APPROFONDIMENTO MODULO 3:

La Blockchain di Bitcoin

Cos'è Bitcoin e come funziona?

Bitcoin è una rete di consenso che abilita un nuovo sistema di pagamento e una valuta completamente digitale. È la prima rete di pagamento decentralizzata e peer-to-peer gestita dai suoi utenti, senza un'autorità centrale o intermediari. Dal punto di vista dell'utente, Bitcoin è come il denaro per Internet. Bitcoin potrebbe essere l'unico sistema di contabilità a partita tripla esistente.

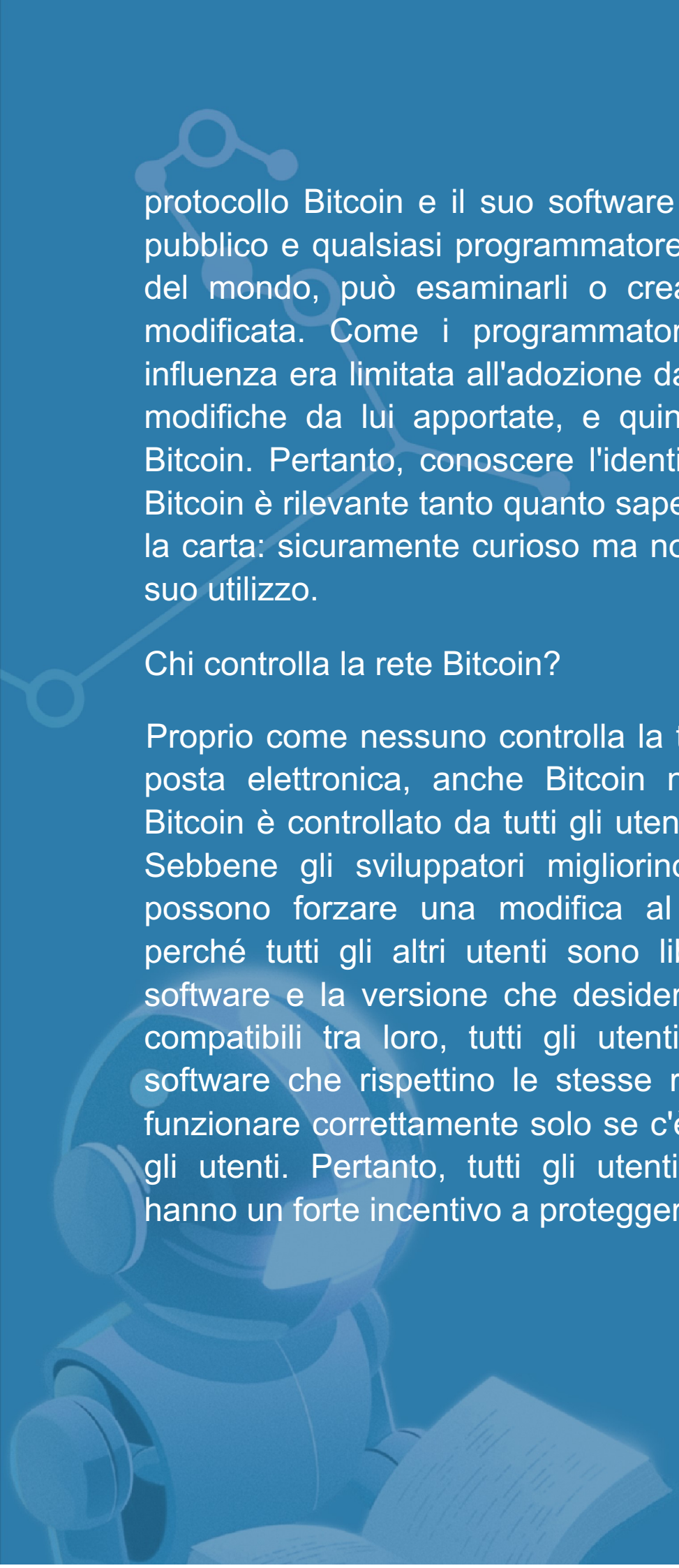
Chi ha creato Bitcoin?

