Alessio Barnini | Alessandro Aglietti

Bitcoin

199 domande

BITCOIN

199 domande

Alessio Barnini

Alessandro Aglietti

Codice ISBN: 978-10-986-12634

2

3

INDICE

61.

Che cosa è un sistema centralizzato?

.....
19

62.

Che cosa è un sistema decentralizzato?

.....
19

63.

Che cosa è un sistema distribuito?

.....
19

64. Che cosa sono i BIP?

Dove si legge il titolo de “The Times” ?

.....
22

93.

Posso scrivere del testo sulla blockchain?

.....
22

94. Che cosa è il Proof of Work?

.....
22

95.

Quando venne usato per la prima volta l’algoritmo PoW?

8

Premessa

–

Viviamo in una società in continua evoluzione, internet è entrato in maniera prepotente

nelle nostre vite, l'email è diventata uno strumento indispensabile per la comunicazione, il

mondo dei pagamenti sta cambiando, spazzando via il vecchio per far spazio al nuovo.

Siamo convinti che Bitcoin è il cambiamento che la società sta aspettando da tempo, non c'è

più tempo per essere analfabeti, non è ammissibile partecipare passivamente.

La vera rivoluzione deve iniziare dentro di noi.

La sfida che ci siamo prefissati è stata

quella di rispondere esaustivamente utilizzando poche

righe, chiarendo dubbi ai neofiti e incuriosendo i più esperti.

Siamo però consapevoli che domande più tecniche hanno bisogno di risposte più ampie, per

questo consigliamo il libro “Bitcoin dalla teoria alla pratica1” che affronta in modo

dettagliato il protocollo con esempi pratici e reali.

Salutate il presente, benvenuti nel futuro.

1 https://amzn.to/2Xwu7BW

9

LOADING...

Ho trovato un errore nel vostro bellissimo libro!

Accidenti! Dai perdonaci :)

Abbiamo predisposto un metodo per segnalare errori, oppure se vuoi contribuire a

migliorare i contenuti di questo libro.

Per inviare la tua segnalazione puoi creare una issue su GitHub dal seguente

indirizzo

https://github.com/bitcoin-dalla-teoria-alla-pratica/errata-corrige-e-sorgente-

esempi/issues/new/choose

Non sai cosa sia una “issue su GitHub”?

Sono simili a dei messaggi in un forum. Quando viene creata una issue si aprirà una

discussione in merito.

Inoltre, al seguente indirizzo potrai consultare tutta l’errata corrige.

https://github.com/bitcoin-dalla-teoria-

alla-pratica/errata-corrige-e-sorgente-esempi/tree/master/errata/199

Buona caccia all’errore!

Contatti

LinkedIn: http://bit.ly/2H38ovs

Twitter: https://twitter.com/satoshiwantsyou

Facebook: http://bit.ly/2Lq4f96

Medium: http://bit.ly/2FvflnR

Sito ufficiale: https://www.corsobitcoin.com

Email: corsobitcoin@gmail.com

Ringraziamenti

- Caterina Bonistalli (https://www.linkedin.com/in/caterina-bonistalli-ba5267162)

per la revisione.

- Stefania Pizzichi (https://www.linkedin.com/in/stefaniapiz
per la copertina.

- Felice Rocchitelli (https://www.linkedin.com/in/felice-rocchitelli) per la revisione

tecnica e preziosi spunti.

10

11

LIVELLO BASE

1. Che cosa è Bitcoin?

Bitcoin con la B maiuscola si identifica il protocollo. Come spiegato nel whitepaper2 di

Satoshi Nakamoto, Bitcoin è un sistema di pagamento peer to peer il quale permette di

inviare denaro senza un’istituzione finanziaria.

2. Che cosa è bitcoin?

bitcoin con la b minuscola si intende la criptovaluta.

3. Che cosa è un protocollo?

Il protocollo è un insieme di regole che i partecipanti alla rete devono rispettare per farne

parte.

4. Chi ha creato Bitcoin?

Probabilmente è la domanda a cui non troveremo mai risposta. Il merito è attribuito a

Satoshi Nakamoto, ma nessuno conosce con certezza la sua identità.

Molti attribuiscono al movimento cypherpunk l'invenzione di Bitcoin.

5. Che cosa è un movimento cypherpunk?

È un movimento che si pone come obiettivo quello di migliorare la privacy delle persone

tramite la crittografia al fine di ottenere un cambiamento socio-politico.

6. Chi sono i padri del movimento cypherpunk?

- Julian Assange.

- Adam Back.

- David Chaum.

- Wei Dai.

- Hal Finney.

- John Gilmore.

- Dave Kleiman.

- Tim C. May.

- Nick Szabo.

- Phil Zimmermann.

2 http://bit.ly/2PWpyh2

7. Quanti anni ha Bitcoin?

Bitcoin nasce nel 2009, al momento della stesura del libro ha 10 anni. Il primo blocco è stato

emesso il 3 gennaio 20093.

8. Perché Bitcoin non ha un ente centrale?

È proprio uno degli scopi di Bitcoin non avere un ente centrale per creare una nuova

economia indipendente senza un unico punto manipolabile.

9. Che cosa è una rete P2P?

Possiamo definire P2P (peer to peer) una rete resiliente e decentralizzata, dove non ci sono

nodi “speciali”, tutti hanno gli stessi diritti e doveri. I nodi sono i partecipanti alla rete.

10. Bitcoin è anonimo?

No. Bitcoin garantisce lo pseudo-anonimato. Ciò permette di raggiungere, in condizioni

ideali di utilizzo, un elevato livello di privacy.

11. Quanti bitcoin sono in circolazione?

Al momento della stesura del libro (maggio 2019) sono in circolazione più di 17 milioni di

bitcoin4.

12. Chi sviluppa Bitcoin?

Bitcoin è opensource. Chiunque può proporre modifiche e correggere errori. In questo

momento ci sono state 621 persone che hanno contribuito al codice.5

13. Quanti bitcoin possono essere emessi?

Il numero massimo di bitcoin che saranno emessi è definito nel protocollo ed è 21 milioni. Si

stima che l'ultimo bitcoin verrà emesso nel 2140.

14. Perché Bitcoin ha un'emissione limitata?

Perché lo scopo dei suoi progettisti era quello di riprodurre l'idea di scarsità reale, tipica di asset di valore come le commodities (gold, silver, .), nel mondo digitale.

