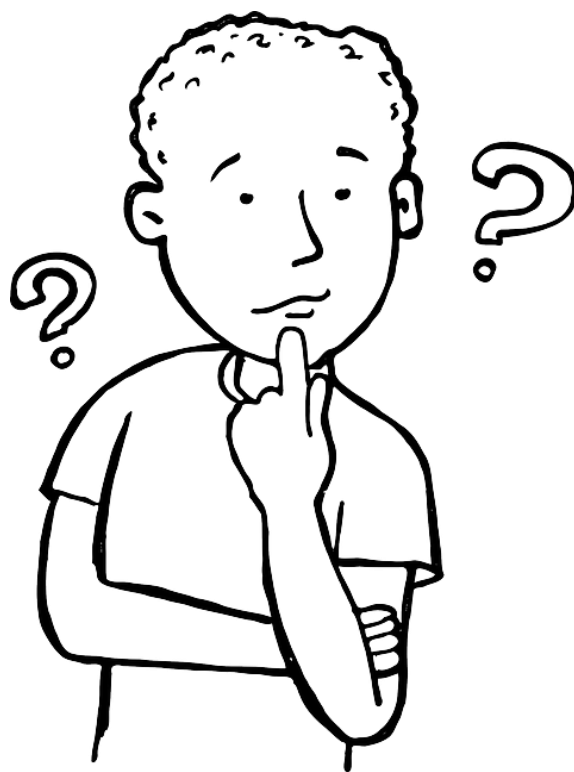
Services > Money
(5 EU CC No.1
Seller: fair-deals (74)

3.20000 BTC

BTC e BlackMarket

Bitcoin vs Blockchain





Perché il Bitcoin?

Verità e Fiducia: 2 problemi centrali

- **Verità:** capacità di ricostruire la **storia** esatta di come fatti/eventi sono avvenuti
- In informatica: **fatti \equiv informazioni**
 - verità \Leftrightarrow capacità di gestire una **struttura dati** (logica) rappresentativa della realtà e/o coerente a determinati vincoli di dominio
- **Fiducia:** credere che una certa entità agisca in un determinato modo, senza poterlo verificare

Verità vs Autenticità

- ***Autenticità***: capacità di verificare se una data informazione è stata prodotta e/o sottoscritta da una specifica entità (fonte)



Autenticità tramite Crittografia

Fiducia



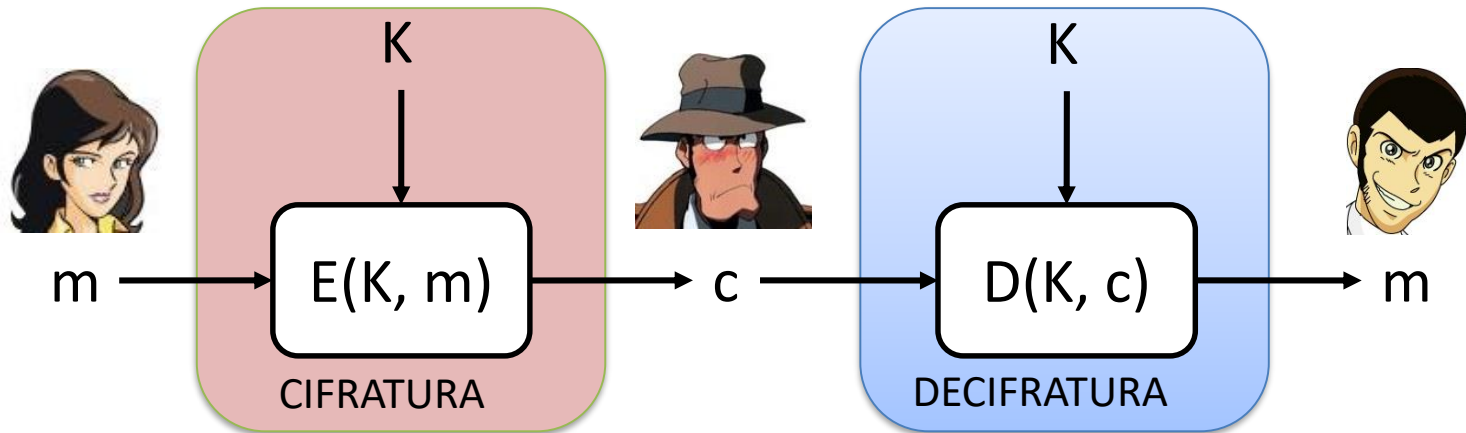
Prova Crittografica





Come si realizza una prova crittografica?

Crittografia a *chiave segreta* (o *simmetrica*)



m: testo in chiaro

c: testo cifrato

K: chiave crittografica segreta

$E(K, m)$: funzione di cifratura

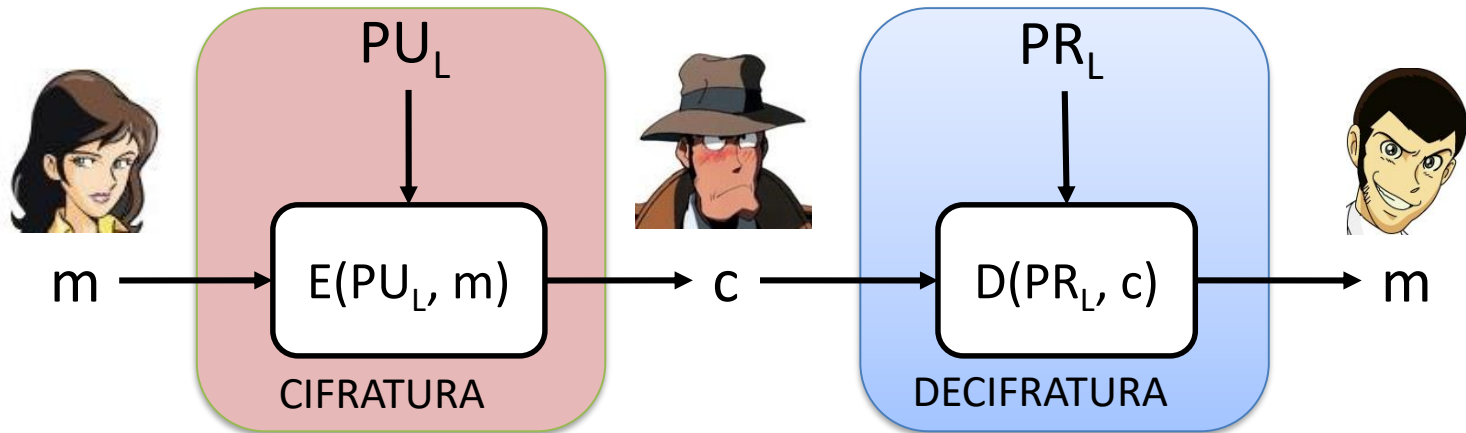
$D(K, m)$: funzione di decifratura

impiego classico: **protezione della confidenzialità**

Crittografia a *chiave pubblica* (o *asimmetrica*)

- Anziché **una** chiave segreta condivisa K
- Due chiavi accoppiate $\langle PU, PR \rangle$
 - **PU: chiave pubblica**, da divulgare
 - **PR: chiave privata**, da custodire segretamente
- Impiego
 - protezione della confidenzialità
 - protezione dell'**autenticità** (**firma digitale**)

Crittografia a *chiave pubblica* (o *asimmetrica*)



m : testo in chiaro

c : testo cifrato

PU_L : **chiave pubblica** di Lupin

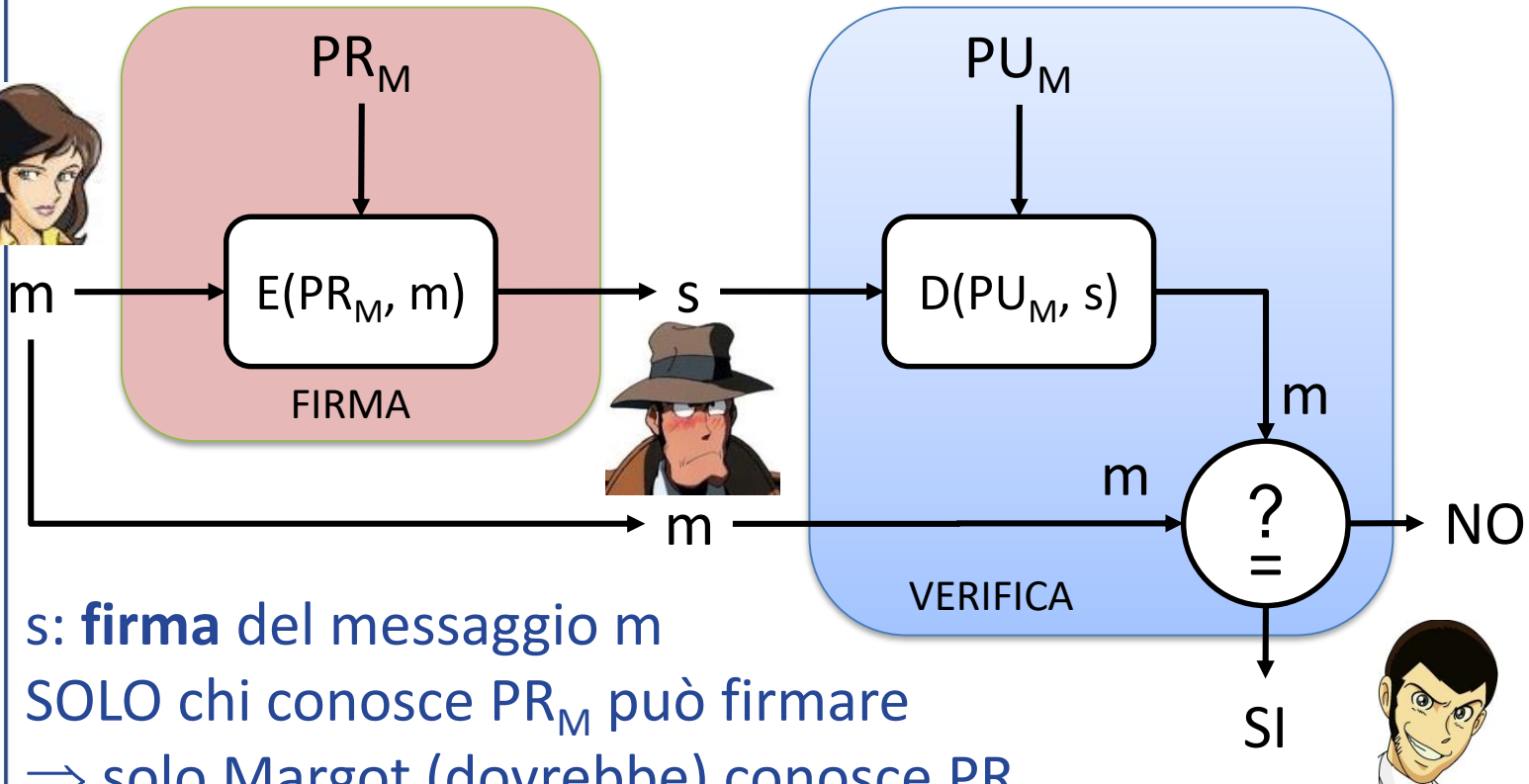
PR_L : **chiave privata** di Lupin

$E(PU_L, m)$: funzione di cifratura a chiave pubblica

$D(PR_L, m)$: funzione di decifratura a chiave pubblica

impiego: **protezione della confidenzialità**

Firma digitale



s : **firma** del messaggio m

SOLO chi conosce PR_M può firmare

\Rightarrow solo Margot (dovrebbe) conosce PR_M

Lupin (o chiunque) può verificare l'**autenticità** del messaggio effettuando un semplice test

... quindi ...