Bitcoin è la prima implementazione di un concetto noto come "criptovaluta", descritto per la prima volta nel 1998 da Wei Dai sulla mailing list "cypherpunks". Propose l'idea di un nuovo tipo di denaro che avrebbe utilizzato la crittografia per controllare la sua creazione e le sue transazioni, anziché un'autorità centralizzata. La prima specifica del protocollo Bitcoin e la sua proof of concept furono pubblicate da Satoshi Nakamoto nel 2009 su una mailing list. Satoshi abbandonò il progetto alla fine del 2010 senza rivelare molto di sé. Da allora, la comunità è cresciuta esponenzialmente e include numerosi sviluppatori che lavorano sul protocollo Bitcoin.
L'anonimato di Satoshi ha talvolta suscitato sospetti ingiustificati, molti dei quali derivanti dalla scarsa comprensione della natura open source di Bitcoin. Il

protocollo Bitcoin e il suo software sono disponibili al pubblico e qualsiasi programmatore, in qualsiasi parte del mondo, può esaminarli o crearne una versione modificata. Come i programmatori di oggi, la sua influenza era limitata all'adozione da parte di altri delle modifiche da lui apportate, e quindi non controllava Bitcoin. Pertanto, conoscere l'identità dell'inventore di Bitcoin è rilevante tanto quanto sapere chi ha inventato la carta: sicuramente curioso ma non essenziale per il suo utilizzo.

Chi controlla la rete Bitcoin?

Proprio come nessuno controlla la tecnologia dietro la posta elettronica, anche Bitcoin non ha proprietari. Bitcoin è controllato da tutti gli utenti in tutto il mondo. Sebbene gli sviluppatori migliorino il software, non possono forzare una modifica al protocollo Bitcoin perché tutti gli altri utenti sono liberi di scegliere il software e la versione che desiderano. Per rimanere compatibili tra loro, tutti gli utenti devono utilizzare software che rispettino le stesse regole. Bitcoin può funzionare correttamente solo se c'è consenso tra tutti gli utenti. Pertanto, tutti gli utenti e gli sviluppatori hanno un forte incentivo a proteggere tale consenso.



Chi c'è dietro lo sviluppo di Bitcoin?

Naturalmente, sappiamo tutti che il creatore di Bitcoin è l'ancora relativamente sconosciuto Satoshi Nakamoto. Ma la verità è che, 11 anni dopo il blocco genesi, ci sono centinaia di altre persone coinvolte nel suo sviluppo come software.

Ad oggi, esistono diverse implementazioni (versioni) di Bitcoin, ciascuna con i propri sviluppatori responsabili della manutenzione del codice e del miglioramento delle sue funzionalità e scalabilità. La più popolare di queste, sebbene non l'unica, è Bitcoin Core.

Una delle caratteristiche chiave della decentralizzazione di Bitcoin è che chiunque, in qualsiasi parte del mondo, abbia le conoscenze necessarie può contribuire volontariamente al suo sviluppo. Tuttavia, le proposte di modifica del codice devono essere concordate prima di essere approvate.

Come spiegato su Bitcoin.org, la pagina informativa più consultata su Bitcoin: sebbene i programmatori migliorino il software, non possono forzare una modifica al protocollo Bitcoin perché tutti gli altri utenti sono liberi di scegliere il software e la versione che desiderano. Affinché la compatibilità rimanga, tutti gli utenti devono utilizzare software che rispetti le stesse regole. Bitcoin può funzionare correttamente solo se c'è consenso tra tutti gli utenti. Ciò significa che, sebbene chiunque possa partecipare al suo sviluppo, è

impossibile per un singolo individuo o un piccolo gruppo modificare il protocollo senza il consenso della maggioranza. Proprio come chiunque può partecipare al suo sviluppo, ognuno è libero di utilizzare la versione che desidera e il protocollo seguirà le regole del software compatibile utilizzato dalla maggioranza.
Tenendo presente questo, possiamo esplorare alcune di queste versioni per scoprire chi c'è dietro, mantenendo in funzione Bitcoin.