15. È possibile spegnere Bitcoin?

Il protocollo Bitcoin è in esecuzione su molti computer sparsi nel mondo. Per spegnerlo

nessuno di questi computer dovrebbe essere connesso alla rete.

3 http://bit.ly/2vOx7gr

4 http://bit.ly/2LAE3J4

5 http://bit.ly/2He7Kdp

16. Quanti computer sostengono la rete Bitcoin?

In questo momento (5 giugno 2019) ci sono più di 95006 computer (nodi) che risultano

pubblicamente attivi.

17. Che cosa è la crittografia?

Crittografia proviene dal greco e significa *scrittura nascosta*.

Può essere usata per cifrare messaggi, quindi nasconderli, oppure può essere usata per

verificare che un messaggio non sia stato manomesso e che sia stato inviato dal mittente

voluto.

18. Quale tipo di crittografia usa Bitcoin?

Bitcoin utilizza la crittografia a chiave pubblica, conosciuta anche come crittografia

asimmetrica.

19. Quanto vale 1 bitcoin?

In questo momento vale 6000$. (10 maggio 2019)

20. Chi determina il prezzo di bitcoin?

Il prezzo, come per qualsiasi bene

all'interno di economie di mercato, è determinato dalla

domanda e dall’offerta.

21. Che cosa è un exchange?

Un exchange è una piattaforma di scambio dove è possibile acquistare e scambiare bitcoin.

22. Chi sono i partecipanti della rete Bitcoin?

I partecipanti alla rete Bitcoin sono i nodi, chiunque può farne parte.

23. Che cosa è la blockchain?

È l’insieme dei blocchi che sono stati creati dai miner.

Possiamo immaginare la blockchain come una struttura dati ordinata temporalmente dove

ogni blocco è collegato al blocco precedente.

24. Chi possiede la blockchain?

Ogni nodo che partecipa alla rete ha l'esatta copia della blockchain completa.

25. Come posso scaricare la blockchain?

Il metodo più semplice è scaricare il

software messo a disposizione per questo scopo: Bitcoin

Core7.

6 http://bit.ly/2JYWmWv

7 http://bit.ly/2VDNQTh

26. Quanto tempo occorre per scaricare la blockchain?

Come puoi immaginare dipende dal tipo di connessione che hai a disposizione. In media si

va da un minimo di 1 giorno al massimo

di 7 giorni.

27. Che computer devo avere per scaricare la blockchain?

Non serve un computer particolare, serve invece spazio libero sul tuo hard disk. La

blockchain completa è di circa 200 gigabyte. (5 giugno 2019)

28. Che cosa è un blocco?

Un blocco è un contenitore di dati che aggrega transazioni e altre informazioni. Il blocco è

parte integrante della blockchain.

29. Che cosa contiene un blocco?

Più del suo 60% di spazio è occupato dalle transazioni. Contiene altre informazioni utili

come la data e un riferimento al blocco precedente.

30. Chi emette i nuovi bitcoin?

Il protocollo Bitcoin prevede la creazione di nuovi bitcoin ogni qual volta un nuovo blocco

viene aggiunto alla Blockchain. I nuovi bitcoin, così creati, vengono assegnati come

ricompensa al nodo che ha aggiunto il blocco (miner).

31. Bitcoin è legale?

Nella maggior parte degli stati è ritenuto legale, Italia8 compresa.

32. Bitcoin è una bolla?

No, Bitcoin è una nuova tecnologia. Le bolle sono quelle che dobbiamo farci controllare dal

dermatologo :)

33. Qual è il vantaggio di Bitcoin?

La possibilità di spostare il proprio

patrimonio in piena autonomia, quindi senza

intermediari e senza spese di commissione elevate.

34. Possiamo pagare il caffè con bitcoin?

Si, già dal 2009. La community Bitcoin sta lavorando per migliorare i micro-pagamenti con

la tecnologia lightning network.

35. Bitcoin e blockchain sono la stessa cosa?

No. Hanno una relazione molto stretta.

Bitcoin è il protocollo, e la blockchain è la collezione

dei blocchi che contengono le transazioni.

8 http://bit.ly/30zq74p

36. Perché la blockchain è immutabile?

La blockchain è composta da blocchi, ogni blocco ha la sua impronta digitale e quella del suo

predecessore. Se un blocco della blockchain viene alterato la sua impronta digitale cambia

compromettendo la coerenza e l'integrità delle informazioni presenti nella catena. Il

protocollo predispone un serie di regole che rendono economicamente proibitiva la

possibilità di modifica unilaterale (senza consenso) della catena.

37. Come posso ottenere bitcoin?

Ci sono molteplici modalità per ottenere bitcoin. Ad esempio, è possibile acquistarli tramite

gli exchange online, possono essere ricavati come ricompensa per l'attività

di mining,

oppure possono essere comprati fisicamente tramite appositi ATM.

38. Che cosa posso fare con i bitcoin?

Ad oggi non è diffusa come la moneta cartacea, ma è comunque possibile comprare beni e

servizi.

39. Dove tenere i bitcoin?

I bitcoin vengono conservati nel wallet. Questa affermazione non è del tutto corretta, perché

i wallet contengono le nostre chiavi private che ci rendono proprietari dei nostri bitcoin.

40. Che cosa è un wallet?

Un wallet permette di conservare le chiavi private. Tali chiavi private mi permettono di

spendere bitcoin ad esse collegati.

41. Che cosa è un hardware wallet?

È molto simile a una pennetta usb. Il vantaggio, in termini di sicurezza, rispetto ai classici

(hot) wallet è quello di avere le chiavi

su un dispositivo che risulti per la maggior parte del

tempo offline.

42. Che cosa è un wallet online?

È un software che gestisce le nostre chiavi private online tramite un sito internet.

43. Che cosa è un software wallet?

Sono programmi per laptop, pc desktop, e smartphone. Uno di questi è Bitcoin Core9.

44. Che cosa è un paper wallet?

Un vero e proprio wallet di carta. La chiave privata e la chiave pubblica sono scritte sopra a

un foglio. È possibile proteggere la chiave privata con una password.