- **Firma digitale \Rightarrow autenticità *senza doversi fidare***
- **Firma digitale $?\Rightarrow?$ verità *senza doversi fidare***

... quindi ...

- Firma digitale \Rightarrow autenticità *senza doversi fidare*
- Firma digitale $?\Rightarrow?$ verità *senza doversi fidare*

NO!!!

- **Esistono le MENZOGNE AUTENTICHE**
 - falsità prodotte da fonti (crittograficamente) verificabili

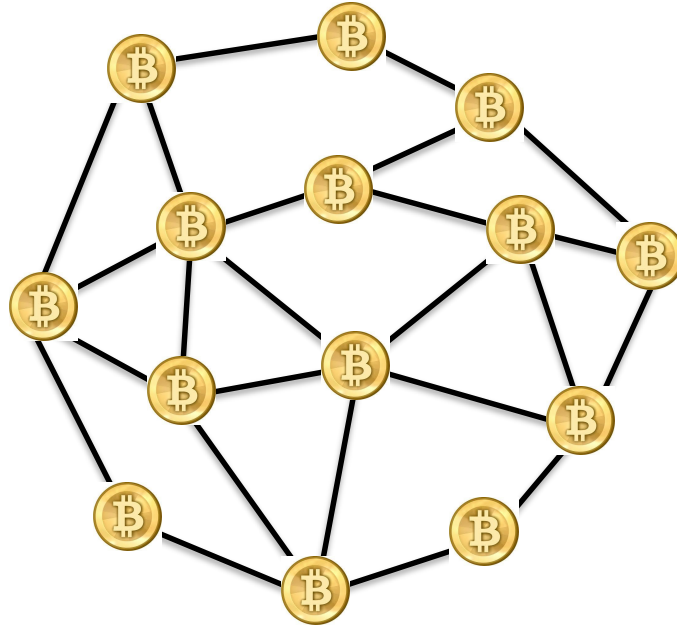
Verità \Rightarrow Fiducia

- **Verità** ottenibile tramite
 - verifiche (crittografiche) di autenticità
 - controlli sulla coerenza logica dei dati
 - accessibilità ai dati (trasparenza)
 - immutabilità dati accettati
 - ...
- \Rightarrow richiede comunque **fiducia** in chi esegue queste verifiche/controlli
 - soprattutto in processi **fortemente dinamici**

Modelli per la gestione della fiducia



Bitcoin/Blockchain



Primo esempio di modello decentralizzato
aperto e pubblico



Altri ingredienti **crittografici fondamentali**

Funzioni crittografiche di hash

- NON richiedono l'uso di una chiave crittografica
 - INPUT: stringa binaria di qualsiasi lunghezza
 - OUTPUT: stringa binaria di lunghezza prefissata (128 bit, 256 bit, 512 bit)
- Proprietà
 - **pseudo-randomicità** (instabilità)
 - **resistenza alla preimmagine**
 - **resistenza alle collisioni**

Un hash a 128 bit – MD5

INPUT

$m \in \{0,1\}^*$

OUTPUT

$h(m) \in \{0,1\}^{128}$

Nel mezzo del cammin di nostra vita
mi ritrovai per una selva oscura
ché la diritta via era smarrita.
Ahi quanto a dir qual era è cosa dura
esta selva selvaggia e aspra e forte
che nel pensier rinova la paura!
Tant'è amara che poco è più morte;
ma per trattar del ben ch'i' vi trovai,
dirò de l'altre cose ch'i' v'ho scorte.

MD5

c7c35bbb41968390f816a8a6a6dc3932

Un hash a 256 bit – SHA-256

INPUT

$m \in \{0,1\}^*$

OUTPUT

$h(m) \in \{0,1\}^{256}$

Nel mezzo del cammin di nostra vita
mi ritrovai per una selva oscura
ché la diritta via era smarrita.
Ahi quanto a dir qual era è cosa dura
esta selva selvaggia e aspra e forte
che nel pensier rinova la paura!
Tant'è amara che poco è più morte;
ma per trattar del ben ch'i' vi trovai,
dirò de l'altre cose ch'i' v'ho scorte.

SHA-256

494ac477c5f0b482673dee9d68bfd4d2f41c874a9757a8759ea65b4c79db5c7c

Hash di messaggi quasi identici

Nel mezzo del cammin di nostra vita
mi ritrovai per una selva oscura
ché la diritta via era smarrita.
Ahi quanto a dir qual era è cosa dura
esta selva selvaggia e aspra e forte
che nel pensier rinova la paura!
Tant'è amara che poco è più morte;
ma per trattar del ben ch'i' vi trovai,
dirò de l'altre cose ch'i' v'ho scorte.

MD5

c7c35bbb41968390f816a8a6a6dc3932

Ne **centro** del cammin di nostra vita
mi ritrovai per una selva oscura
ché la diritta via era smarrita.
Ahi quanto a dir qual era è cosa dura
esta selva selvaggia e aspra e forte
che nel pensier rinova la paura!
Tant'è amara che poco è più morte;
ma per trattar del ben ch'i' vi trovai,
dirò de l'altre cose ch'i' v'ho scorte.

MD5

496849de742cbdc4f7490c25f76ad798

Hash: *impronta digitale* di un file

Nel mezzo del cammin di nostra vita
mi ritrovai per una selva oscura
ché la diritta via era smarrita.
Ahi quanto a dir qual era è cosa dura
esta selva selvaggia e aspra e forte
che nel pensier rinova la paura!
Tant'è amara che poco è più morte;
ma per trattar del ben ch'i' vi trovai,
dirò de l'altre cose ch'i' v'ho scorte.

MD5



c7c35bbb41968390f816a8a6a6dc3932

Ne centro del cammin di nostra vita
mi ritrovai per una selva oscura
ché la diritta via era smarrita.
Ahi quanto a dir qual era è cosa dura
esta selva selvaggia e aspra e forte
che nel pensier rinova la paura!
Tant'è amara che poco è più morte;
ma per trattar del ben ch'i' vi trovai,
dirò de l'altre cose ch'i' v'ho scorte.

MD5



496849de742cbdc4f7490c25f76ad798

Resistenza alla preimmagine

- Calcolare l'hash $h(m)$ di un messaggio m è relativamente **facile**
- ... e l'inversione di un hash noto? È ancora facile?
- Fissato un hash h'
- Trovare m tale che $h(m) = h'$
- ... è un problema MOLTO complesso!
- Unico approccio noto è procedere per tentativi (approccio a *forza bruta*)

Invertire un hash ... a forza bruta

- h' : hash che si desidera invertire
- PROCEDIMENTO
 - 1. generare un messaggio m_i
 - 2. calcolare $h(m_i)$
 - 3. **TEST**: $h(m_i)$ coincide con h' ?
 - 3.a SE esito TEST **positivo** $\Rightarrow m_i$ è una soluzione accettabile
 - 3.b SE esito TEST **negativo** \Rightarrow ritornare al punto 1.

Quanti tentativi (statisticamente)?

- Mediamente circa metà dei possibili hash
 - 2^{127} per hash a 128 bit
 - 2^{255} per hash a 256 bit
 - Quanto tempo ci vuole, insomma?
 - con una CPU molto potente
 - **1 tentativo in 1 nanosecondo**
 - numero medio di tentativi: $2^{127} \cong 10^{0.3 \cdot 127} \cong 10^{38}$
 - \Rightarrow necessari in media 10^{29} secondi
 - \Rightarrow **più di 10^{21} anni**

Inversione parziale

- A volte può interessare trovare
 - un messaggio m
 - tale che $h(m)$ abbia una struttura **parzialmente** prefissata

- Esempio
 - $h(m)$ deve iniziare con k bit (64 bit) nulli

00000000000000000007fe93b67d1f3caf9d76f7973b16049400a1145ff2ad6f38a

- \Rightarrow necessari mediamente 2^{k-1} tentativi
- $k = 64 \text{ bit} \Rightarrow 2^{63} \cong 10^{0.3 \cdot 63} \cong 10^{18.9}$

Resistenza alle collisioni

- È computazionalmente **infattibile** trovare due messaggi m_1 e m_2 tali che $h(m_1) = h(m_2)$
- Anche in questo caso **solo** approcci a **forza bruta** sono noti
- Si dimostra che sono richiesti, in media, $2^{k/2}$ tentativi
 - 2^{64} per hash a 128 bit
 - 2^{128} per hash a 256 bit

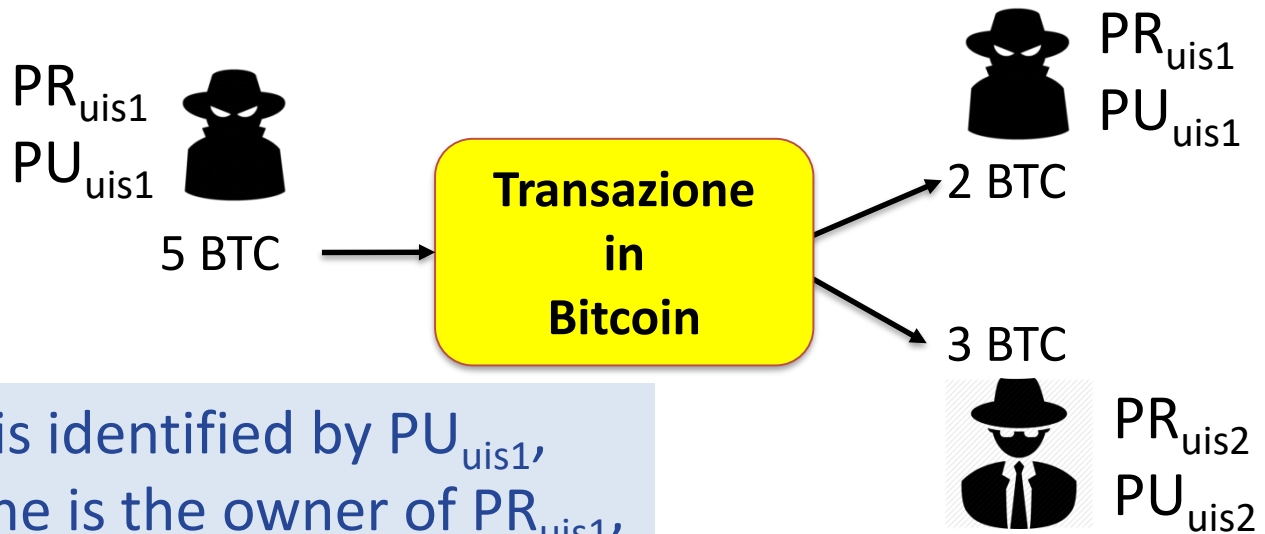


Come funziona il Bitcoin?