Bitcoin Core

Si tratta della prima implementazione di Bitcoin, originariamente creata da Satoshi Nakamoto come Bitcoin 0.1 e rilasciata il 9 gennaio 2009 su SourceForge, pochi giorni dopo la creazione del blocco genesi. Fin dall'inizio, il software è stato presentato come open source, il che significa che chiunque è libero di utilizzarlo e modificarlo.
Satoshi continuò a collaborare allo sviluppo, correggendo bug e proponendo miglioramenti su GitHub fino alla versione 0.3.9, alla fine del 2010. A quel punto, si dimise e nominò Gavin Andresen responsabile della manutenzione. Sebbene alcune fonti sostengano che sia semplicemente scomparso, Andresen, essendo l'unico ad avere il potere di apportare modifiche al codice (che Satoshi gli aveva precedentemente concesso), assunse il ruolo. Sotto la guida di Andresen, questa implementazione fu

rinominata Bitcoin QT nel novembre 2011. Anni dopo, il 19 marzo 2014, fu rinominata Bitcoin Core, tra alcune polemiche, poiché il termine implicava una centralizzazione contraria agli ideali di Bitcoin. Meno di un mese dopo, anche Bitcoin Core cambiò il suo responsabile della manutenzione, affidando il timone a Wladimir van der Laan, che ha mantenuto tale ruolo fino ad oggi.

Come funziona il processo di sviluppo?

Come spiegato su GitHub, chiunque può contribuire allo sviluppo; tuttavia, per "ragioni pratiche", esiste una gerarchia consolidata tra i contributori basata sulla meritocrazia. Vale a dire, coloro che hanno dedicato più tempo e contribuito di più al codice hanno un maggiore potere decisionale finale.
Allo stesso modo, su GitHub ci sono le figure dei “manutentori” del codice, che hanno accesso privilegiato e sono responsabili della gestione delle richieste di inclusione di nuove proposte di codice nel repository principale (pull request); il ruolo del manutentore principale, responsabile in ultima analisi della nomina di nuovi manutentori e dell’implementazione di nuove versioni.
È importante notare che quando queste nuove versioni comportano una modifica significativa e irreversibile al software, la decisione di adottarle o meno dipende interamente dalla comunità Bitcoin, non dagli

sviluppatori. In questi casi, la comunità vota sul futuro della rete utilizzando la versione del software Bitcoin che preferisce e/o supportando tale versione con la propria potenza di elaborazione (miner), come accaduto con SegWit nel 2017.

Se un numero sufficiente di utenti utilizza la versione che si desidera mantenere, la rete adotta le regole di quella versione nel protocollo. Pertanto, le versioni con regole compatibili vengono mantenute sulla catena Bitcoin principale, mentre altre si biforcano, creando potenzialmente una nuova criptovaluta se la nuova catena ha abbastanza nodi e miner per supportarla.

Il percorso per modificare il codice inizia con la creazione di una Proposta di Miglioramento Bitcoin (BIP), che qualsiasi sviluppatore può inviare come idea per la discussione alla mailing list Core della Linux Foundation. Una volta discussa, una bozza formale con linee guida specifiche viene creata su GitHub come pull request, che può quindi essere esaminata dalla community. La bozza viene quindi inviata all'editor di BIP, attualmente Luke Dashjr. Solo dopo l'approvazione, le vengono assegnati un numero e una categoria e viene integrata nel repository Bitcoin. Quando i manutentori approvano una pull request, questa viene sottoposta a un approfondito processo di peer review a cui chiunque può partecipare tramite GitHub e il canale IRC #bitcoin-dev.

Freenode, il canale Core Slack, Bitcoin Stack

Exchange, la mailing list Core presso la Linux Foundation e il forum di sviluppo su Bitcointalk.

Sviluppatori in primo piano

Il numero totale di collaboratori di Bitcoin Core, così come i loro contributi individuali, è disponibile su GitHub. Bitcoin.org conta circa 368 programmatori da tutto il mondo. Attualmente, oltre a van der Laan, Pieter Wuille e Jonas Schnell sono i responsabili del codice.
Di seguito puoi trovare un elenco di sviluppatori che si distinguono sia per il numero e la qualità dei loro contributi, sia per il tempo che hanno dedicato a questo compito.

Wladimir van der Laan

Ad oggi, ha effettuato 5.778 commit sul codice. A parte il fatto che risiede ad Amsterdam, nei Paesi Bassi, si sa poco di questo programmatore. In precedenza, ha rifiutato interviste e i suoi profili sui social media non includono alcuna informazione personale.
È attivo nel repository Core dal 2011 e, a partire dal 2015, è stato assunto dalla Digital Currency Initiative del MIT Media Lab per proseguire lo sviluppo di Bitcoin dopo il fallimento della Bitcoin Foundation. I suoi pseudonimi noti includono laanwj, wumpus e orionwl.

