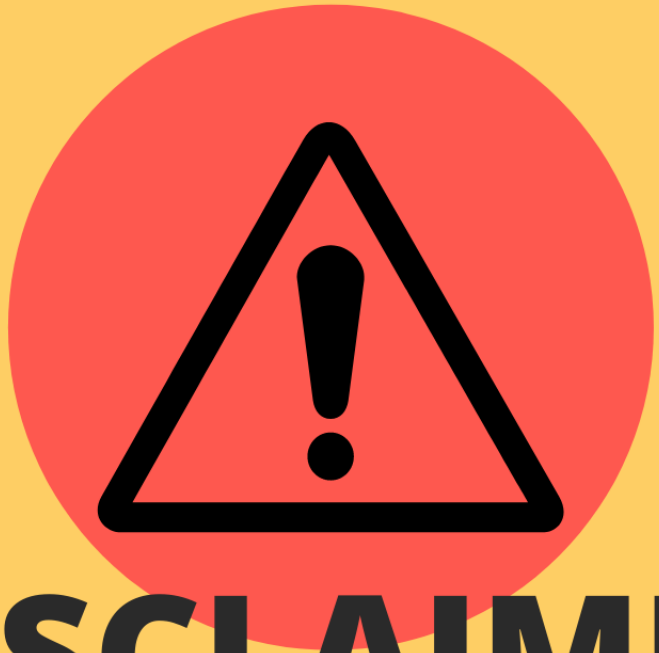

DISCLAIMER

Il materiale contenuto nel drive è stato raccolto e richiesto tramite autorizzazione ai ragazzi frequentanti il corso di studi di Informatica dell'Università degli Studi di Salerno. Gli appunti e gli esercizi nascono da un uso e consumo degli autori che li hanno creati e risistemati per tanto non ci assumiamo la responsabilità di eventuali mancanze o difetti all'interno del materiale pubblicato.

Il materiale sarà modificato aggiungendo il logo dell'associazione, in tal caso questo possa recare problemi ad alcuni autori di materiale pubblicato, tale persona può contattarci in privato ed elimineremo o modificheremo il materiale in base alle sue preferenze.

Ringraziamo eventuali segnalazioni di errori così da poter modificare e fornire il miglior materiale possibile a supporto degli studenti.

CoScienze
Associazione

OPCODE BITCOIN

Descrivere il significato del seguente script BitCoin:

2 sha256 3 swap ae7sdafdsf43sdf953asd4822348489221 equal checksig

RISPOSTA:

2: inserisce il valore 2 in cima allo stack
SHA256: Prende il valore in cima allo stack e ne fa l'hash ottenendo una stringa di 256 bit e la inserisce in cima allo stack.
3: inserisce il valore 3 in cima allo stack
SWAP: Toglie i due elementi in cima allo stack, li scambia e li inserisce nello stack in ordine opposto
ae…9221: inserisce l'hash in cima allo stack
equal: verifica che i due valori in cima allo stack siano uguali e se lo sono inserisce true in cima allo stack, false altrimenti.
Checksig: controlla la firma della transazione, ovvero controlla il contenuto dello stack. Se true la transazione procede, altrimenti viene interrotta.

Descrivere il significato del seguente script BitCoin:

HASH160 9af61346ce0aa2dffcf697352b4b704c84dcbaff EQUAL

RISPOSTA:

HASH160: Prende il valore in cima allo stack, ne fa l'hash e ottiene una stringa di 160 bit e inserisce il valore in cima allo stack.
9af…ff: inserisce l'hash in cima allo stack
EQUAL: va a controllare i due valori in cima allo stack, se i due valori corrispondono inserisce true in cima allo stack, altrimenti inserisce false.

Descrivere il significato del seguente script BitCoin:

2DUP EQUAL NOT VERIFY SHA1 SWAP SHA1 EQUAL

RISPOSTA

2DUP: Prende i due valori in cima allo stack, li duplica e li inserisce in cima allo stack
EQUAL: Prende i due valori in cima allo stack, verifica che siano uguali e mette true se lo sono, false altrimenti.
NOT: prende il valore in cima allo stack, e ne inverte il valore, in questo caso inverte il valore booleano ottenuto dall'EQUAL.
VERIFY: Verifica che in cima allo stack ci sia True e in tal caso continua, altrimenti interrompe la transazione.
SHA1: Fa l'hash dell'elemento in cima allo stack, ottenendo una stringa di 160 bit
SWAP: toglie i due elementi in cima allo stack, li scambia e li inserisce in cima allo stack in ordine opposto.
SHA1: Fa l'hash dell'elemento in cima allo stack, ottenendo una stringa di 160 bit
EQUAL: va a controllare i due valori in cima allo stack, se i due valori corrispondono inserisce true in cima allo stack, altrimenti inserisce false.

Descrivere il significato del seguente script BitCoin:

DUP HASH160 62e907b15cbf27d5425399ebf6f0fb50ebb88f18 EQUALVERIFY CHECKSIG

RISPOSTA:

DUP: Prende l'elemento in cima allo stack, lo duplica e lo inserisce in cima allo stack
HASH160: Fa l'hash dell'elemento in cima allo stack, e inserisce in cima allo stack una stringa di 160 bit
62…f18: inserisce l'hash in cima allo stack
EQUALVERIFY: Controlla se i due elementi in cima allo stack sono uguali, se sono uguali inserisce true in cima allo stack, altrimenti false, se restituisce true la transazione è valida.
CHECKSIG: Controlla la firma della transazione in input, se è true la transazione procede altrimenti viene interrotta.

Descrivere il significato del seguente script BitCoin:

2 3 ADD 6 EQUAL

RISPOSTA:

2: Inserisce il valore 2 in cima allo stack (stato stack = 2)
3: Inserisce il valore 3 in cima allo stack (stato stack = 2 - 3)
ADD: Effettua una somma tra i due elementi in cima allo stack (che vengono anche consumati) e mette il risultato in cima allo stack (stato stack = 5)
6: Inserisce il valore 6 in cima allo stack (stato stack = 5 - 6)
EQUAL: Verifica che i due elementi in cima allo stack siano uguali, mette true se sono uguali, false altrimenti.

Descrivere il significato del seguente script BitCoin:

<Bob's signature> <Bob's public key> OP_DUP OP_HASH160 <Bob's public address> OP_EQUALVERIFY OP_CHECKSIG

<Bob's signature>: Mette la firma di Bob in cima allo stack
<Bob's public key>: Mette la chiave pubblica di Bob in cima allo stack
OP_DUP: Prende l'elemento in cima allo stack e lo duplica, ovvero la chiave pubblica di Bob, e inserisce il duplicato in cima allo stack
OP_HASH160: Fa l'hash dell'elemento in cima allo stack e inserisce in cima allo

stack la stringa di 160 bit corrispondente
<Bob's public address>: Inserisce l'indirizzo pubblico di Bob in cima allo stack
OP_EQUALVERIFY: Verifica se i due valori in cima allo stack sono uguali, se lo sono inserisce true in cima allo stack, false altrimenti, nel caso sia true la transazione è valida
OP_CHECKSIG: Verifica la firma della transazione,quindi il contenuto dello stack, se è true la transazione procede altrimenti viene interrotta,l'elemento true o false viene inserito in cima allo stack.