... transazioni in Bitcoin ...

BTC prevede transazioni anonime



$uis1$ is identified by PU_{uis1} ,
he/she is the owner of PR_{uis1} ,
but who is $uis1$?

$\sum \text{BTC input} \approx \sum \text{BTC output}$
usati **solo** codici identificativi **anonimi**
tipicamente **chiavi pubbliche**
 \Rightarrow difficile risalire alle identità

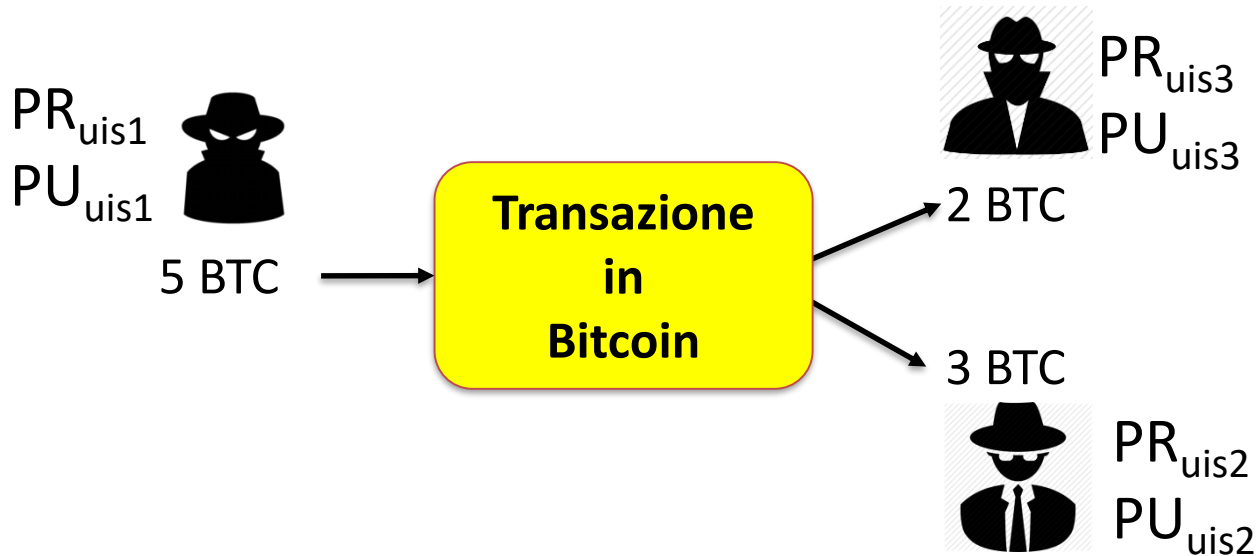
... anonimato rafforzato da ...

- ogni soggetto può avere un numero **arbitrario** di **codici anonimi** (pseudonimi)
- \Rightarrow transazioni verso se stessi non riconoscibili



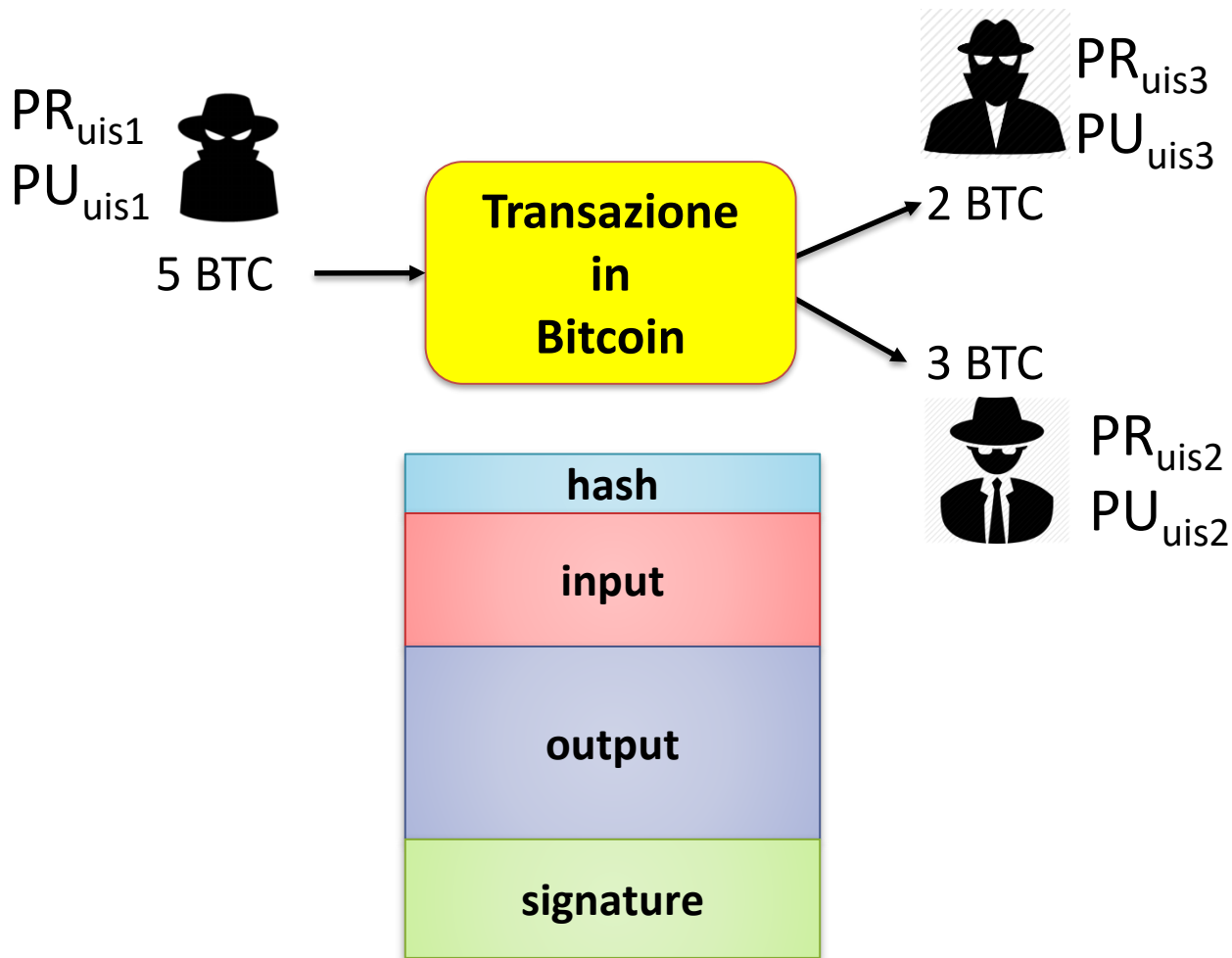
una coppia PU, PR **non** viene **assegnata** da una authority
ma è **generata** dal suo **proprietario**

... anonimato rafforzato da ...