Pieter Wuille

Pieter Wuille è una delle figure chiave dietro SegWit. Dal 2011, ha contribuito a 1.584 revisioni del codice, è stato autore di 12 Bitcoin Improvement Proposal (BIP) ed è stato uno dei principali sviluppatori che hanno lavorato all'implementazione di SegWit. Inoltre, nel luglio 2018, ha presentato ufficialmente lo schema di firma Schnorr come Bitcoin Improvement Proposal.
Ha conseguito un dottorato di ricerca in Informatica presso l'Università Cattolica di Lovanio (Belgio). Ha lavorato, tra gli altri, per Google ed è anche co-fondatore di Blockstream, un'azienda specializzata nella creazione di “sidechain” blockchains. Il suo pseudonimo su GitHub è "sipa".

Marco Falke

Questo è un altro sviluppatore che ha scelto di rimanere anonimo. È stato nominato responsabile della manutenzione nel 2014 da van der Laan, ma ha lasciato il ruolo all'inizio del 2018. Durante questo periodo, ha eseguito 1.175 revisioni.
Secondo il suo GitHub, è originario di Monaco di Baviera, in Germania, anche se un breve profilo dell'azienda in cui lavora, Chaincode Labs, indica che si è trasferito a New York nel 2017 per "lavorare a tempo pieno su software open source".

Gavin Andresen

Indubbiamente uno degli sviluppatori più importanti, con 1.101 revisioni e 12 Bitcoin Investment Points (BIP) al suo attivo. È stato uno dei principali manutentori di Bitcoin sin dal suo inizio per quattro anni ed è stato responsabile della creazione della Bitcoin Foundation per fornire finanziamenti e formazione sull'ecosistema. Quando la fondazione ha esaurito i fondi nel 2015, Andresen, come van der Laan, è stato assunto dalla Digital Currency Initiative del MIT Media Lab. Ha conseguito una laurea in Informatica presso la Princeton University e risiede nel Massachusetts (USA). Nel 2016, è stato coinvolto in una controversia sulla presunta identità di Craig Wright come Satoshi Nakamoto, che ha portato van der Laan a revocare il suo status di manutentore della rete per timore che questo potere cadesse nelle mani sbagliate. Da allora, Andresen si è tenuto per lo più lontano dai riflettori dei media e lontano dal mondo Bitcoin.

Matt Corallo

Dal 2011, ha contribuito a 619 revisioni e 4 BIP. Co-fondatore di Blockstream, ha collaborato al White Paper sulla blockchain.
Ha sviluppato sidechain e implementato Elements Sidechain. Attualmente lavora per Chaincode Labs.
Ha conseguito una laurea in Informatica presso l'Università della Carolina del Nord (USA). Il suo

pseudonimo su GitHub è TheBlueMatt.

Jonas Schnelli

Originario della Svizzera, ha contribuito a 611 revisioni del codice e 3 BIP dal 2013. È co-fondatore di Shift Cryptosecurity, il cui prodotto di punta è il portafoglio hardware BitBox. In precedenza, ha sviluppato app per aziende come Coop e Credit Suisse.
Senza rivelare troppe informazioni su di sé, si dichiara cypherpunk e hacker sul suo account GitHub.

Cory Fields

Dal 2013 ha scritto 573 recensioni. Nel 2015 è stato assunto dalla Digital Currency Initiative del MIT Media Lab, insieme a van der Laan e Andresen. Ha inoltre fatto parte del Consiglio di Amministrazione della XBMC Foundation, che gestisce il software di intrattenimento Kodi, di cui è anche sviluppatore.
Il suo pseudonimo su GitHub è "theuni". È noto anche per aver rivelato una vulnerabilità critica in Bitcoin Cash.

John Newberry

Ha 399 revisioni dal 2015. Proviene da Chaincode Labs e lavora a tempo pieno su Bitcoin dal 2016 a New York. Attualmente è anche direttore della ONG Bitcoin Optech, un'iniziativa che mira ad aiutare le

aziende a comprendere e migliorare le loro implementazioni Bitcoin.
È anche uno sviluppatore di Lightning Network e, come molti dei suoi colleghi, ha preferito mantenere un profilo piuttosto basso.

