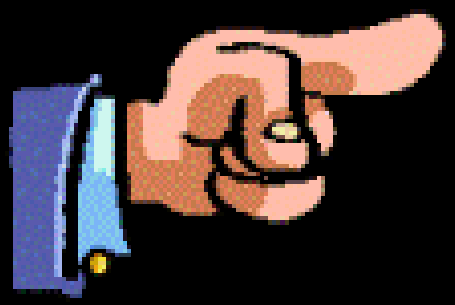
monete digitali

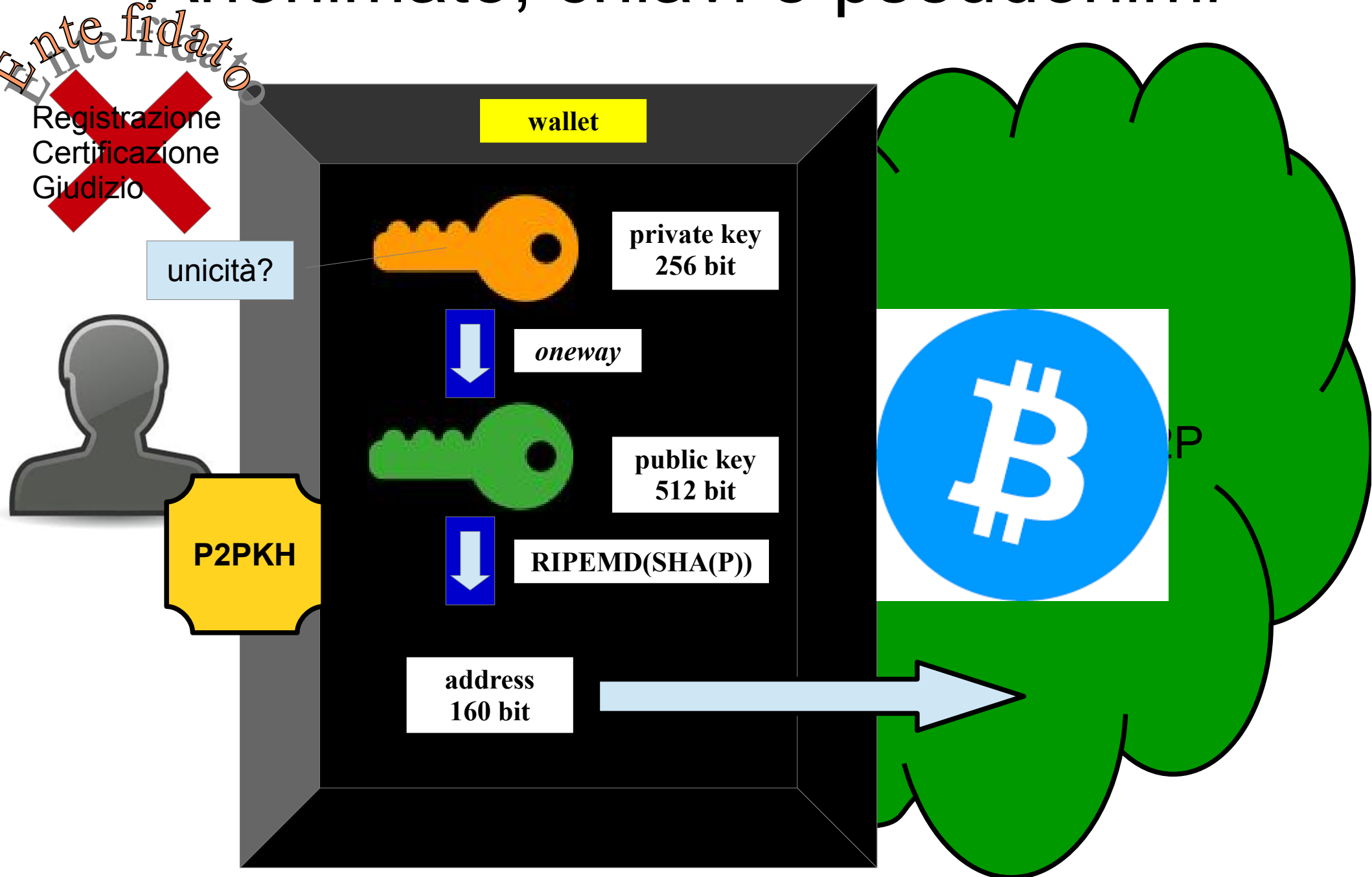
il libro master



la transazione

il portafoglio

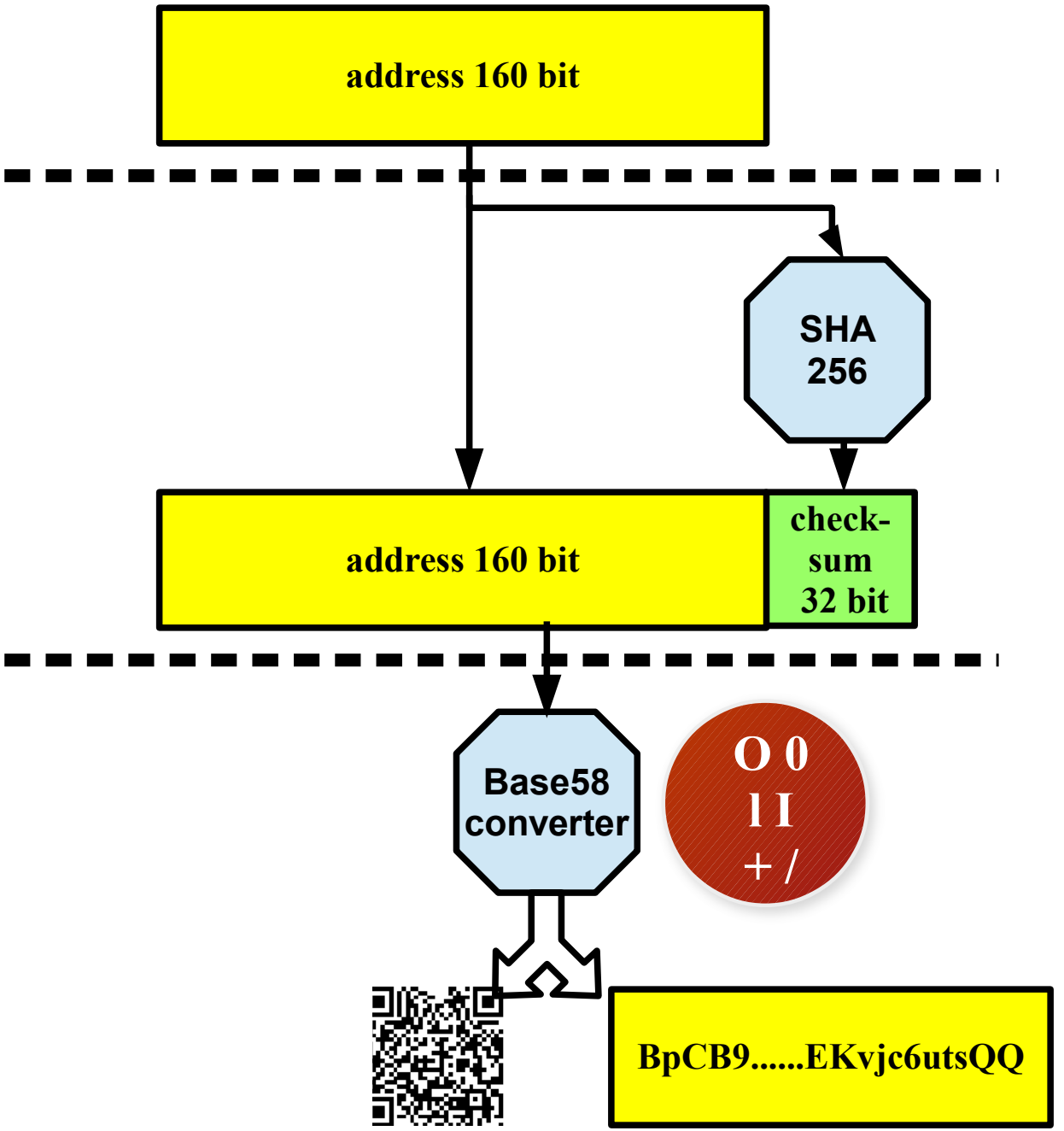