è possibile che uis1, uis2 e uis3
siano la **stessa persona!!**

Bitcoin: dati di una transazione



PR_{uis1}
PU_{uis1}

5 BTC

**Transazione
in
Bitcoin**



PR_{uis3}
PU_{uis3}

2 BTC

3 BTC



PR_{uis2}
PU_{uis2}

hash: b6b89c32.....beca582b

input

prevTxHash: 78e7f.....a14fc5

n: 2

output

value: 3.00000000 BTC

PU_{uis2}: 66be69ac.....e27dcfe7

value: 2.00000000 BTC

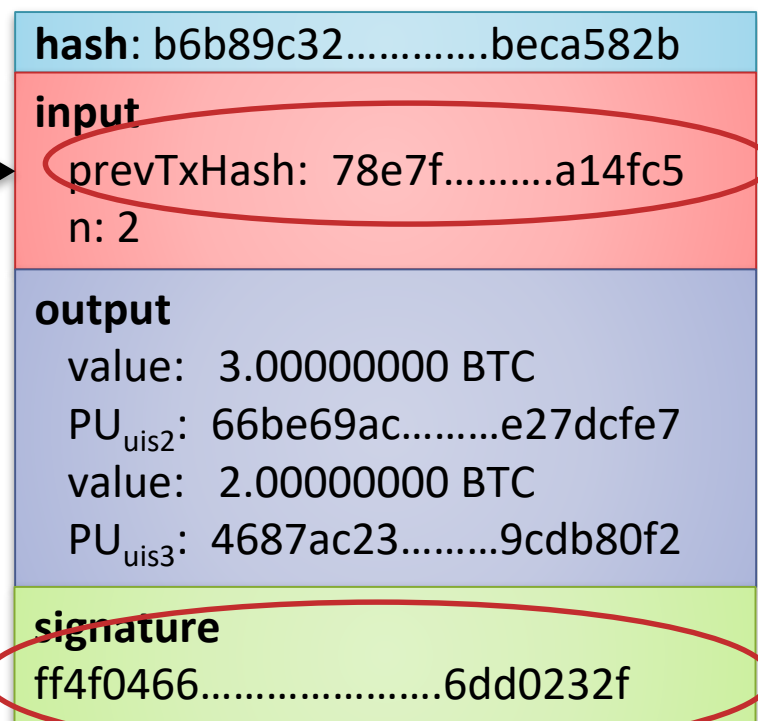
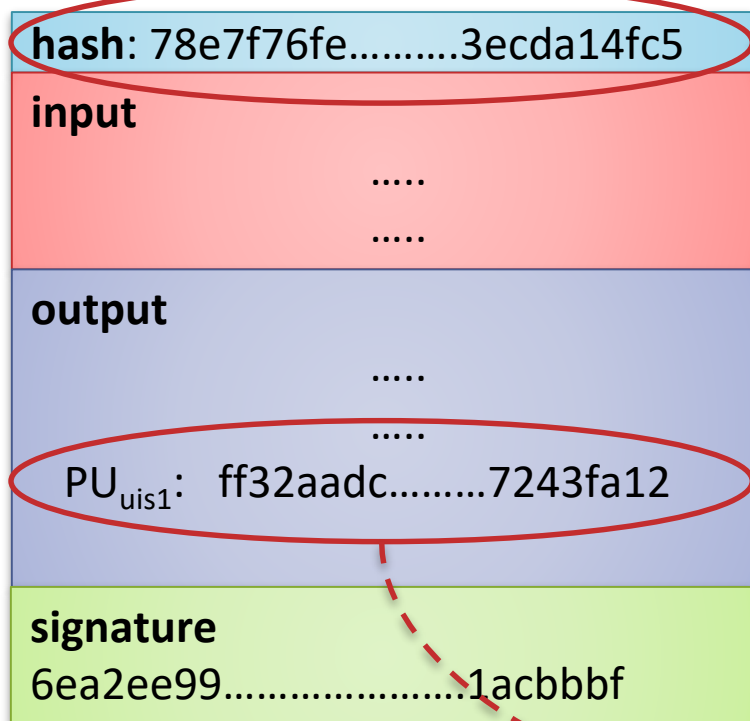
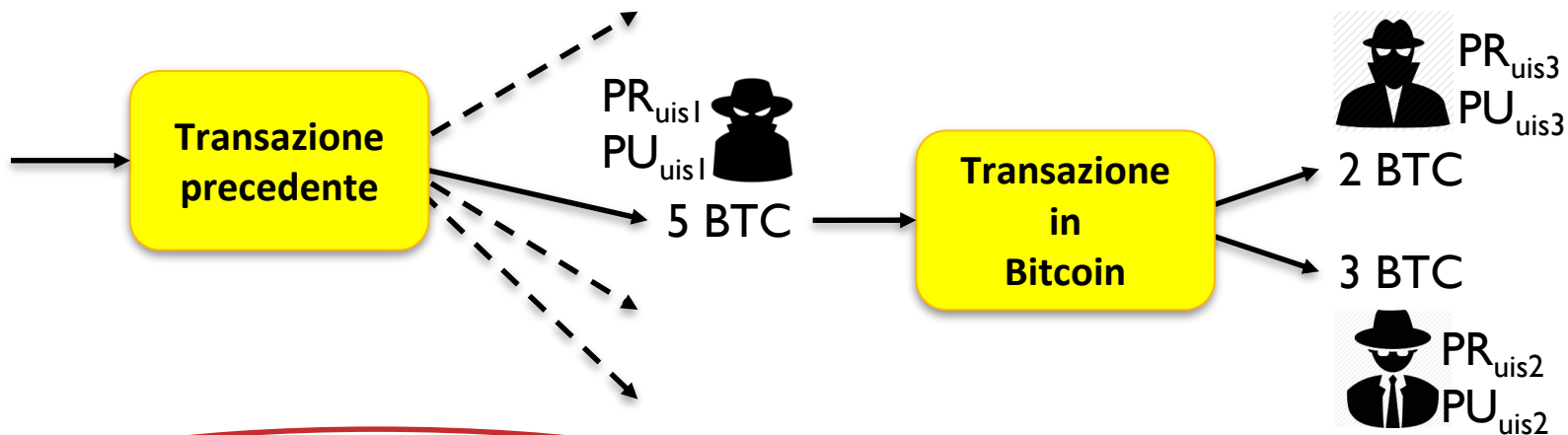
PU_{uis3}: 4687ac23.....9cdb80f2

signature

ff4f0466.....6dd0232f

sign(•, •)

SHA-256

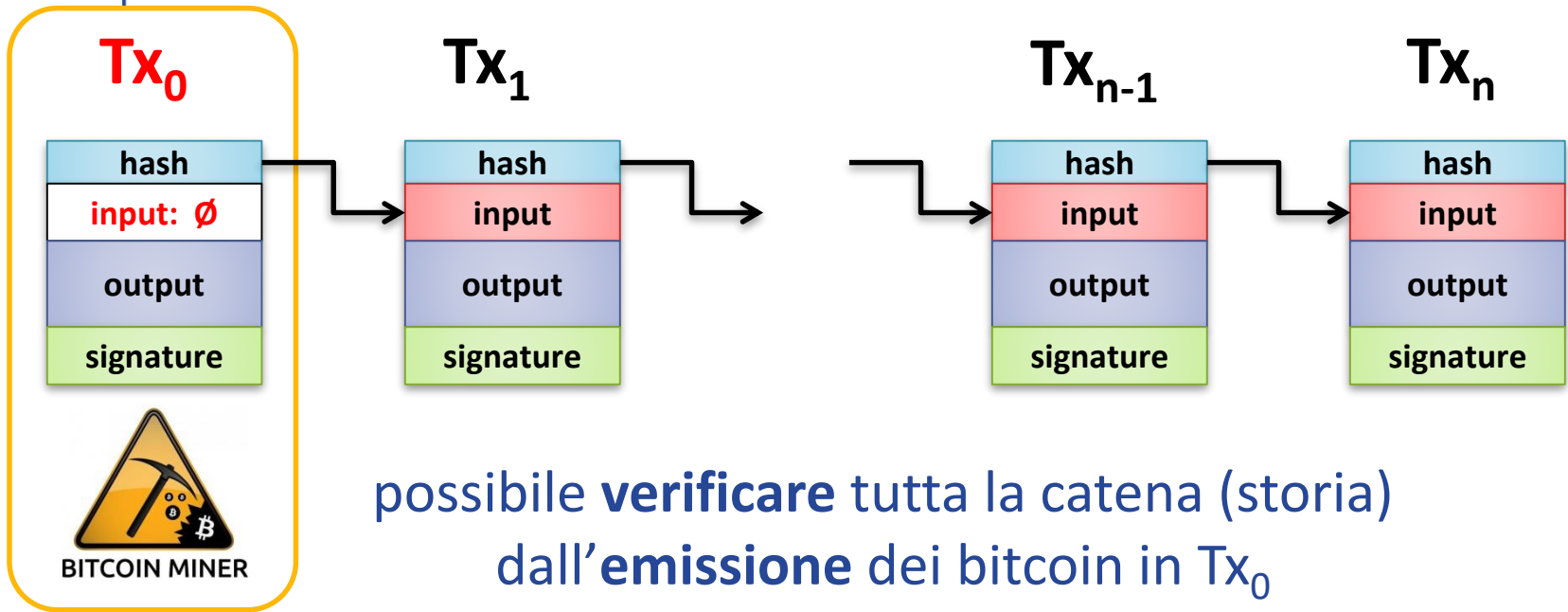


chiave pubblica per **verifica** firma

Firmatario di una transazione

- Il **proprietario** dei 5 BTC in input alla transazione, **firma la transazione**
 - per **verificare** l'autenticità della firma serve la **chiave pubblica** di tale proprietario
 - che deve essere contenuta nella transazione precedente quella corrente
 - nella sezione **input** della transazione corrente è inserito l'hash della precedente transazione
 - \Rightarrow **concatenamento** (o **catena**) delle **proprietà**