9 http://bit.ly/2VDNQTh

16

45. Mi possono rubare i bitcoin?

Sì, qualora ti venissero sottratte le chiavi private collegate ai tuoi bitcoin. Tuttavia, vi sono diversi metodi per minimizzare il rischio di furto. Per esempio, proteggendo le chiavi private

con una password.

46. Come trasferisco bitcoin?

Tramite i software wallet abbiamo la possibilità di trasferire i bitcoin dal nostro address

all'address del destinatario.

47. Che cosa è una chiave privata?

La chiave privata è l'elemento fondamentale per creare la firma digitale. Tramite la chiave

privata possiamo testimoniare al network di essere i possessori di un certo address. Deve

rimanere segreta. Potete paragonarla al vostro PIN del bancomat, chi ne entra in possesso

può utilizzare i fondi collegati.

48. Che cosa è un address?

Potete immaginare l'address come il vostro IBAN. È l'indirizzo da comunicare per ricevere

bitcoin.

49. Che cosa è un vanity wallet?

Vanity wallet è un wallet che permette di creare un address personalizzato, ad esempio

1BarnoCmwrfRUi5Nmq8957dWdtqE5C

50. Che cosa è la fee?

La fee è la commissione da pagare per effettuare la transazione. Non è obbligatoria, anche se

fortemente consigliata per completare la transazione.

51. Chi paga la fee?

Il mittente.

52. Quanto costa spostare 1000 bitcoin?

La fee della transazione non si basa sull'ammontare di bitcoin che vogliamo

spostare, ma

dalla dimensione - in byte - della transazione che stiamo effettuando. Tale dimensione è

condizionata dal numero di transazioni in mio possesso (UTXO) che devo utilizzare per

arrivare all’importo voluto e dal numero di destinatari che inserisco all'interno della

transazione stessa.

53. Come posso verificare la transazione?

Potete verificare la transazione tramite i servizi di block explorer10. Solitamente i software

wallet comunicano la transazione id (txid) o forniscono direttamente il link. Se la

transazione è confermata significa che è andata a buon fine. Una transazione può essere

considerata sicura al 100% dopo la 6° conferma.

10 http://bit.ly/2Jdq4XE

54. Che cosa sono le 12-24 parole del wallet?

Tali parole sono utilizzate per derivare una serie di chiavi private e chiavi pubbliche.

Possiamo immaginarle come una super password per i nostri bitcoin. Prende il nome di seed

phrase.

55. Perché devo tenere al sicuro la seed phrase?

Tramite la seed phrase è possibile recuperare tutte le chiavi private e quindi prendere

possesso dei bitcoin ad esse collegati.

56. Che cosa succede se perdo la seed phrase?

Non potrai ripristinare il tuo wallet in caso di necessità. Perderai il controllo delle chiavi

private e quindi dei tuoi bitcoin. Per sempre. Da grandi poteri derivano grandi responsabilità.

57. Che cosa succede se perdo l'accesso al wallet?

Il wallet è un portachiavi e le chiavi possono essere rigenerate dal seed. Se perdi l'accesso al

wallet puoi inserire nuovamente la seed phrase per ripristinarle.

58. Dove posso vedere la transazione della pizza da 10000

bitcoin?

Il 22 maggio 2010 due pizze furono acquistate per 10000 bitcoin11 .

59. Che cosa sono le altcoins?

Le altcoins sono le “sorellastre” di bitcoin. Alternative coins, quindi altre criptovalute con,

in alcuni casi, altre blockchain. Ognuna con diversi scopi.

60. Quando venne fatta la prima transazione?

La prima transazione12 tra due indirizzi venne fatta il 12 gennaio 2009, tra Satoshi Nakamoto

e Hal Finney. Blocco numero 170.

11 http://bit.ly/2WJxEft

12 http://bit.ly/2HY2wUU

LIVELLO INTERMEDIO

61. Che cosa è un sistema centralizzato?

In un sistema centralizzato (centralized ledger) tutte le operazioni sono elaborate da un

singolo nodo, ovvero un singolo computer.

Ogni individuo dipende dall'ente centrale.

I dati risiedono su un database centralizzato proprietario, quindi dobbiamo *fidarci* dell'ente con cui stiamo interagendo per quanto riguarda l'integrità e la validità dei dati.

62. Che cosa è un sistema decentralizzato?

In un sistema decentralizzato non c'è un punto di controllo centrale.

Le operazioni sono effettuate da più nodi.

I dati sono replicati su più nodi, più server lavorano insieme per fornire il dato desiderato.

63. Che cosa è un sistema distribuito?

In un sistema distribuito (distribuited ledger) non esiste nessuna macchina specializzata per

l'archiviazione dei dati.

Tutti i nodi sono di pari livello, ovvero

possiedono i medesimi diritti.

I dati sono replicati su ogni nodo.

Sono dette anche reti trustless, proprio perché non è necessario “fidarsi” di un terzo, dato

che le informazioni sono condivise.

64. Che cosa sono i BIP?

Bitcoin Improvement Proposal. Le modifiche o implementazioni del protocollo vengono

discusse dalla community e vengono catalogate come BIP.

65. Che cosa è lo SHA256?

È una funzione crittografica. Secure Hash Algorithm. Da un input arbitrario restituisce

sempre come risultato 256 bit.

66. Quante unità di misura ha bitcoin?

1 bitcoin (BTC) può essere rappresentato fino alla sua centomilionesima parte, chiamata

satoshi (0.00000001 BTC).13

67. Che cosa è una funzione di hash?

È un algoritmo matematico che da una

lunghezza arbitraria restituisce una dimensione fissa.

13 http://bit.ly/2vPYmHs

19

68. Che cosa è un digest?

Output ottenuto da una funzione crittografica di hash.

69. Come si identifica un blocco?

Può essere identificato tramite il suo hash o tramite la sua altezza.

70. Che cosa è una transazione?

È tra le principali forme di messaggi previste dal protocollo Bitcoin. Permette il

trasferimento di porzioni di bitcoin da un address a un altro.

71. Che cosa è l'hashrate?

Con hashrate si identifica la quantità di hash al secondo che la rete è in grado di sostenere.

72. Come si identifica una transazione?

Ogni transazione è identificata dal suo hash, che rappresenta la sua impronta digitale

ottenuta dalla funzione crittografica SHA256.