Anonimato, chiavi e pseudonimi



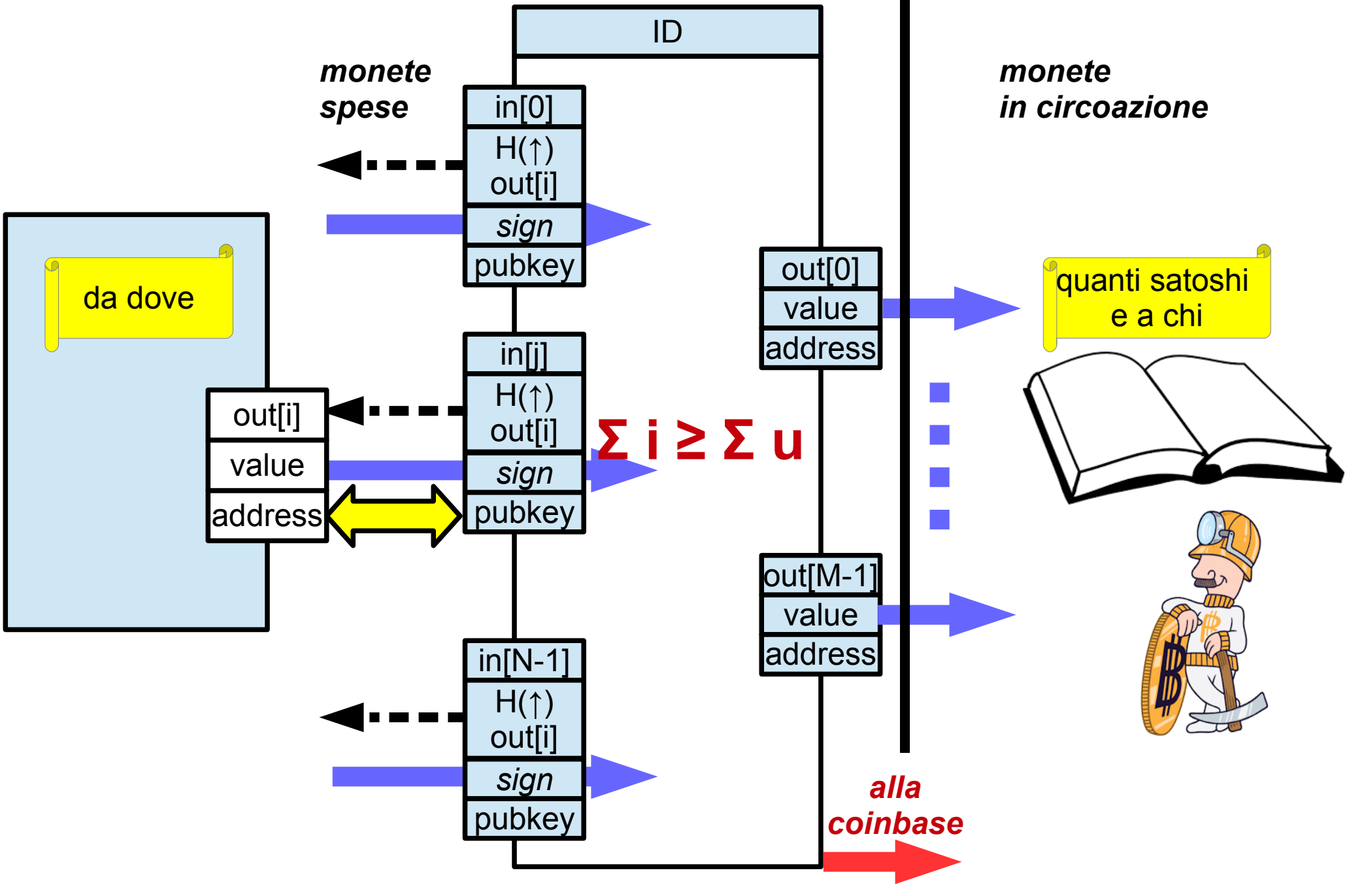
comunicazione del address

file binario

stringa di testo
QR code

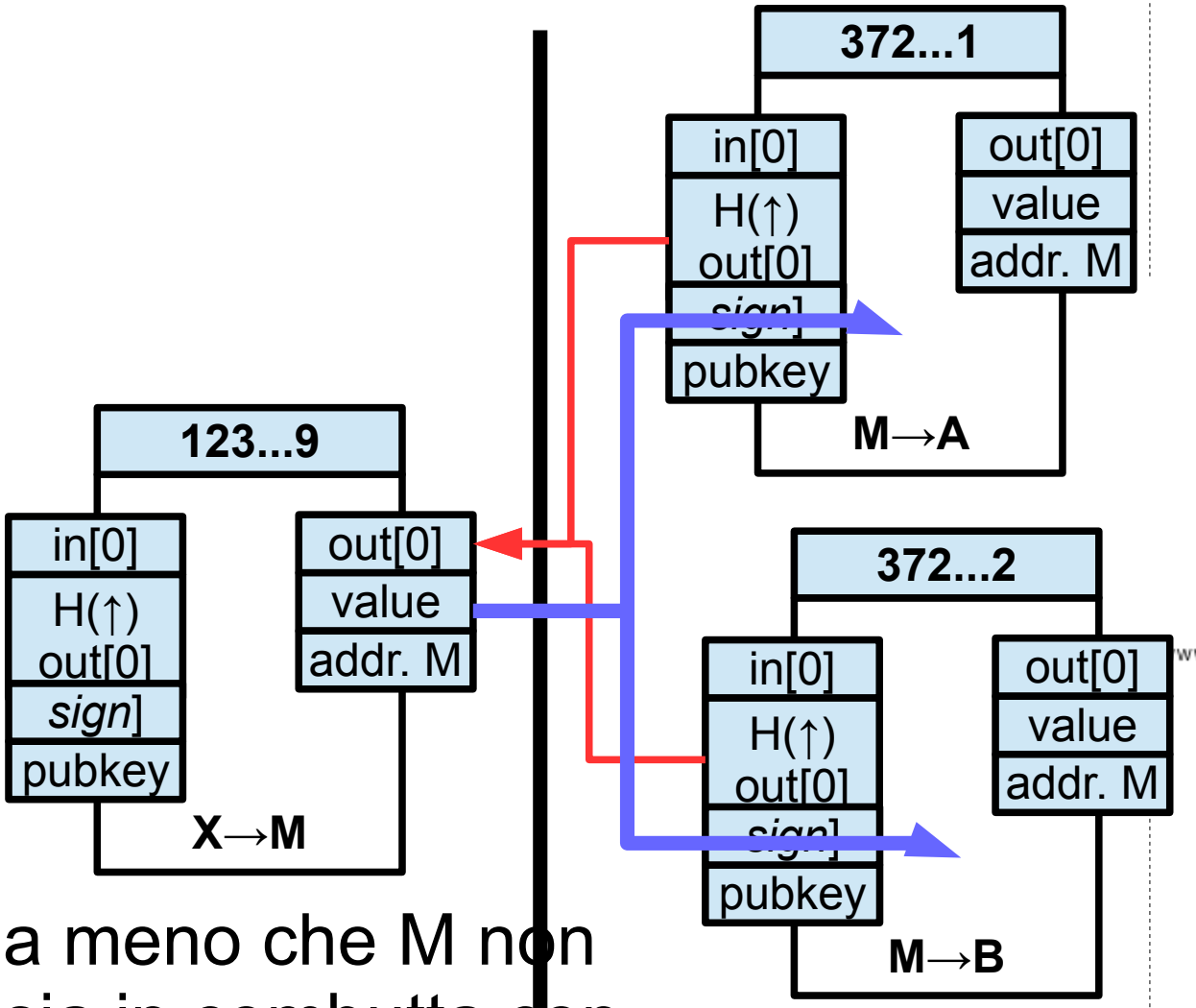


Tx P2PKH e le monete in circolazione



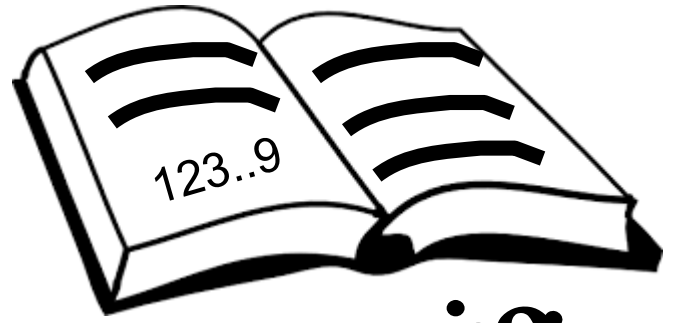
La difesa all'attacco con doppia spesa

Un truffatore M può spendere due o più volte la stessa valuta?