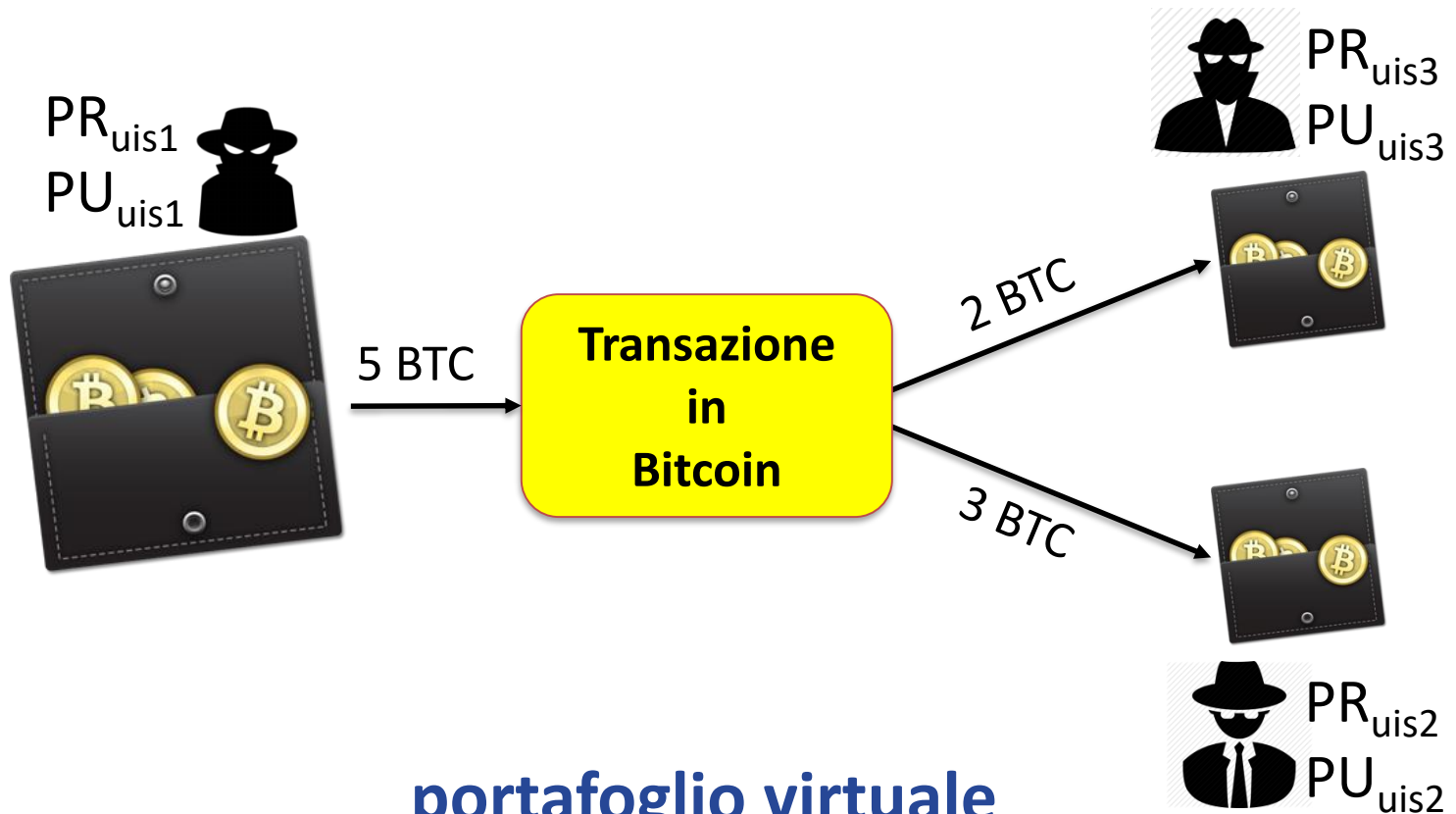
Emissione e catena delle proprietà



Irreversibilità/integrità transazioni

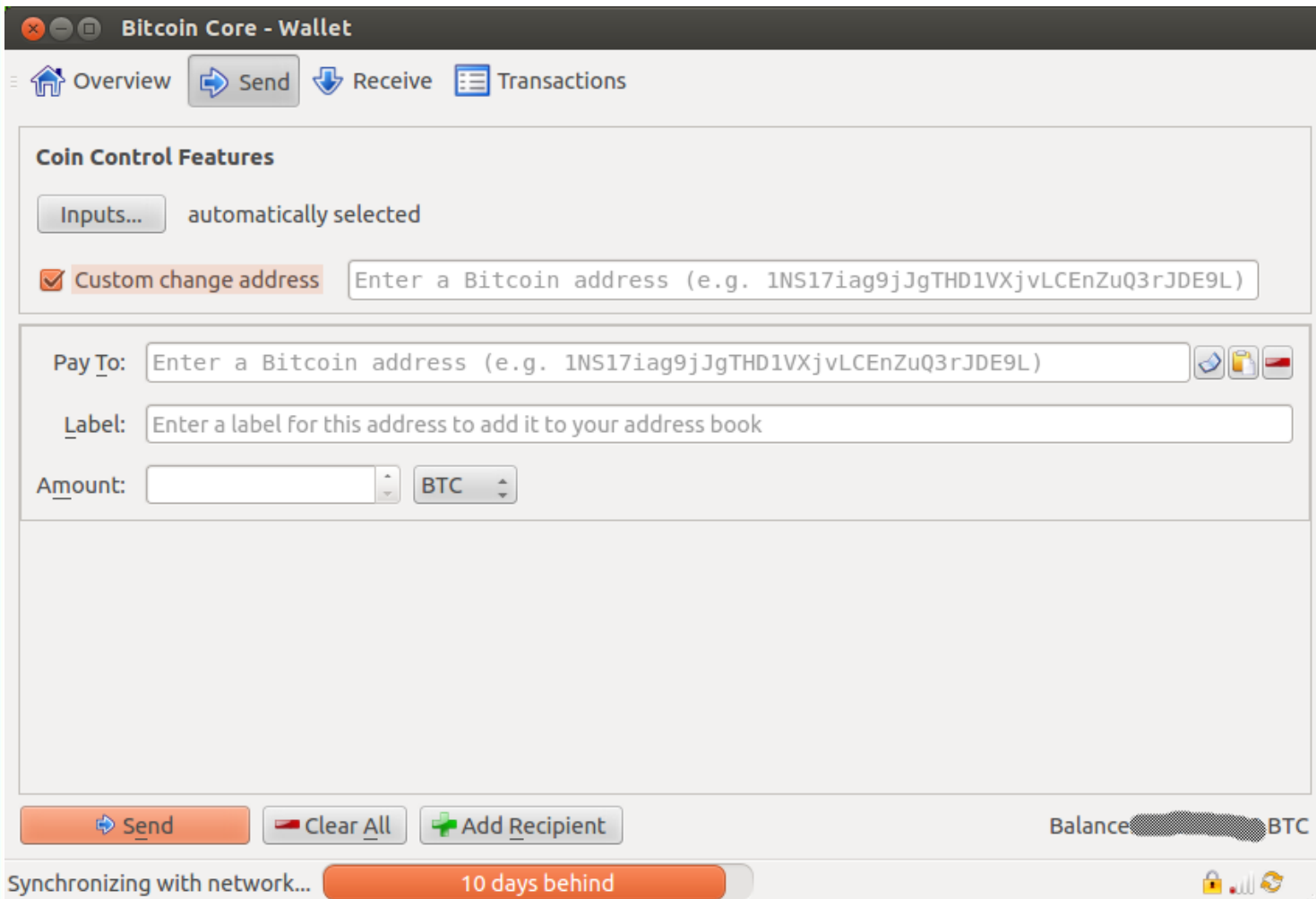
una modifica dei dati di una transazione Tx_i
 \Rightarrow **invalida** Tx_i e tutte le successive transazioni

Portafoglio virtuale (eWallet)



portafoglio virtuale
semplice software per eseguire transazioni

Scegli il tuo portafoglio



Bitcoin Core - Wallet

Overview Send Receive Transactions

Coin Control Features

Inputs... automatically selected

☒ Custom change address Enter a Bitcoin address (e.g. 1NS17iag9jJgTHD1VXjvLCEnZuQ3rJDE9L)

Pay To: Enter a Bitcoin address (e.g. 1NS17iag9jJgTHD1VXjvLCEnZuQ3rJDE9L)

Label: Enter a label for this address to add it to your address book

Amount: BTC

Send Clear All Add Recipient

Balance: [Redacted] BTC

Synchronizing with network... 10 days behind



... ma la firma digitale
non risolve tutti i problemi ...

Attenzione al double spending

- Il problema del **double-spending** rimane!
 - un utente può effettuare una transazione se è il **proprietario** dei bitcoin in input
 - \Rightarrow la firma digitale **non** gli impedisce di ripeterla in seguito anche se non è più il proprietario
- Unica soluzione possibile
 - **tracciare e archiviare tutte le transazioni valide** eseguite da tutti gli utenti
 - una transazione **non appartenente** all'archivio **non** può ritenersi **valida**

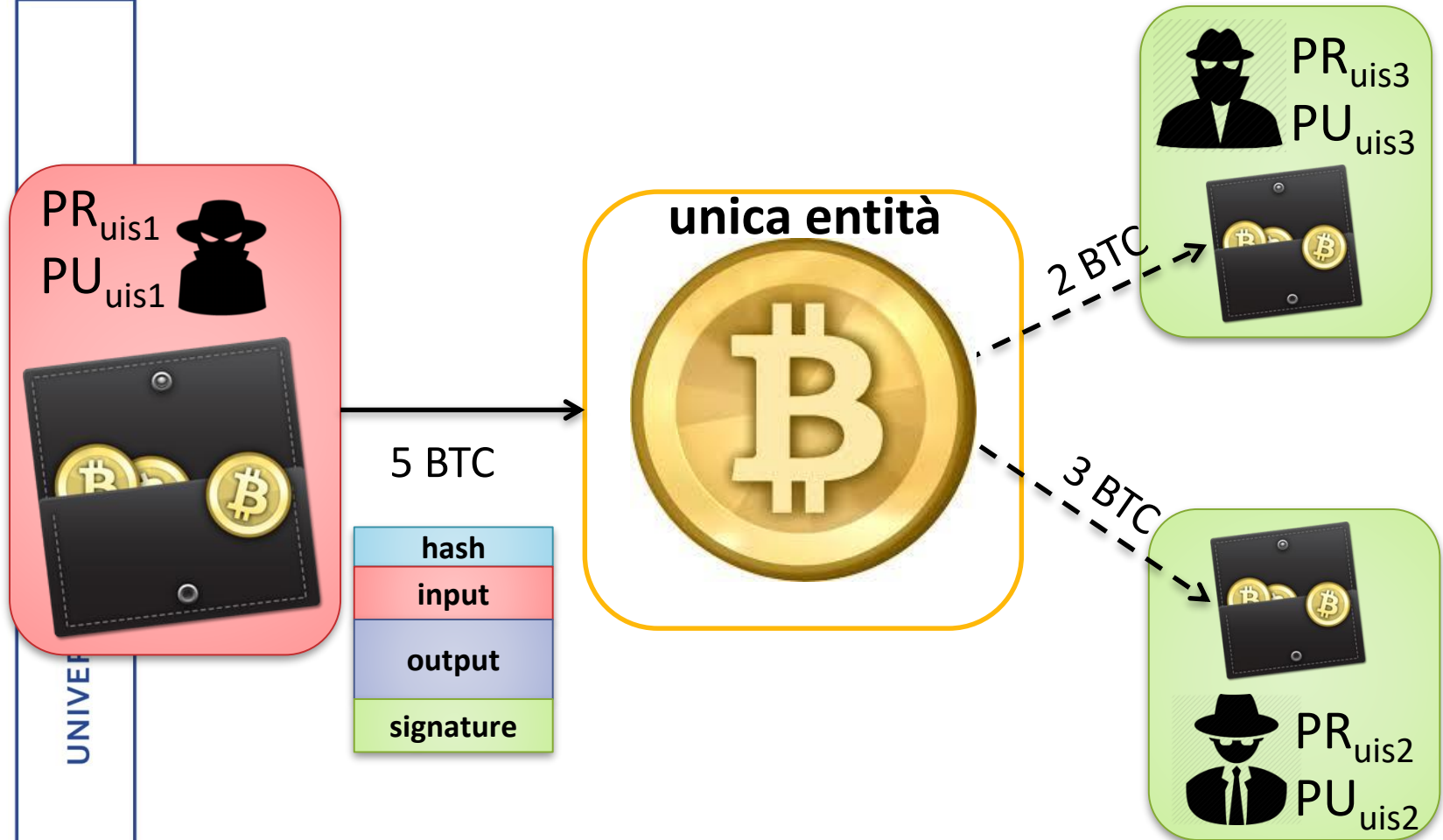


... ma chi traccia, valida e
archivia le transazioni?