73. Posso annullare la transazione?

Dipende dai casi. Il protocollo Bitcoin prevede alcuni metodi che permettono la modifica di

un transazione prima che essa venga confermata, quindi inserita all'interno di un blocco e

aggiunta alla blockchain. In questo caso, l'unico modo per annullare gli effetti di una

transazione è quello di creare una nuova transazione che invalidi gli effetti della

precedente

prima che questa venga inserita
all'interno di un blocco.

74. Che cosa si intende con transazione non confermata?

Si intende una transazione che è stata verificata dai nodi ma che ancora non è stata inclusa

nel blocco.

75. Che cosa si intende con transazione confermata?

Si intende una transazione che è stata verificata dai nodi e che è stata inclusa

nel blocco. Tale transazione fa parte della blockchain.

76. Chi conferma la transazione?

La transazione è confermata quando il blocco viene minato dal miner aggiungendolo alla

blockchain.

77. Come si raggiunge il consenso della transazione?

Ogni nodo verifica e asserisce che la transazione è valida. Si ottiene così il consenso,

conosciuto anche come consenso

emergente.

78. Chi crea il blocco?

Il blocco viene creato dal miner.

20

79. Chi verifica il blocco?

Il blocco viene verificato dai tutti i nodi nel momento della ricezione, prima di essere

aggiunto alla rispettiva copia locale della blockchain.

80. Che cosa è un miner?

Il miner è un nodo che cerca di risolvere il puzzle crittografico imposto dal protocollo al fine

di mettere in sicurezza la blockchain ed ottenere il reward.

81. Che cosa significa minare?

È quel processo in cui il miner cerca di stare sotto alla difficoltà imposta dal protocollo

creando l'hash del block header per il candidate block. L'hash sarà l'identificativo del blocco

quando farà parte della blockchain.

82. Perché un blocco è minato ogni 10 minuti?

Un blocco viene minato in media ogni 10 minuti. Il timing è pensato per evitare fork

frequenti e per motivi di sicurezza.

83. Che cosa è il reward?

Il reward è il premio che il miner riceve per aver risolto il puzzle crittografico in cambio del

suo sforzo computazionale.

84. Da che cosa è formato il reward?

Oggi, 2019, il reward è di 12.5 bitcoin a blocco.

85. Che cosa è l'halving?

L'halving14 è il dimezzarsi del reward.

Avviene all'incirca ogni 4 anni, o più precisamente ogni 210000 blocchi. Il protocollo ha

iniziato con un reward di 50 bitcoin a blocco nel 2009. Nel novembre 2012 il reward si è

dimezzato a 25 bitcoin.

A Luglio 2016 è stato dimezzato ancora a 12.5 bitcoin e nel 2020 passeremo a

6,25 bitcoin.

86. A chi è destinata la fee?

Le fee si sommano al reward del miner. Dopo che saranno stati emessi tutti i bitcoin dal

protocollo, i miners saranno incentivati solo dall'ammontare delle fees.

87. Come si calcola la fee?

La fee è ottenuta dalla differenza tra l'input e l'output della transazione.

14 http://bit.ly/2vKlXt3

88. Perché alcuni address iniziano con 1?

Gli address P2PKH (Pay To Pubkey Hash) iniziano sempre con il numero 1 perché durante la

generazione vengono mappati con il prefisso15 esadecimale 0x00.

89. Perché alcuni address iniziano con 3?

Gli address P2SH (Pay To Script Hash) iniziano sempre con il numero 3, perché durante la

generazione vengono mappati con il prefisso16 esadecimale 0x05.

90. Come vengono scelte le parole della seed phrase?

Vengono scelte dal dizionario17 tramite dei passaggi di crittografia. Se si scelgono 12 parole,

abbiamo a disposizione 2048^{12} combinazioni.

91. Che cosa è la coinbase?

La coinbase è la prima transazione di ogni blocco. È la transazione con cui il miner assegna a

se stesso il reward per aver risolto il PoW.

92. Dove si legge il titolo de “The Times” ?

È possibile leggere il titolo storico “The Times 03/Jan/2009 Chancellor on brink of second

bailout for banks.“ nella coinbase del primo blocco18. Il suo formato è in esadecimale.

93. Posso scrivere del testo sulla blockchain?

Si, è possibile scrivere del testo sulla blockchain. Guarda questo messaggio

http://bit.ly/2H22qJQ19.

94. Che cosa è il Proof of Work?

Il Proof of Work (PoW) è l'algoritmo di consenso della blockchain Bitcoin.

95. Quando venne usato per la prima volta l'algoritmo PoW?

Nel progetto Hashcash20 di Adam Back per limitare lo spam email e attacchi DoS.

96. Che cosa è la difficoltà?

La difficoltà è il valore imposto dalla rete che il miner deve riuscire a *battere* per aggiudicarsi il reward e aggiungere il blocco alla chain.

15 http://bit.ly/2YuRvjk

16 http://bit.ly/2YuRvjk

17 http://bit.ly/2WLfg64

18 http://bit.ly/2Sju4au

19 http://bit.ly/2H22qJQ

20 http://bit.ly/2WlnQMN

22

97. Ogni quanto si regola la difficoltà?

La difficoltà si regola ogni 2016 blocchi, in modo da mantenere la media di risoluzione del

puzzle crittografico a 10 minuti *(2 settimane / 10 minuti = 14 * 24 * 60 / 10 = 2016).*

98. Che cosa è il problema dei generali bizantini?

Il problema dei generali bizantini è un classico problema informatico riguardante i sistemi

distribuiti che si incontra quando si deve trovare un *accordo* fra parti, i nodi, comunicando solo tramite messaggi.

99. Come si risolve il problema dei generali bizantini?

Il protocollo Bitcoin utilizza Proof of

Work per essere più resistente al problema dei generali

bizantini.

Attenzione, più resistente, proprio perché non risolve al 100% il problema, ma grazie al fatto

che minare ha un costo economicamente elevato, semplicemente non conviene comportarsi

contro le regole del protocollo.

23

LIVELLO AVANZATO

100. Dove posso leggere il codice sorgente di Bitcoin?

Il codice Bitcoin è opensource ed è disponibile su GitHub21.

101. Che cosa è un wallet non deterministico?

È un wallet dove le chiavi non sono in relazioni tra loro. È opportuno avere un backup per

ogni singola chiave privata.