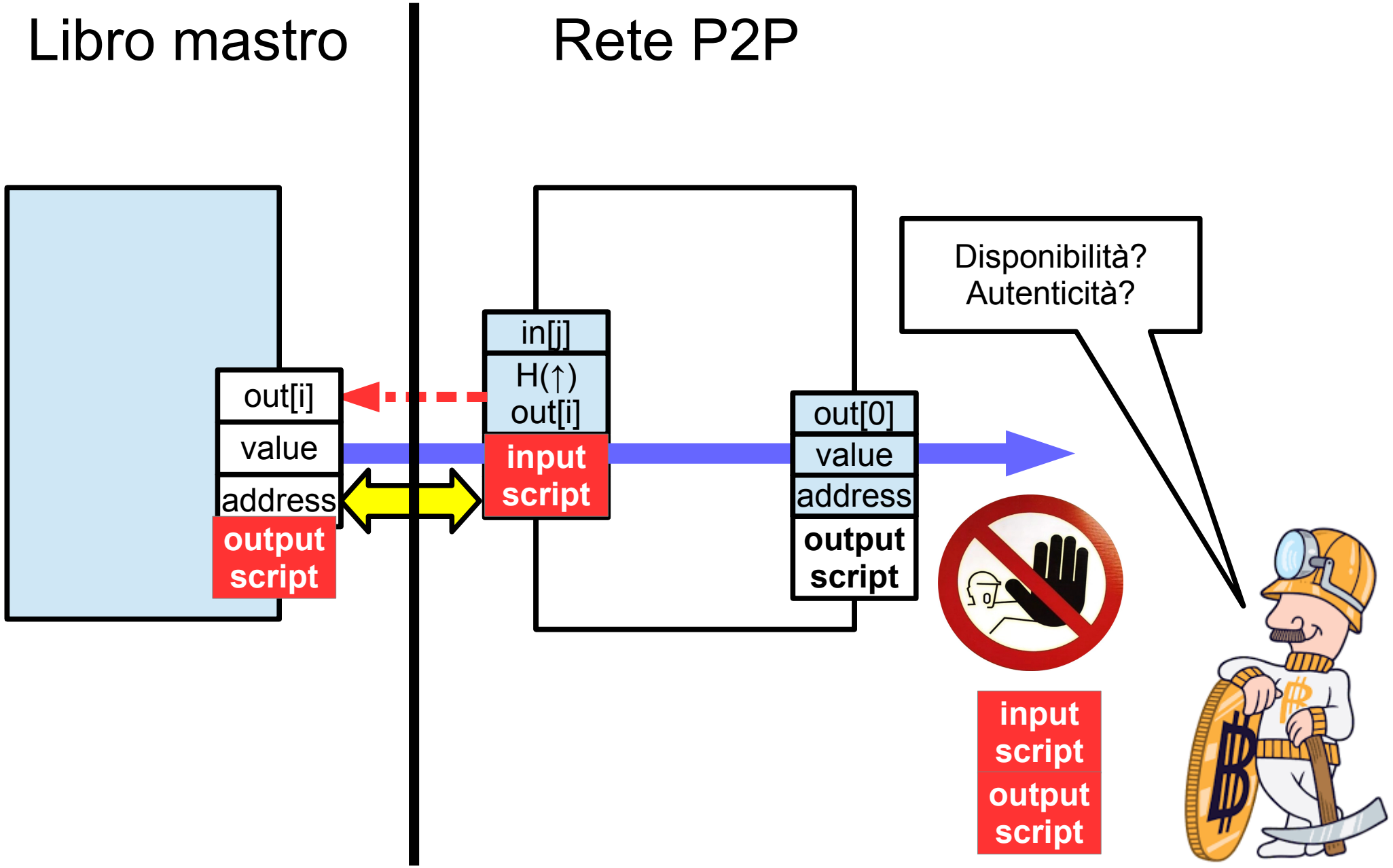


a meno che M non sia in combutta con il **51%** dei minatori

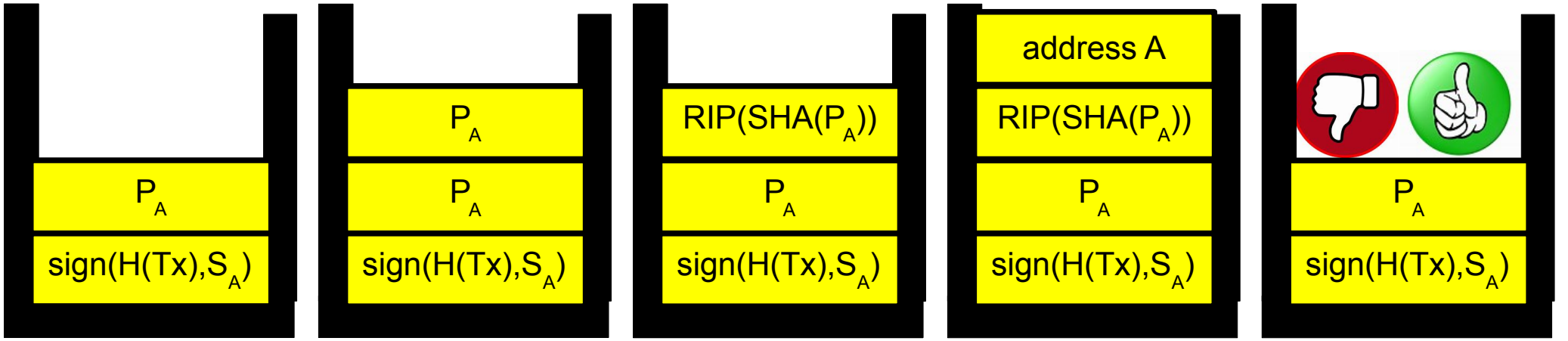
Ogni minatore ha un registro delle Tx "non ancora spese"



Tx P2PKH e gli script



Gli script, lo stack, la verifica e l'attacco



❶ ❷ ❸ ❹ ❺ ❻

Input script

<sign(H(Tx),S_A)>
<P_A>

Output script

OP_DUP
OP_HASH160
<address A>
OP_EQUALVERIFY
OP_CHECKSIG

E' possibile rubare monete di altri?

1 - Tx con uscita non spesa: facile

checksig **2 – Modifica del beneficiario: facile**

3 - P da address: difficile

4 – S da P: difficile

Pay_to_Script_Hash

P2SH - “multisig”

Regola espressa dallo script: la transazione che spenderà queste monete deve essere firmata da M delle N≥M chiavi private corrispondenti alle chiavi pubbliche: P_1,...,P_N

3 su 5: consente di dividere la responsabiità di una spesa con un voto a maggioranza

2 su 3: consente di “spendere” le monete anche se non si ha più una delle tre chiavi

2 su 2: consente di difendersi dal fatto che un intruso riesca a scoprire una delle due chiave

P2SH multisig

script: OP_M <P_1>...<P_n> OP_N OP_CHECKMULTISIG

address: RIPEMD160(SHA256(script))

input_script:

<$firma_A$>, <$firma_B$>, ….

<script>

output_script:

OP_DUP

OP_HASH

<address>

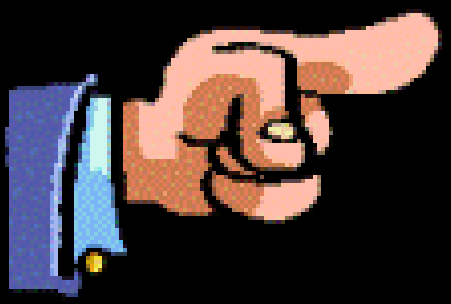
OP_EQUAL

monete virtuali

il libro master

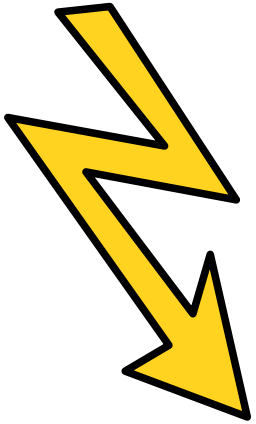
la transazione

il portafoglio



funzioni, minacce e contromisure

chiave privata & sicurezza:
- **imprevedibilità,**
- **disponibilità**
- **riservatezza**



- indovinare
- malware
- furto
- guasto
- dimenticanza

off-line

Generare S

alta entropia

Memorizzare S

ridondanza

Calcolare P, H(P)