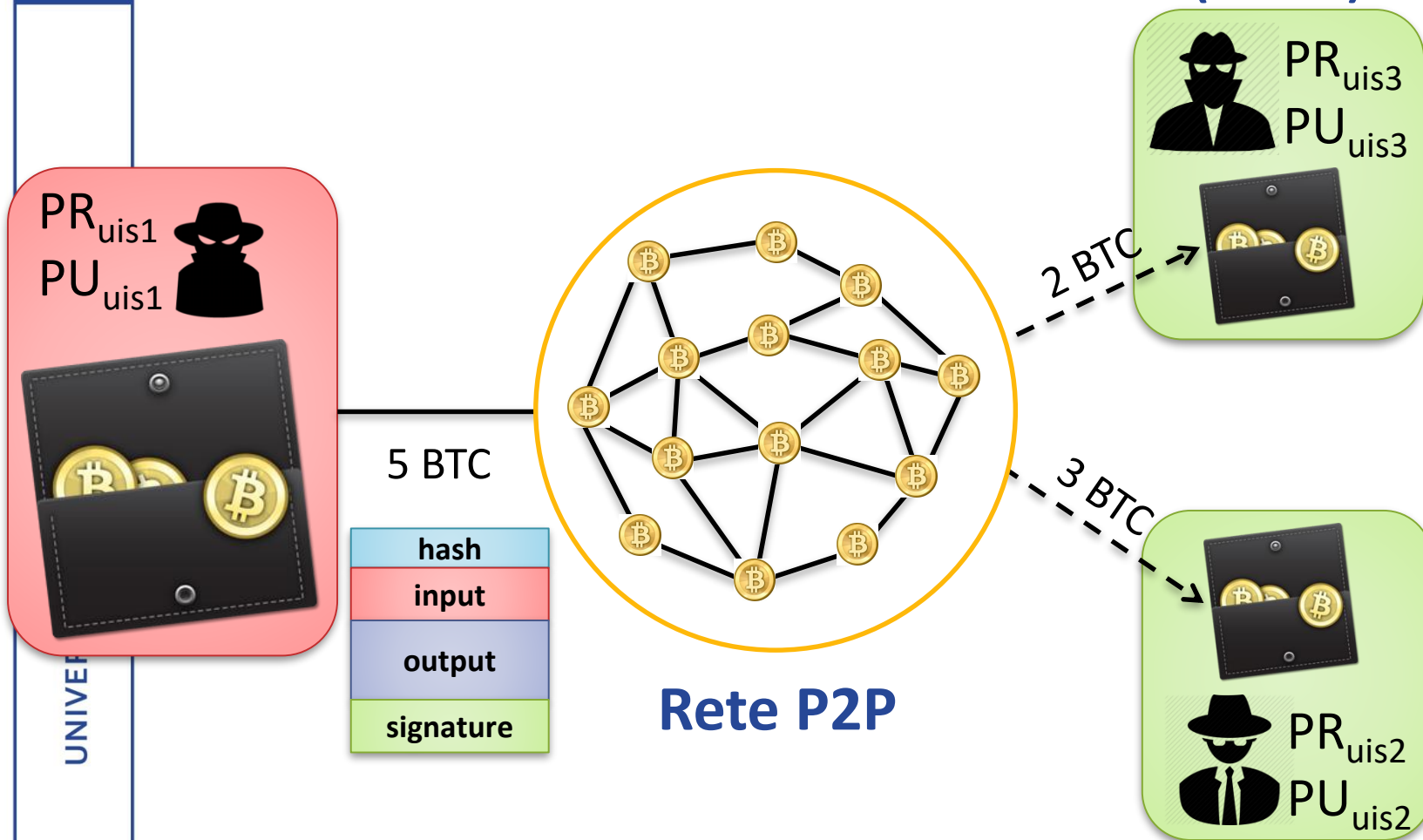
UNIVERSITÀ DEGLI STUDI
DI PERUGIA

Tracciare, archiviare, validare ... chi?

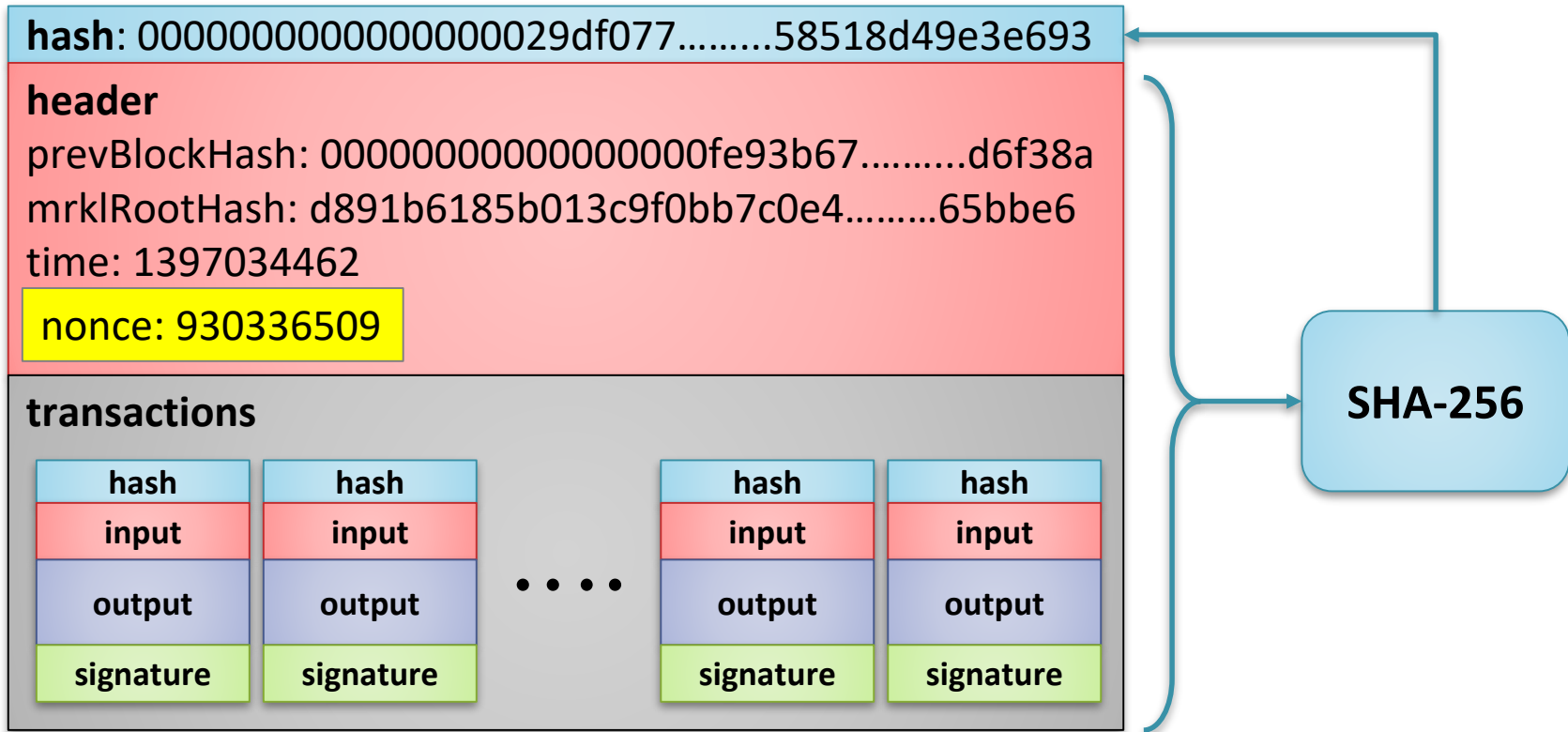


**Nakamoto: "soluzione *INACCETTABILE*
si riottiene un unico intermediario"**

Soluzione: rete Peer-to-Peer (P2P)

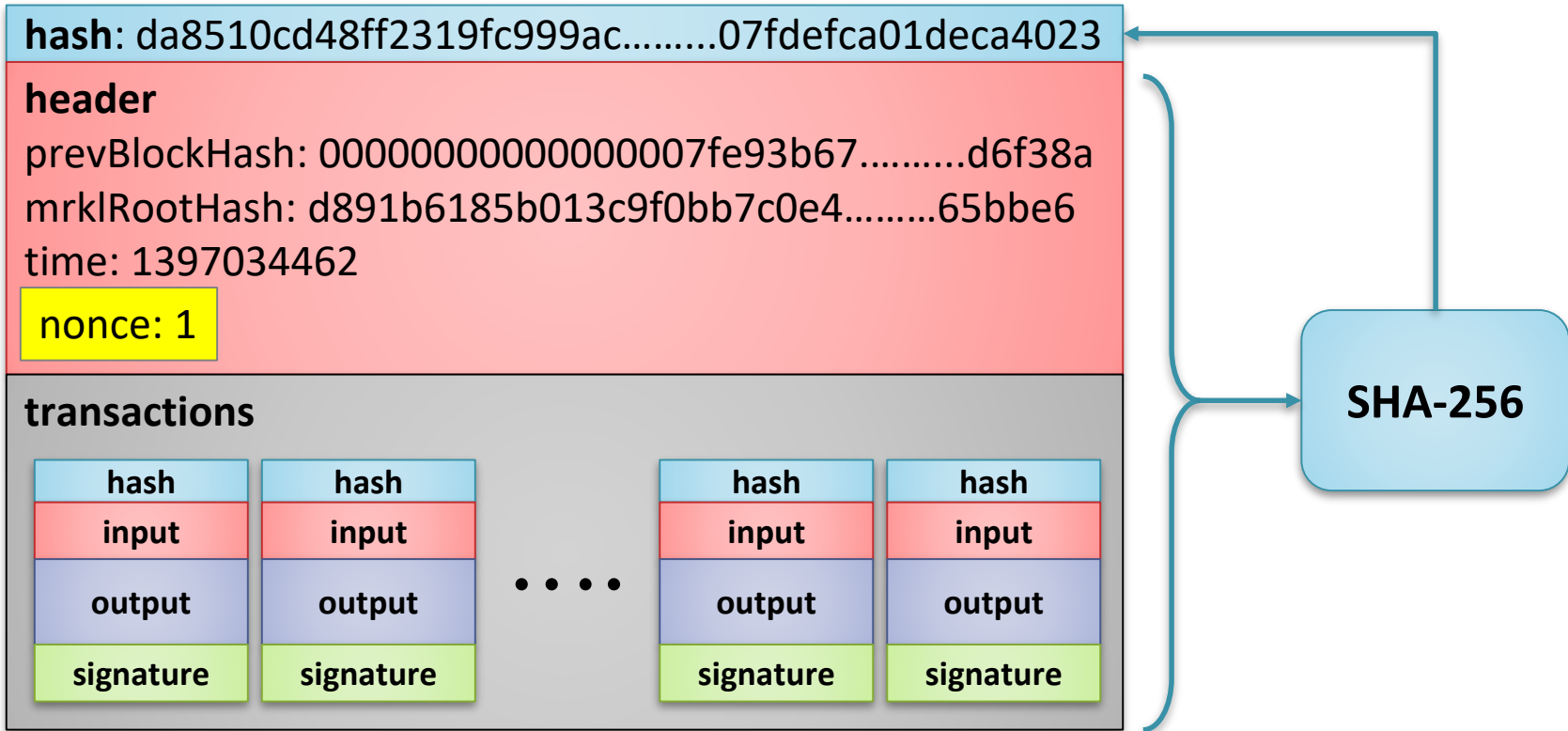


Blocco (accettabile) di transazioni



- l'hash (256 bit) di un blocco **deve** iniziare con almeno 68 bit a 0
- ⇒ inserito il campo **nonce** nell'header
- ⇒ ad ogni tentativo il **nonce** viene incrementato di una unità