102. Che cosa è un wallet deterministico?

È un wallet con la caratteristica che tutte

le chiavi private sono derivate da una singola

master key, attraverso un processo deterministico. Tale determinismo rende possibile il

recupero di tutte le chiavi a partire dalla seed phrase.

103. Che cosa è una chiave pubblica?

La chiave pubblica è derivata dalla chiave privata e non può avvenire il contrario. Grazie alla

chiave pubblica è possibile verificare la firma digitale prodotta con la corrispettiva chiave

privata.

104. Che cosa è la firma digitale?

La firma digitale è il meccanismo con il quale si può dimostrare l'autenticità e l'integrità di

un messaggio.

105. Come si effettua la firma digitale?

Si crea con la chiave privata e si verifica con la chiave pubblica.

106. Che problemi risolve la firma digitale?

Autenticità, integrità e non ripudio.

107. Dove viene usata la firma digitale in Bitcoin?

Nelle transazioni.

Solo il possessore di una data chiave privata può derivare una certa chiave pubblica e fornire

una firma che sia comprovata dalla chiave pubblica stessa.

108. Posso salvare l’intera blockchain in un hard disk esterno?

Certamente, abbiamo diverse opzioni da poter utilizzare nel file bitcoin.conf22. In questo caso

l’opzione da usare è -datadir.

21 http://bit.ly/2He7Kdp

22 http://bit.ly/2I0c95v

109. Bitcoin core, di default, dove salva la blockchain?

~/.bitcoin/ (linux)

~/Library/Application Support/Bitcoin/ (mac)

110. Che cosa è SigHash?

Indica quale parte della transazione è

stata firmata, o meglio, i differenti modi per firmarla.

111. Dove si trova SigHash?

È un flag23 che si trova nell'input della transaction data. Il flag 0x01 indica SIGHASH_ALL.

112. Perché la chiave privata è cosi importante?

Perché è l'elemento fondamentale per creare la firma digitale.

113. Che cosa è la crittografia asimmetrica?

Chiamata anche crittografia a chiave

pubblica ha la caratteristica di avere due chiavi

(pubblica e privata) differenti, ma collegate da particolari proprietà algebriche relative alle

operazioni sui campi finiti.

La chiave pubblica del destinatario è utilizzata dal mittente per cifrare il messaggio, la

chiave privata del destinatario - collegata alla chiave pubblica utilizzata dal mittente - è

utilizzata dal destinatario per decifrare il messaggio.

114. Quali sono i punti di forza della crittografia asimmetrica?

Dalla chiave pubblica non si può derivare la chiave privata.

Possiamo quindi distribuirla in modo sicuro, a differenza della crittografia simmetrica.

Univocità nel derivare la chiave pubblica dalla chiave privata.

115. Che cosa è ECDSA?

Elliptic Curve Digital Signature Algorithm, l'algoritmo utilizzato da Bitcoin per la firma

digitale.

116. Che cosa è ECC?

Elliptic Curve Cryptography. La crittografia ellittica

117. Che cosa sono big endian e little endian?

Sono metodi di ordinamento dei bytes.

Nella rappresentazione big endian, il byte più significativo è memorizzato nella cella di

memoria con l'indirizzo più piccolo.

Nella rappresentazione little endian il

byte più significativo è memorizzato nella cella di

memoria con l'indirizzo più grande.

23 http://bit.ly/2WfGIIe

25

118. Come si calcola un hash di un blocco?

Applicando la funzione crittografica SHA256 per due volte agli elementi del block header.

119. Come si calcola l'hash di una transazione?

Applicando la funzione crittografica SHA256 per due volte alla transaction data.

120. Dove sono le transazioni non confermate?

In uno spazio di archiviazione, presente all'interno di ogni Bitcoin client (fatta eccezione per

i client SPV), definito mempool.

121. Come viene calcolata la fee?

La fee è data dal peso in byte della transazione.

Più alto è il numero di bytes che

compongono la transaction data e più alte saranno le fee.

122. A quanto ammontano le fee della coinbase?

La transazione coinbase non ha fee.

123. Da quanti input è formata la coinbase?

La coinbase è sempre formata da un solo input. Può avere, invece, un numero arbitrario di

destinatari.

124. Chi crea la coinbase?

È il miner stesso che crea la transazione verso se stesso, rispettando le regole del protocollo.

125. Che cosa contiene lo scriptSig della coinbase?

Dato che la coinbase non sblocca nessuna UTXO, può contenere qualsiasi dato. È stato

introdotto il BIP3424 che obbliga ad inserire l'altezza del blocco così da eliminare il rischio di ottenere la stessa TXID di coinbase passate.

126. Perché ad ogni transazione cambia l’address Bitcoin?

Per rendere difficile aggregare i mittenti e destinatari delle transazioni, migliorandone la

privacy.

127. Quale algoritmo di hash viene utilizzato in Bitcoin?

SHA256. Da un input di qualsiasi lunghezza otteniamo sempre un output di 256 bits.

128. Che differenza c'è tra nodo e miner?

Possiamo differenziare un nodo dal miner dicendo che il nodo ha il compito di verificare le

transazioni e blocchi, mentre il miner crea i blocchi.

24 http://bit.ly/2WgTDJV

129. Quante transazioni entrano in un blocco?

Ogni transazione ha una dimensione differente. Quindi non è possibile dire con certezza un

numero esatto.

130. Qual è la dimensione massima di un blocco?

1 megabyte.

131. Che cosa è il candidate block?

Il candidate block è il blocco che crea il miner durante il tentativo di risoluzione del puzzle

crittografico inserendo al suo interno le transazioni recuperate dalla mempool.

132. Che cosa è il nonce?

Il nonce fa parte del block header e viene utilizzato dal miner per ottenere hash differenti

durante il processo di mining.

Cambiando il valore del nonce è possibile creare infiniti digest fino a trovare l'hash voluto.

133. Che cosa è un fork?

Un fork si verifica quando due miner trovano contemporaneamente la soluzione al puzzle

crittografico propagando due blocchi validi.

134. Che cosa è un soft fork?

Il soft fork è una modifica del protocollo retrocompatibile.

Permette ai nodi non aggiornati di

continuare ad operare anche se utilizzano un client

Bitcoin con il protocollo non aggiornato.