Inviare address

Controllare conferme

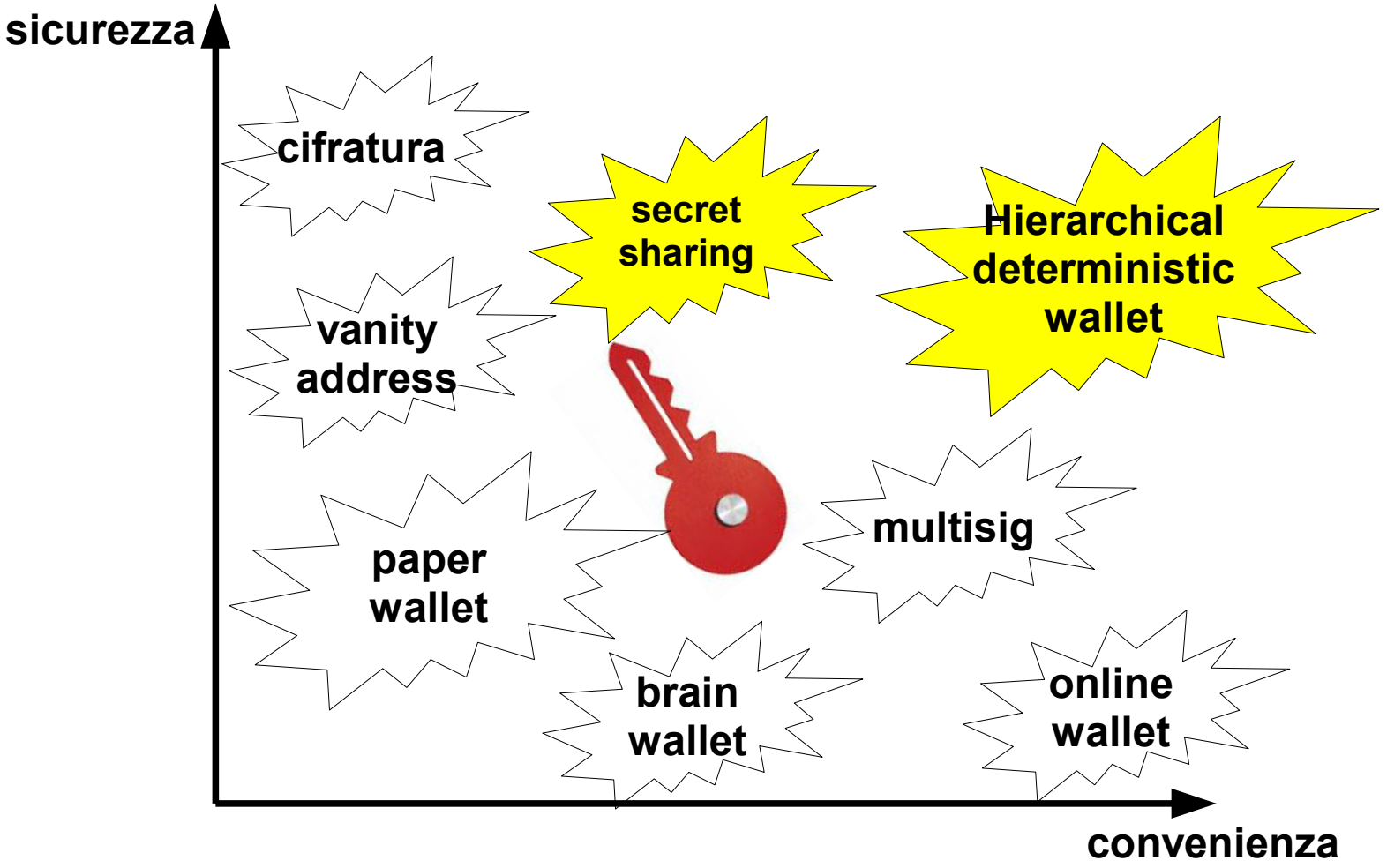
off-line

Firmare transaz.

Inviare transaz.

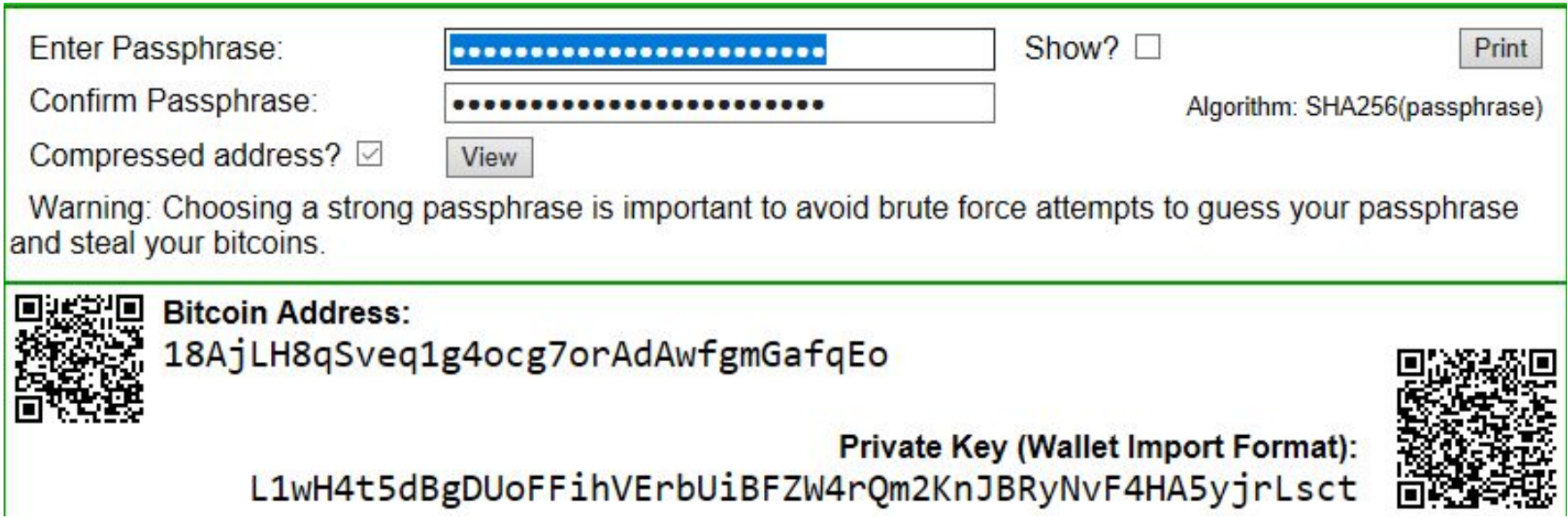
compromesso e soluzioni disponibili

Per difendere la privacy e per limitare i danni
è opportuno
che una coppia di chiavi venga usata una volta sola



Paper wallet

Brain wallet



Hierarchical Deterministic Wallet: la teoria

Proprietà notevole delle curve ellittiche:

"il prodotto scalare è **distributivo** rispetto alla somma"

Conseguenza:

"data la coppia di chiavi **S**, **P=S*G mod p** ed un numero **i**, la chiave pubblica P_i corrispondente alla chiave privata **(S+i)** si può calcolare senza conoscere **S**"