Un blocco NON accettabile

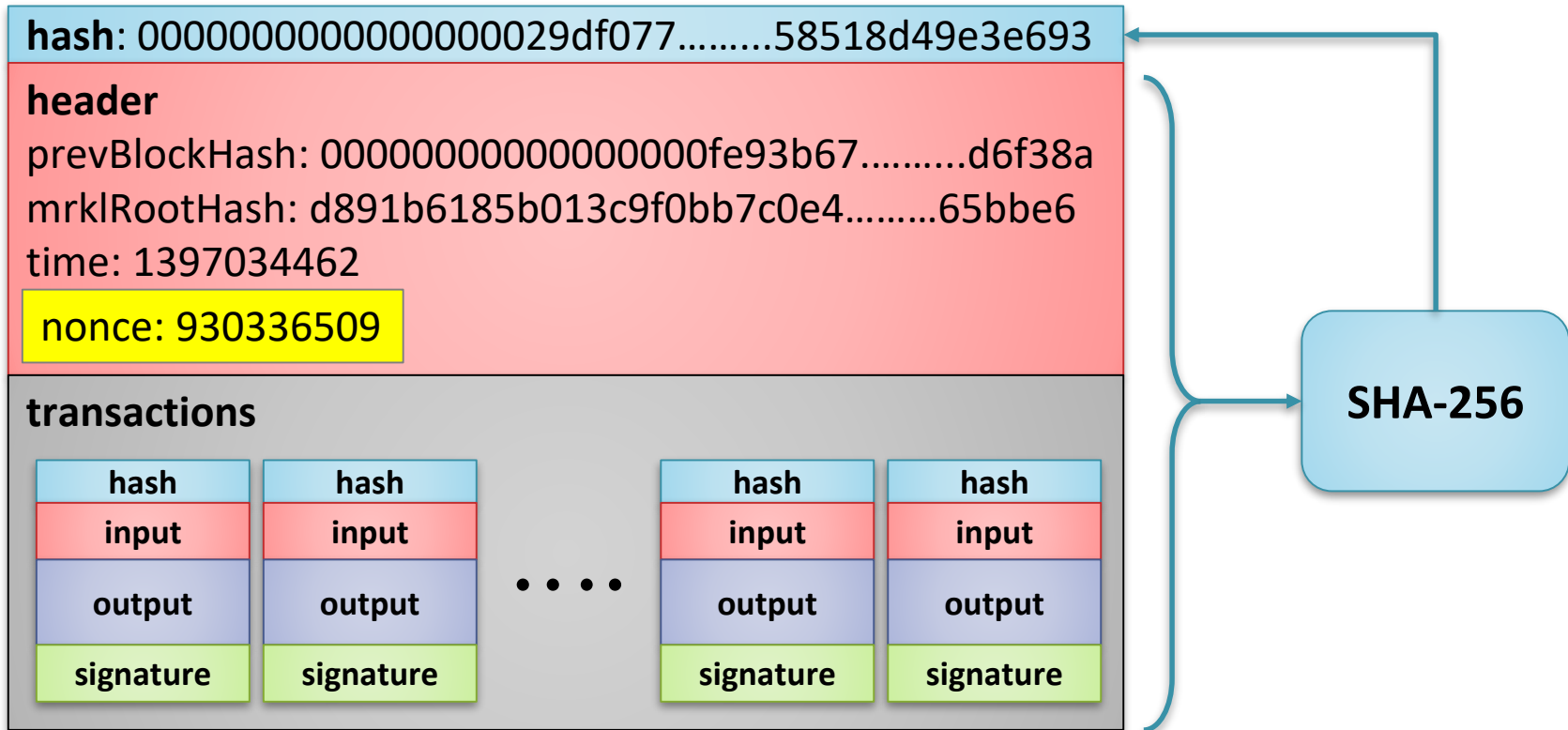


blocco non accettabile: il suo hash **non** inizia con 68 bit a 0

Trovare un blocco accettabile

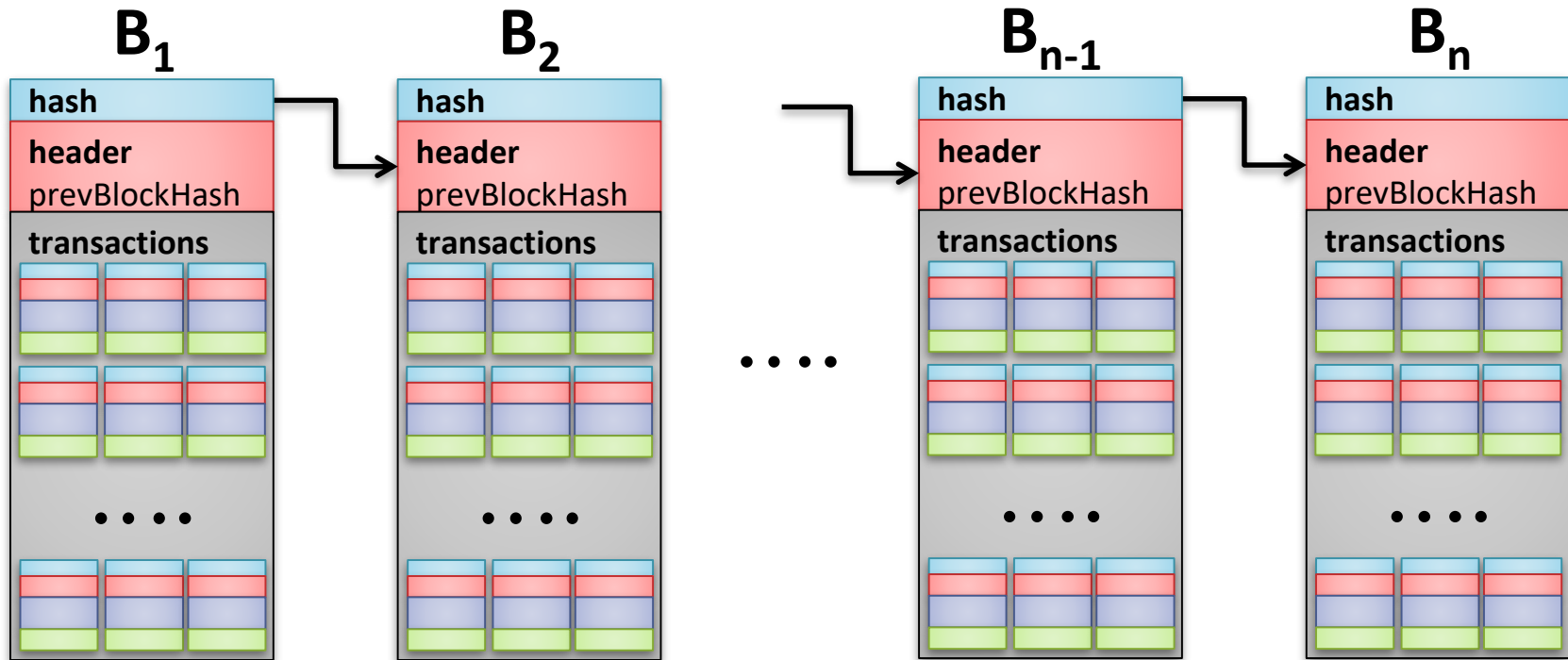
- Approccio a **forza bruta**
 - 1. poni nonce = 1
 - 2. calcola l'hash del blocco
 - 3. TEST: l'hash ottenuto inizia con almeno 68 bit nulli?
 - 3.a SE esito **positivo**: il blocco è **valido**
 - 3.b SE esito **negativo**: poni nonce = 2 e **ritorna** al punto 2.
- Necessari mediamente 2^{67} tentativi
- \Rightarrow tale processo è noto come
proof-of-work

Blocco accettabile di transazioni



time: timestamp del momento in cui
il blocco valido (o meglio il nonce) è stato individuato

Concatenazione dei blocchi



irreversibilità/integrità transazioni

una modifica dei dati di una blocco B_i

\Rightarrow **invalida B_i e tutti i blocchi successivi**

Rete P2P: algoritmo distribuito

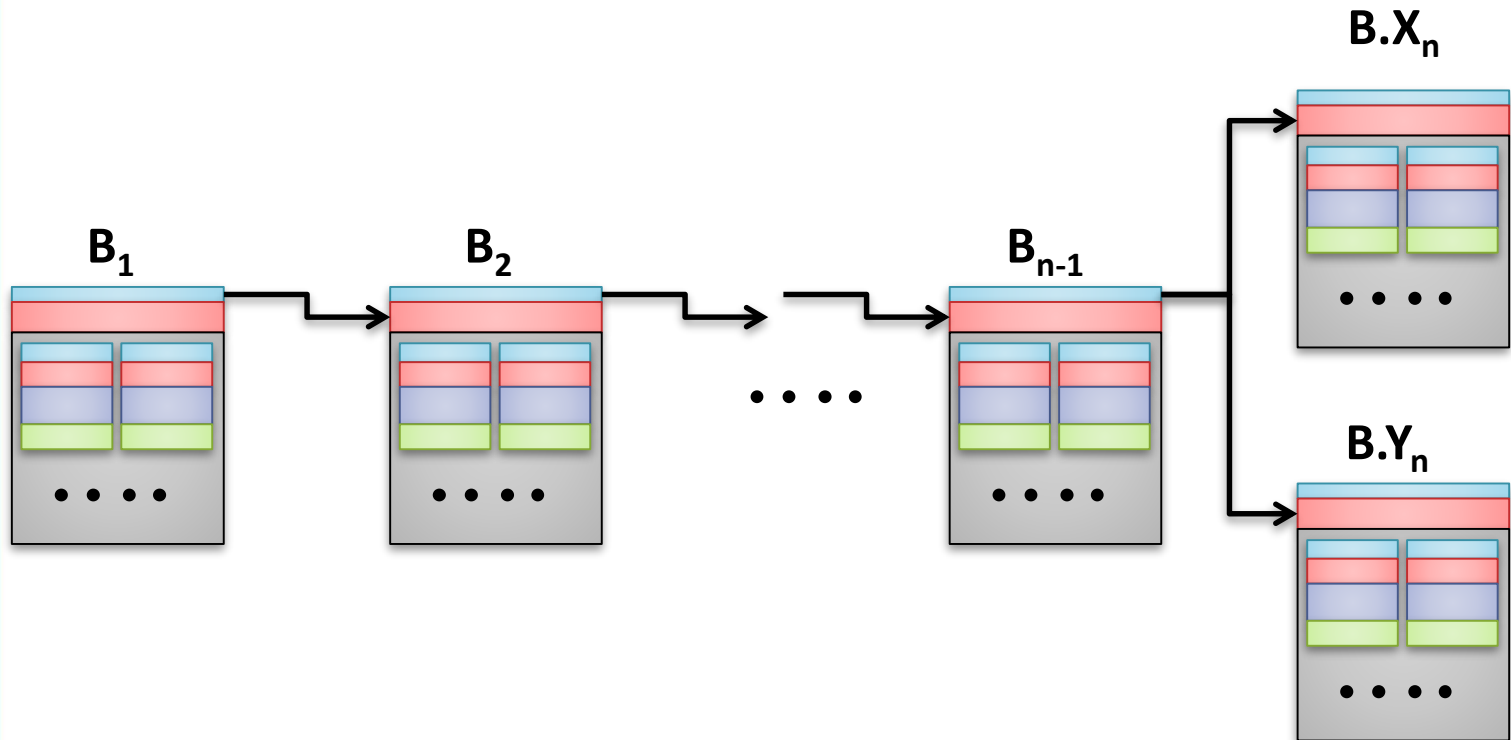
- Catena dei blocchi creata dalla rete P2P
 - 1) transazioni **recenti** (non appartenenti ad alcun blocco della catena) sono annunciate a tutti i nodi
 - 2) ogni nodo **colleziona transazioni** recenti in un **blocco**
 - 3) ogni nodo cerca una **proof-of-work** per il suo blocco
 - 4) non appena un nodo **trova** una **proof-of-work**, invia in **broadcast** il blocco a tutti i nodi