135. Che cosa è un hard fork?

Hard fork è una modifica del protocollo non retrocompatibile. Si dividono in programmati e

controversi.

136. Che cosa sono gli hard fork programmati?

Gli hard fork programmati sono quelle modifiche che tutta la community condivide,

cercando di aggiornare il software prima possibile.

137. Che cosa sono gli hard fork controversi?

Gli hard fork controversi si verificano quando parte della community non è d'accordo,

rimanendo così sulla *vecchia* chain continuando a operare secondo le regole del *vecchio* protocollo, mentre chi è d'accordo, aggiorna il protocollo e si *sposta* sulla *nuova* chain.

138. Perché ottengo delle criptovalute durante un hard fork?

Se si posseggono delle criptovalute prima dell'hard fork si ottengono delle criptovalute della

nuova blockchain gratuitamente perché l'input della transazione si forma utilizzando anche

UTXO antecedenti al fork.

27

139. Che cosa è la UTXO?

UTXO, unspent transaction output, rappresenta gli output delle transazioni precedenti non

spesi. La somma di tali output forma il

saldo disponibile.

140. Perché quando effettuo una transazione ci sono più

mittenti?

Può accadere che per arrivare all'input desiderato si debba aggregare più UTXO che fanno

riferimento anche ad address differenti. Tali address sono sempre di nostra *proprietà*.

141. Se utilizzo sempre lo stesso address ho meno UTXO?

No. Gli output precedenti non spesi sono

collegati alle transaction id e non al Bitcoin address.

142. Perché non posso trasferire l'esatto valore di bitcoin?

È possibile solo se la somma delle UTXO restituisce l'esatto valore che vogliamo trasferire,

altrimenti l'ammontare di bitcoin che si ottiene tramite il modello UTXO è un numero

discreto e indivisibile.

143. Che cosa è RPC?

Remote Procedure Call, la possibilità di

eseguire dei comandi su una macchina remota. Tali

comandi vengono utilizzati per interagire con il nodo remoto.

144. Dove posso trovare i comandi RPC?

In questa pagina25 puoi trovare molti comandi RPC utili, oppure dal proprio nodo puoi

digitare:

bitcoin-cli **help**

25 http://bit.ly/2wG3AG8

NERD ZONE

146. Che cosa è lo scriptSig?

Sono tutte le condizioni necessarie per soddisfare lo scriptPubKey così da sbloccare UTXO di

riferimento.

Lo scriptSig è scritto nell'input della transazione.

147. Che cosa è l'unlocking script?

Con unlocking script ci riferiamo allo scriptSig.

148. Che cosa è lo scriptPubKey?

Sono tutte le condizioni che devono essere soddisfatte dallo scriptSig per rendere possibile lo

sblocco della UTXO di riferimento. Lo scriptPubKey è nell'output della transazione.

149. Che cosa è il locking script?

Con locking script ci riferiamo a scriptPubKey.

150. Che cosa è script?

È il linguaggio di programmazione utilizzato dai nodi per validare le

transazioni. È Turing

incomplete e stack based.

151. Che cosa è un linguaggio Turing complete?

Un linguaggio Turing complete, chiamato anche universal language, è un linguaggio che

deve poter risolvere qualunque problema risolvibile che anche la macchina di Turing

Universale è in grado di eseguire.

152. Che cosa è un linguaggio Turing incomplete?

Un linguaggio non-universal o Turing incomplete ha dei limiti, molto spesso non si ha la

possibilità di fare dei loop, oppure *andare* da una funzione a un'altra "*saltando*" da un pezzo di codice a un altro.

153. Perché script è Turing incomplete?

Per motivi di sicurezza. Ogni nodo deve assicurare che il programma termini. Per esempio,

se fosse possibile fare dei cicli potremmo entrare in dei loop infiniti.

154. Che cosa è un linguaggio stack

based?

È un linguaggio di programmazione che si basa sulla struttura dati stack, nel caso di Bitcoin

si utilizza LIFO, Last Input First Output. L'ultimo elemento che entra (push) nello stack è il

primo ad uscire (pop).

29

155. Dove sono salvate le UXTO?

Ogni nodo ha un database LevelDb26 chiamato chainstate. Alcune UTXO sono tenute nella

RAM del nodo per velocizzarne il controllo.

156. Come posso recuperare tutte le UTXO dal mio nodo?

Utilizzando il comando listunspent.

157. Cosa è il change address?

Con change address si intende l'indirizzo di resto di una transazione.

158. Come si genera un Bitcoin address?

Da una chiave privata deriviamo la chiave pubblica. Sulla chiave pubblica vengono applicati

due funzioni crittografiche SHA256 e RIPEMD160. Al risultato viene aggiunto il version

prefix27 e viene utilizzato base58check encode, ottenendo cosi il Bitcoin address.

159. Che cosa è il version prefix nel Bitcoin address?

Il version prefix28 è rappresentato da un flag, solitamente 1 byte, che identifica l'address che

verrà generato.

160. Perché viene utilizzato base58 per generare il Bitcoin

address?

Base5829 ha la caratteristica di eliminare alcuni caratteri ambigui, come ad esempio lo 0

(zero) e la O maiuscola per evitare errori di trascrittura.

161. Che cosa è la coinbase maturity?

La coinbase maturity è una costante del protocollo che indica che la coinbase può essere

spesa dopo aver ottenuto 100 conferme30.

162. Che cosa è il merkle tree?

Il merkle tree è un albero binario che offre la possibilità di effettuare delle ricerche dentro di esso molto velocemente.

163. Dove viene usato il merkle tree e perché?

Il merkle tree viene utilizzato per verificare se una data transazione fa parte del blocco.

Grazie alla sua logica, il nodo esaminerà solamente quelle parti di albero necessarie per

ottenere la verifica, così da avere un carico di lavoro molto più leggero.

26 http://bit.ly/2JZkisU

27 http://bit.ly/2YuRvjk

28 http://bit.ly/2W1oMVs

29 http://bit.ly/2DPAmcb

30 http://bit.ly/2Hrz1cD

164. Che cosa è il merkle root?

È l’impronta digitale di tutte le transazioni contenute nel blocco. Il merkle root rappresenta

il vertice del merkle tree.

165. Che dimensioni ha il merkle root?

Sempre 256 bits, perché ottenuto dalla funzione crittografica SHA256.