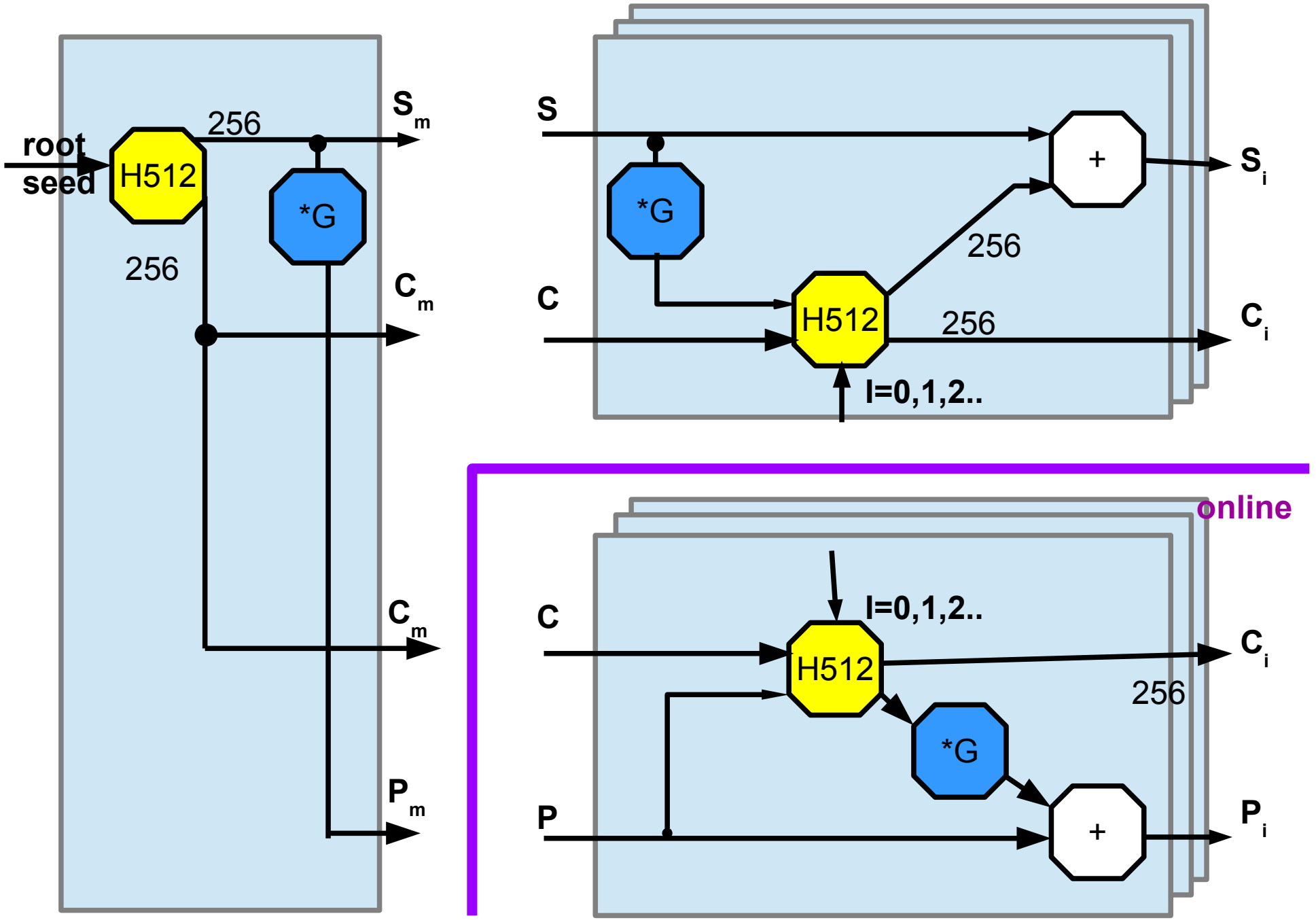
Infatti:

$$P_i=(S+i)*G \bmod p$$

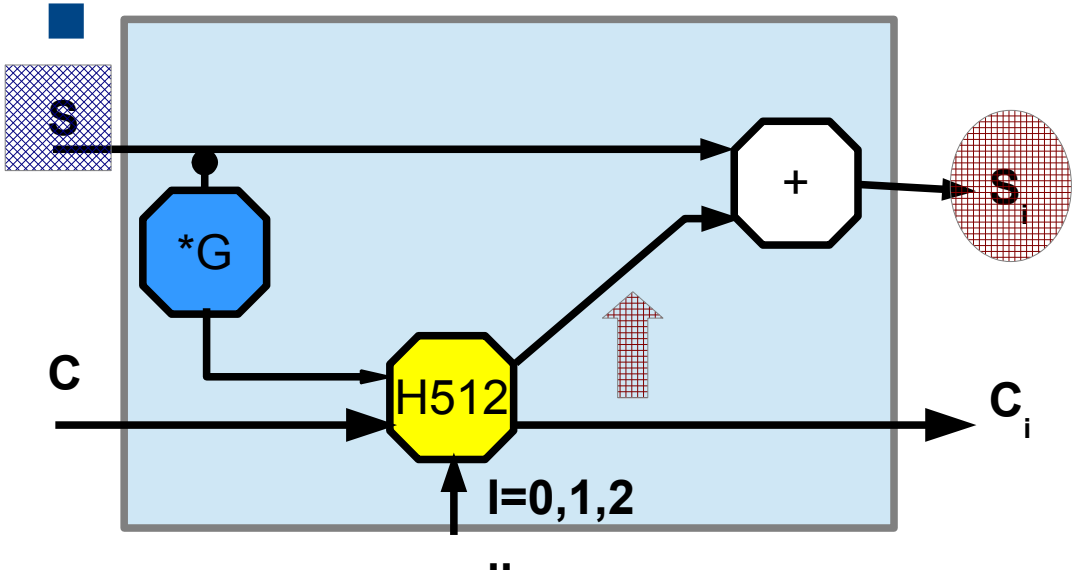
$$P_i=(S*G+i*G) \bmod p$$

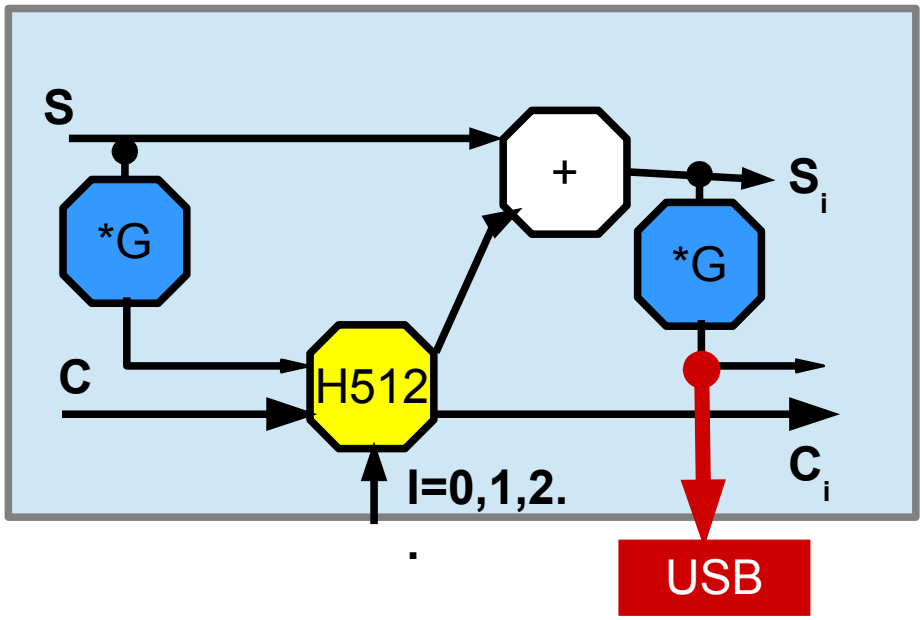
$$P_i= P+ i*G \bmod p$$

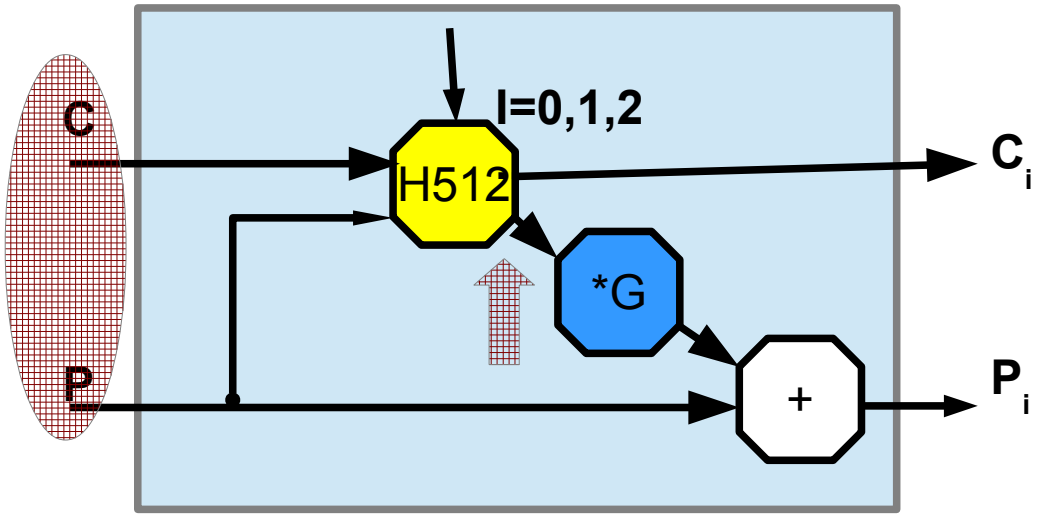
HDW: chiavi *master*, *parent*, *child*

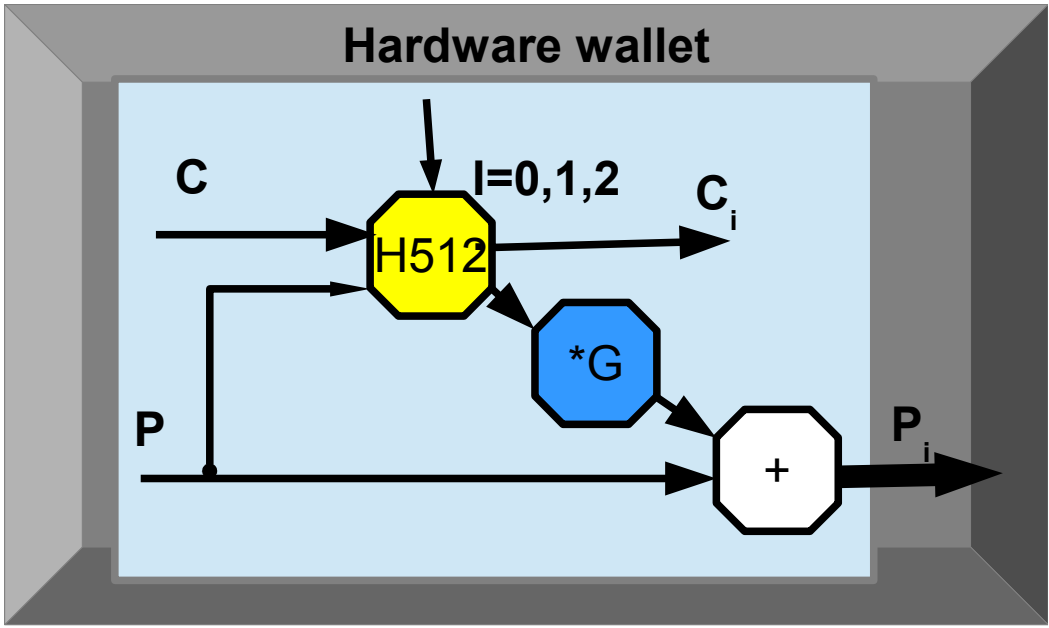


HDW: attacchi e difese

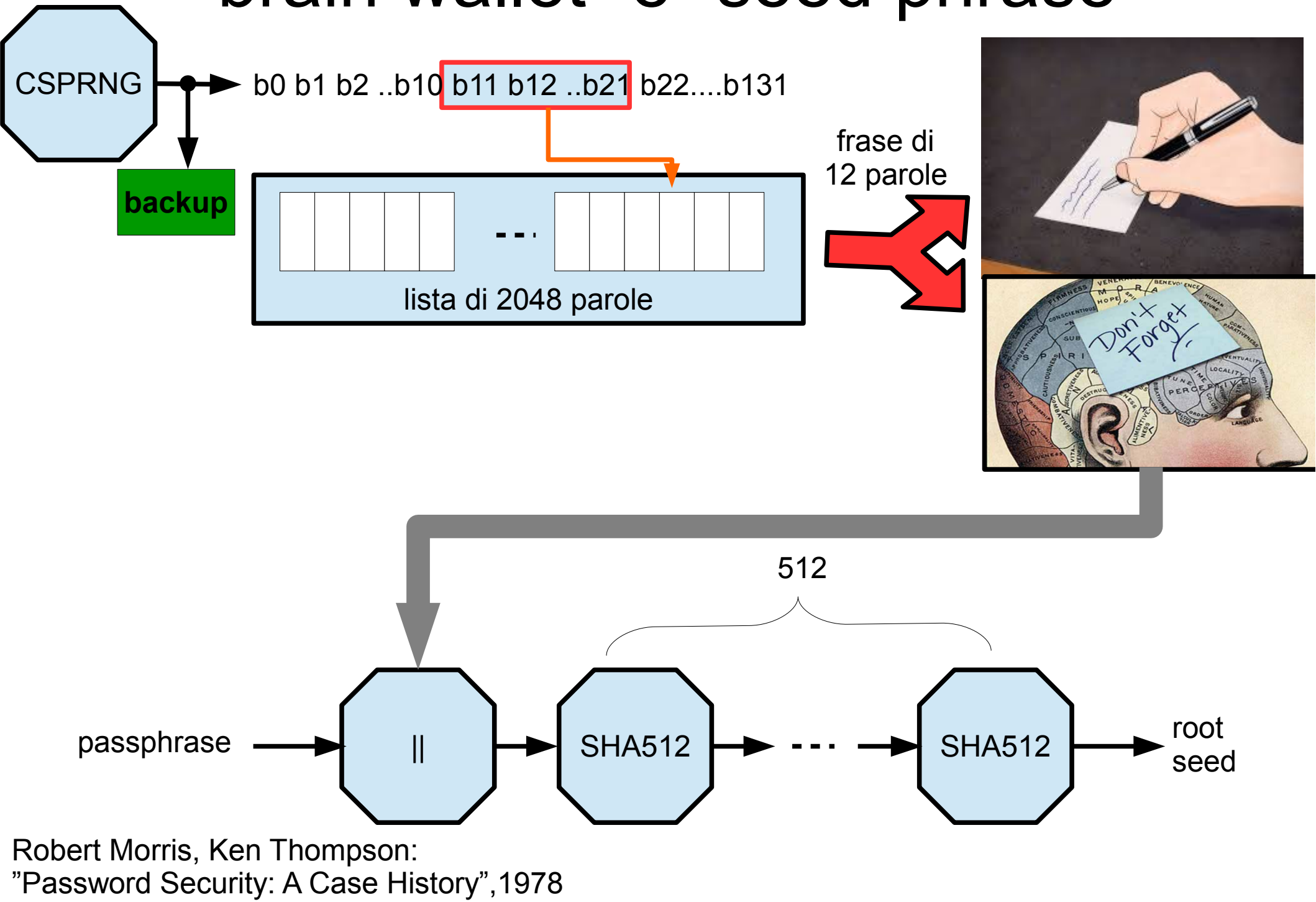








“brain wallet” e “seed phrase”



Robert Morris, Ken Thompson:
”Password Security: A Case History”,1978

Secret sharing: la teoria

Shamir A.”How to share a secret” 1979
https://it.wikipedia.org/wiki/Interpolazione_di_Lagrange

$$f(x) = a_0 + a_1 x + a_2 x^2 + .. + a_{M-1} x^{M-1} \pmod p$$

valutazione ⇓ ⇑ *interpolazione*

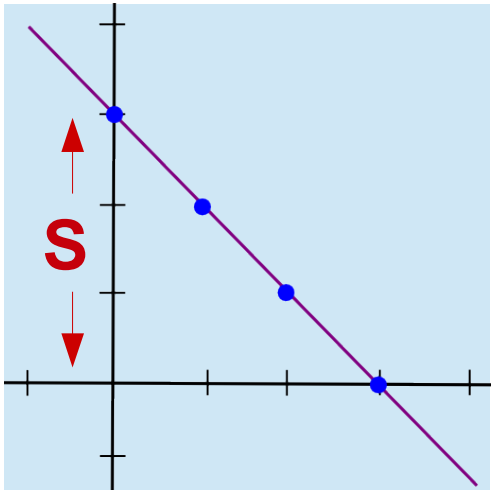
shares **f(x1), f(x2), f(x3),....,f(xM),....,f(xN)**

split wallet:
la decentralizzazione di un segreto

Dati il segreto **S** ed un numero casuale **R**,

si calcolano e si memorizzano tre o più

punti della retta **Y= S+X*R (mod p)**



La conoscenza delle coordinate X,Y di un solo punto non consente di individuare la retta.

2 su 3 (o più) -La conoscenza di due punti qualsiasi consente di ricostruire la retta e di recuperare il segreto (S è l'ordinata in corrispondenza di X=0)

- **Bitaddress.org**
- **GitHub.org**

www.bitcoin.org

https://www.blockchain.com/it/charts

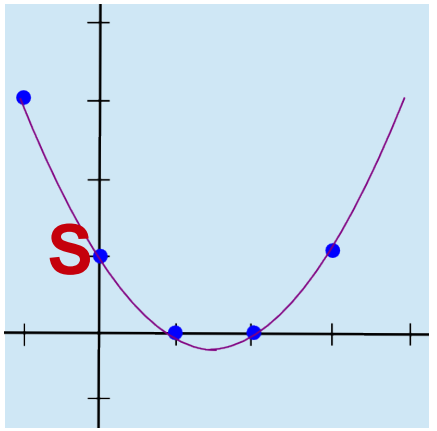
Ripasso

criptocurrencies	NO autorità, NO singolarità, SI crittografia forte