Rete P2P: algoritmo distribuito

- 5) i nodi **accettano** il blocco soltanto se **tutte** le **transazioni** che contiene sono **valide** e **non già spese**
- 6) i nodi **esprimono l'accettazione** di un blocco B_i cercando il prossimo blocco B_{i+1} e concatenando questi a B_i
 - cioè inserendo l'hash di B_i nel campo prevBlockHash del blocco B_{i+1}

Verità diverse ... catene diverse

- Due nodi X e Y potrebbero annunciare **“simultaneamente”** due versioni distinte $B.X_n$ e $B.Y_n$ del prossimo blocco della catena



Gestione biforcazioni temporanee

- In caso di **biforcazione** ogni nodo accetta **temporaneamente** come ultimo blocco quello ricevuto per primo
 - B.X_n se riceve prima B.X_n di B.Y_n
 - B.Y_n se riceve prima B.Y_n di B.X_n
- Tuttavia, **non rigetta** l'altro blocco e **temporaneamente** gestisce anche l'altro ramo
 - se riceve annunci di blocchi da concatenare a questi esegue la concatenazione

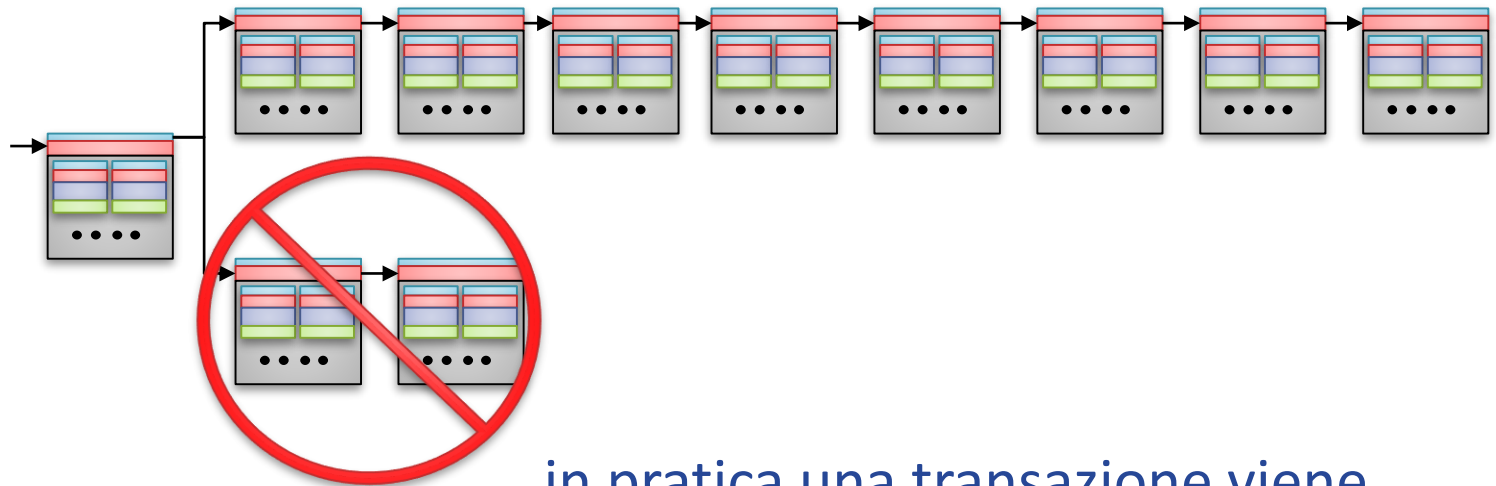
Discernere tra due verità

- Il ramo “vero” viene deciso in base alla sua **lunghezza**
- EURISTICA
 - il ramo che **cresce** più velocemente è quello **accettato**
 - il ramo (o i rami) più corto viene respinto

... sulla lunghezza delle catene

- **Ipotizzando** che i nodi **onesti** dispongano di maggiori risorse di calcolo di quelli **disonesti**
- Anche nel caso di **attacco coordinato** (Bizantino)
- Nakamoto mostra che
- la probabilità di accettare una catena con blocchi contraffatti tende a zero rapidamente se il criterio di scelta è quello della lunghezza
 - una differenza di lunghezza pari a 6,7 blocchi è ampiamente sufficiente

Pochi blocchi in più per decidere



in pratica una transazione viene **confermata** quando appartiene ad un blocco distante almeno 6,7 blocchi dall'estremità della catena

Incentivi ai nodi della rete P2P

- Commissione (Fee)
 - ogni nodo riceve una piccola commissione (o donazione) per ogni transazione associata ad una sua proof-of-work
- Emissione di nuovi BTC (Mining)
 - ogni blocco contiene una transazione speciale che emette un valore prefissato di BTC (oggi 12.5 BTC) assegnati al nodo che ha realizzato la proof-of-work

Chi *stampa* i BTC?

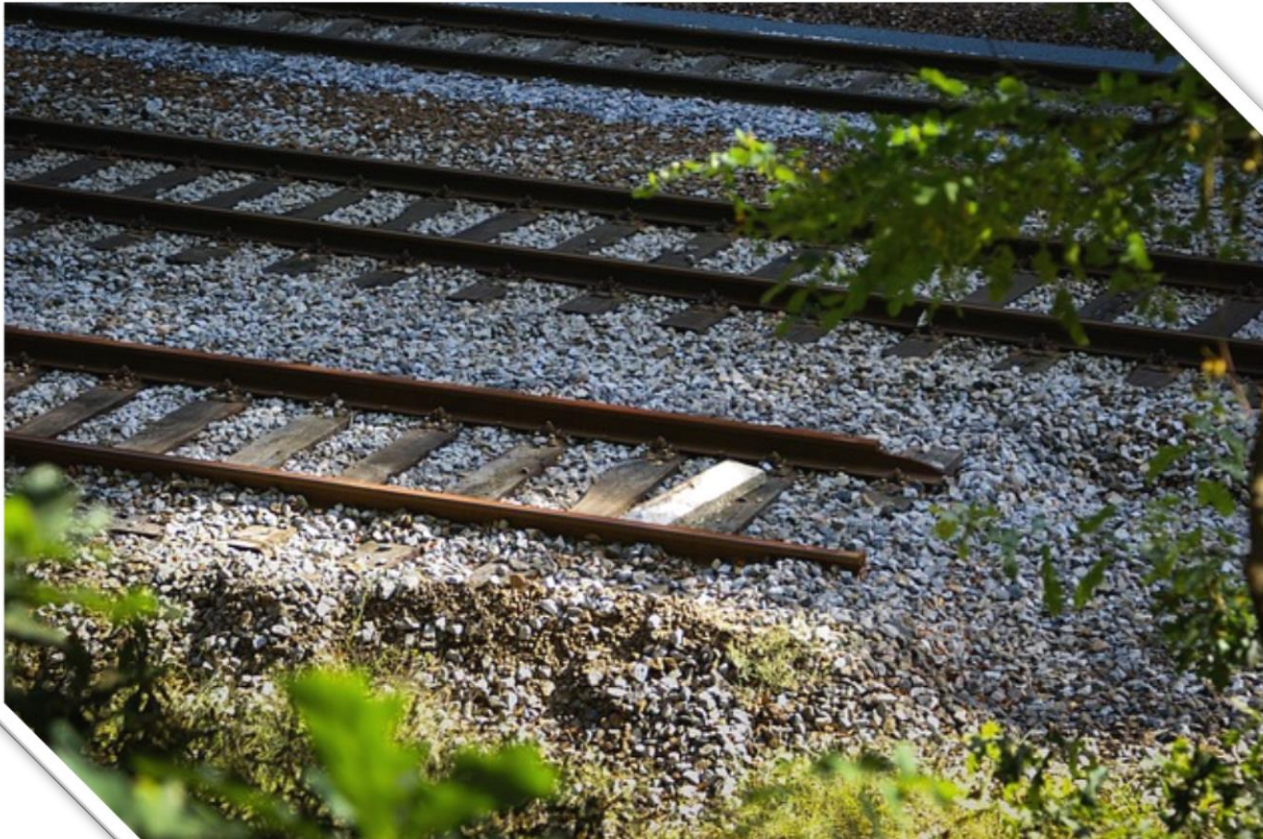
- L'emissione di BTC non dipende da decisioni “politiche”
- Già è stato stabilito il **limite massimo** di BTC che saranno emessi (**21 milioni**)
- Oggi, chi risolve una proof-of-work **emette** 12.5 BTC
 - inizialmente erano 50 BTC
 - ogni quattro anni si dimezza l'incentivo

Conclusioni

- Difficile fare previsioni sul futuro del BTC inteso come critto-valuta
- Riguardo alla tecnologia BTC, cioè la blockchain, già invece possiamo parlare di successo
 - esistono diverse varianti di blockchain
 - alcune che permettono di eseguire **task programmabili (smart contract)**

Alcune fonti consultate

- **Bitcoin: A Peer-to-Peer Electronic Cash System**
Satoshi Nakamoto
- Wikipedia (it,en)
- Bitcoin wiki <https://it.bitcoin.it/wiki>
- Bitcoin Block Explorer <http://blockexplorer.com>
- Blockchain <http://blockchain.info/it>



Grazie per l'attenzione