166. Che cosa è il merkle block message?

Il merkleblock message31 è un messaggio che ottiene il nodo per verificare se la transazione

cercata appartenga al merkle tree e di conseguenza appartenga al blocco.

167. Che cosa è la chiave privata WIF?

Wallet Import Format, è un formato ottenuto per semplificare la copia della

chiave privata.

168. Che cosa è la testnet?

È una blockchain Bitcoin a tutti gli effetti pensata per effettuare dei test.

169. Che cosa è la regtest?

È una Bitcoin blockchain da utilizzare sul proprio computer che replica il protocollo nel suo

complesso e dove si possono minare blocchi istantaneamente.

170. Che cosa sono le faucet?

Sono dei servizi che permettono di

ricevere bitcoin da utilizzare nella blockchain testnet.

171. Che cosa è il P2PKH?

P2PKH è la sigla di Pay-to-PublicKey Hash. È il metodo più comune di verifica della

transazione.

172. Che cosa è il P2PK?

P2PKH è la sigla di Pay-to-public key è un metodo di verifica della transazione, quella che fu

usata da Hal Finney32 nel blocco 17033.

173. Che cosa è il P2MS?

P2MS è la sigla di Pay-to-multisig. Permette di bloccare bitcoin su più public key e richiede

un numero specifico di firme per sbloccarli.

31 http://bit.ly/2JirAXq

32 http://bit.ly/2JjCVaN

33 http://bit.ly/2vVLrUD

174. Che cosa è il P2SH?

P2SH è la sigla di Pay-to-script hash. Permette di creare un proprio script (redeem script) da

utilizzare per sbloccare UTXO.

175. Che cosa è l'attacco del 51%?

Se una gran parte di minatori si uniscono e prendono "possesso" del 51% della rete

potrebbero propagare dei blocchi arbitrari senza consenso.

176. Che cosa è l'attacco Finney?

È un tipo di attacco che si applica sulla transazione non confermata e richiede

l’intervento di

un esperto di mining. Per combattere questo tipo di attacco è consigliata l’attesa della 6°

conferma.

177. Che cosa è il double spending?

Si verifica quando un utente prova a spendere gli *stessi* bitcoin verso due destinatari

differenti. Il mining e quindi il consenso risolvono questo problema.

178. Che cosa è l’attaco Race?

È un tipo di attacco che effettua una spesa doppia contemporaneamente, senza attendere

che queste siano confermate. In questo caso solo uno dei destinatari riceverà effettivamente

l'importo. Per combattere questo tipo di attacco è consigliata attendere la 6° conferma.

179. Che cosa sono le opcodes?

Sono le operazioni che il linguaggio script effettua per validare la transazione. I codici

esadecimali sono mappati con delle

operazioni34.

180. Che cosa è il generator point?

Sono delle coordinate statiche della curva ellittica Secp256k135. Punto di partenza per la

generazione delle chiavi usate in ECDSA36.

181. Quanti bytes ha la chiave pubblica non compressa?

65 bytes. Al suo interno sono riportati la X e la Y della curva ellittica Secp256k1, utilizzate per generarla.

182. Quanti bytes ha la chiave pubblica

compressa?

33 bytes. Al suo interno è riportata solo la X. La Y è derivata dal primo byte.

34 http://bit.ly/2vN3WdU

35 http://bit.ly/2JXzozb

36 http://bit.ly/2JhW4J9

32

183. Che cosa è la derivation path?

È il percorso di derivazione delle chiavi in un wallet deterministico. La struttura del BIP-4437

è
m/purpose’/coin_type’/account’/change/a

184. Che cosa è la xpub?

Extended public key e può derivare solo chiavi pubbliche.

185. Che cosa è la xprv?

Extended private key può derivare sia chiave pubbliche che chiavi private.

186. Che cosa sono gli importi dust?

Sono importi molto piccoli nati dal modello UTXO.

È uno dei suoi aspetti negativi, spesso

generati da piccoli resti.

187. Che cosa è una derivazione hardened?

Il wallet deterministico utilizza la derivazione hardened, che interrompe il legame tra la

chiave pubblica padre e il chain code del figlio.

188. Che cosa è un nodo SPV?

Il nodo SPV38 (simplified payment verification) è un nodo “leggero”.

Non scarica l’intera blockchain, ma richiede solo il block header (80 bytes

per blocco) per

verificare se la transazione, da lui inoltrata o ricevuta fa parte del blocco. Per fare questa

operazione richiede anche il merkleblock message.

189. Che cosa è il target nel candidate block?

Rappresenta la difficoltà che il miner deve “battere” per risolvere il puzzle crittografico e

aggiudicarsi il reward.

190. Che cosa sono i bloom filters e

dove vengono usati?

I bloom filters sono una struttura dati probabilistica usata per verificare se un elemento

appartiene a un insieme oppure no. Vengono utilizzati dai nodi SPV, quando richiedono

informazioni, per verificare se una transazione fa parte di un blocco mantenendo la privacy.

191. Che cosa è la collisione?

In crittografia una collisione hash è una situazione che avviene quando due input diversi

producono lo stesso digest tramite una funzione hash. È proprio perché è altamente

improbabile avere la collisione che i nodi sono in grado di replicare il risultato fornito dal

miner e verificare il lavoro in breve tempo.

37 http://bit.ly/2Jev8L7

38 http://bit.ly/2MrxGId

192. Posso battere la difficoltà del PoW scegliendo l'input?

No, in una funzione di hash, non è possibile scegliere l'input in base all'output desiderato. Si

potrebbe pensare: devo trovare un numero minore di 50, quale input mi crea un digest

minore di 50? Spiacente.

193. Che cosa è una transazione serializzata?

La serializzazione è il processo con cui si rappresenta la struttura dati della transazione.

Questo procedimento è conosciuto anche come byte stream.

194. Che cosa è la deserializzazione?

È il processo inverso della serializzazione, il byte stream viene convertito nella struttura

della transazione.

195. Quando viene usato OP_RETURN?

Viene utilizzato per scrivere del testo sulla blockchain, marcando la UTXO come non

spendibile.