hash pointer	puntatore & impronta
blockchain	blocchi di dati connessi da hash pointer
puzzle	nonce: SHA256(block_header)≤target
hash pointer di un blocco	SHA256(block_header)
transazione garantita da Crittografia	disponibilità dell'ammontare, autenticità del documento
livello di sicurezza di SHA2, ECDSA	128 bit
address	pseudonimo del beneficiario/impronta dello script per spendere
QR code	codice a barre bidimensionale

Secret sharing

Dati il segreto **S** e due numeri casuali **R e Q**, si calcolano e si memorizzano separatamente quattro o più punti del polinomio di secondo grado

$$Y=(S+R*X+Q*X^2) \bmod p$$



- Se p è un primo molto grande, la conoscenza delle coordinate X,Y di uno o di due punti non consente di individuare S.
- La conoscenza di tre punti qualsiasi consente di ricostruire la parabola e di individuarne l'intersezione con l'asse Y

Riferimenti

E-book

A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder:
“Bitcoin and Cryptocurrency Technologies” -
https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf

A.Aantonopulos:
“Mastering Bitcoin”
https://github.com/bitcoinbook/bitcoinbook/blob/develop/book.asciidoc

http://davidederosa.com/basic-blockchain-programming/

Siti e Documenti

https://www.bitaddress.org**/**
https://bitcoin.org/en/developer-guide#transactions
https://blockchain.info/it/stats
https://en.bitcoin.it

Librerie

OpenSSL
Python
https://bitcoinj.github.io/#introduction