196. Come viene ottenuta la seed phrase?

La seed phrase viene calcolata partendo da una entropia di 128 bits. Dopo aver calcolato il

suo checksum viene convertito in base2 (binario). Ogni segmento di binario da 11 bits viene

convertito in base 10 e mappato sul dizionario39.

197. Che cosa è il checksum?

È una sequenza di bit che associata al pacchetto trasmesso verifica l'integrità del messaggio.

198. Come viene calcolato il seed?

Il seed viene calcolato partendo dalla seed phrase alla quale viene aggiunto il salt, che

contiene *mnemonic* come valore di default. Viene applicata la funzione di derivazione

PBKDF240 che genererà un seed di 512 bits.

39 http://bit.ly/2WLfg64

40 http://bit.ly/2QrIDbj

199. Come posso approfondire con la pratica?

Con il libro “Bitcoin dalla teoria alla

pratica”41 puoi interagire con il protocollo grazie a

esempi concreti e reali.

41 https://amzn.to/2Xwu7BW
ISBN:979-12-200-4947-4

Gli autori

Alessio Barnini

Nato a Livorno all’ombra del cacciucco nel 1983.

Fin dai primi anni della mia vita sono stato affascinato dai computer. Il primo amore è stato

il Commodore 64 di mio padre, non ricordo l'età che avevo, ma sicuramente non ero ancora

in grado di leggere e scrivere. Riuscivo però a caricare i giochi, i dischi di cartone, perché mi ricordavo la sequenza delle lettere e il disegno che formavano.

Mi ricordo la passione che mettevo nello sconfiggere i miei fratelli ai videogiochi, che mi

prendevano in giro facendomi giocare

con il joystick scollegato. Ma tanto volavo con la

fantasia che non serviva un controller per immaginare di essere dentro a un altro mondo,

proprio come TRON42.

Ancora oggi mi ricordano questo episodio.

Arrivò poi l'Amiga 500 che mio padre prontamente portò in casa.

Non facevamo niente di programmazione, ma ricordo che iniziavamo a utilizzare gli utility43.

Era qualcosa che andava oltre il semplice gioco.

Ci fu poi il grande passo con il PC.

Iniziammo a esplorare un mondo per noi sconosciuto, MS-DOS.

Ricordo ancora oggi che mio padre teneva un quaderno con tutti i comandi da eseguire e

ricordo con estremo piacere il giorno, o meglio la notte, che mi svegliò perché voleva provare

un gioco, ma era archiviato con ARJ. Non ricordava il comando per scompattarlo, io lo

ricordavo a memoria.

Solo oggi, con il passare degli anni, mi rendo conto che già a quell'età avevo scelto la mia

strada e questo grazie alla curiosità che mio padre trasmetteva.

Nel corso degli anni ho iniziato a studiare da autodidatta, come spesso accade in questo

mondo. I primi esperimenti, i primi server, i primi siti web, i primi terribili tentativi di fare il grafico.

Fino a che è arrivato a essere il mio lavoro, che mi ha portato a lasciare la

mia Livorno per

approdare prima a Roma e poi a Milano, dove ho conosciuto Alessandro Aglietti, co-autore

di questo libro, il quale con un entusiasmo simile al mio quando venni svegliato per

scompattare l'archivio ARJ, mi parlò di Bitcoin.

Non ricordo mai episodio in cui si soffermava sulla parte speculativa, era affamato di

condividere le informazioni che anche lui stava costruendo, con una passione

come per dire

“è impossibile che tu non sia affascinato da questa cosa”.

42 http://bit.ly/2MbGhir

43 http://bit.ly/2QdbH6a

Le nostre strade lavorative poi si sono divise, ma è rimasta l’amicizia e la passione verso

questa rivoluzione che ci porta a fare esperimenti notturni. Ogni esempio di codice su questo

libro è frutto di un nodo Bitcoin che abita a casa sua e che mi ha permesso di usare.

Non poteva essere diversamente :)

È grazie ad Alessandro che ho incontrato Bitcoin e ancora grazie a lui se ho avuto la “fame”

di capirne ogni singolo bit.

38

Alessandro Aglietti

Nato a Firenze, classe 1989, vive a Milano con la sua compagna Stefania e con Eli, un’amica a

quattro zampe mix pastore tedesco. Fin da piccolo ha sempre avuto la campagna nel cuore,

ma con il passare degli anni si è ritrovato sempre più davanti al computer, inizialmente per

giocare ma anche a perder tempo, a onor del vero.

Conosce l'amore della sua vita alle superiori e se non fosse stato per lei sarebbe rimasto

rintanato in sperdute cascine toscane, coltivando la terra e giocando a Caesar III,

Warhammer e così via. Tutt'oggi questo scenario rappresenta il suo piano B.

Il buon esempio della sua compagna lo ha spronato nel dedicarsi ad un'attività nella quale

riuscisse a ottenere ottimi risultati, e l'utilizzo del computer è quindi diventato prima la fine del percorso di studi e successivamente la professione.

Convinto che tutti gli individui abbiano eguali capacità, adora spronare i suoi compagni di

merende nel dare il massimo anche se di fronte ad arditi obbiettivi. Questa sua indole si è

trasformata in un percorso, parallelo al lavoro, come formatore di supporto nella scuola

dove si è diplomato.

Adora consolidare i risultati di esperimenti tecnologici e/o attività lavorative realizzando

talk presso meetup e conferenze, sempre con il secondo fine di spronare la platea a porsi

nuove sfide e obbiettivi.

Grazie ad una rivista, Linux & C., lesse di Bitcoin per la prima volta nel 2009 senza però

coglierne a pieno le potenzialità. Nell'estate 2016, grazie al fermento della community

milanese, ha ripreso in mano questa tecnologia.

Approfondendo il funzionamento di Bitcoin è rimasto affascinato dall'eleganza della

soluzione ed è stato un passaggio naturale decidere di trasformare le competenze apprese in

contenuto divulgativo.

Sempre nel 2016, grazie alla startup brumbrum.it dove lavora tuttóra,

conosce “il Barno”

con il quale – a botte di campanilismi classici degli abitanti del Granducato – entra in

grande sintonia, e insieme decidono che oltre al lavoro avrebbero dovuto combinare

qualcosa di divertente. Il libro –Bitcoin dalla teoria alla pratica44 – ne è il primo risultato.

44 https://amzn.to/2Xwu7BW


4715
brumbru

Document Outline