Gregory Maxwell

Dal 2011, ha contribuito a 265 revisioni del codice, 2 BIP e diverse iniziative incentrate sulla privacy, come CoinJoin. È co-fondatore di Blockstream e ha curato la manutenzione di Bitcoin Core fino al 2015. All'inizio di quest'anno, ha lasciato Blockstream per dedicarsi a tempo pieno allo sviluppo di Bitcoin. Inoltre, il satellite lanciato da Blockstream l'anno scorso per trasmettere i nodi blockchain tramite onde radio è stato originariamente una sua idea.
Prima di Bitcoin, ha lavorato per diversi anni presso Mozilla ed è stato uno dei primi collaboratori di Wikipedia. È un sostenitore dell'open source e della crittografia.

Pietro Todd

È entrato a far parte di Core nel 2012 e ha realizzato 102 revisioni del codice e 5 BIP. Gestisce inoltre il progetto python-bitcoinlib, una libreria di codice per un'interfaccia più semplice in Bitcoin, e OpenTimestamps, un sistema decentralizzato di

marcatura temporale che utilizza Bitcoin per "dimostrare l'esistenza" dei documenti. Si è ritirato da Core nel 2017.
Laureato in Belle Arti, si è specializzato nell'intersezione tra arte e tecnologia. In precedenza, ha collaborato con le startup Coinkite e DarkWallet, oltre che con Chaincode Labs, da cui ha ricevuto una borsa di studio. Risiede a Toronto, in Canada.

Altri nomi

Altri sviluppatori degni di nota per la loro anzianità e il loro contributo a Bitcoin Core includono Luke Dashjr (353 commit e 11 BIP), Alex Morcos (209), Russell Yanofsky (180), Eric Lombrozo (32 e fondatore di Ciphrex) e Jimmy Song (14 e fondatore di Programming Blockchain). Degni di nota anche i manutentori in pensione Martti Malmi (Sirius_m) e Laszlo Hanyecz (famoso per aver comprato la prima pizza con BTC), che condividono con Nakamoto l'account GitHub che ha contribuito a 271 revisioni. Tra i precedenti manutentori figurano anche Jeff Garzik (CEO di Bloq), Nils Schneider (fondatore di Bitcoin Charts) e Chris Moore.

Altri gruppi

Come accennato in precedenza, Bitcoin Core è solo una delle implementazioni di Bitcoin; pertanto, altri gruppi di sviluppatori mantengono le proprie

implementazioni. Qui elenchiamo le alternative più note in base al numero di nodi attivi, insieme ai rispettivi sviluppatori.

Bitcore

Lanciato nel 2013, è descritto come un nodo modulare scritto in Node.js per applicazioni basate su Bitcoin e blockchain. Include un'API, un browser e diverse opzioni di portafoglio. Sebbene open source, è gestito su GitHub dall'azienda BitPay. Dispone di 210 nodi di rete.
Tra i suoi principali collaboratori ci sono gli argentini Manuel Aráoz (co-fondatore degli Zeppelin) ed Esteban Ordano (fondatore di Decentraland).

Bitcoin nodes

È iniziato come un ramo indipendente di Bitcoin Core nel 2014. L'ultima versione, scritta in C++, può essere utilizzata come client per
Può essere utilizzato su desktop, come Bitcoin Core, per pagamenti regolari o come server per commercianti e altri servizi di pagamento. Ha 39 nodi sulla rete.
Attualmente, il suo creatore e unico collaboratore è il co-fondatore di Blockstream e sviluppatore Core Luke Dashjr.

BTCD

Attivo dal 2013, è descritto come un'implementazione completa del nodo scritta in Go. Pur essendo stabile, si segnala che è ancora in fase di test e non possiede intrinsecamente funzionalità di portafoglio. Ha 39 nodi attivi sulla rete. È interessante notare che il suo principale contributore per numero di revisioni (1.576) è Dave Collins, lo sviluppatore principale della criptovaluta Decred. È seguito da David Hill, anch'egli sviluppatore di Decred.

Bitcoin unlimited

È stato scritto in C++ e risale al 2009 su GitHub. La sua caratteristica principale è la dimensione dei blocchi regolabile, accompagnata da Xtreme Thin Blocks (Xthin) e dalla convalida parallela. Ha ancora 30 nodi attivi sulla rete e nel 2017 ha raggiunto quasi 1.000.
Poiché è un derivato diretto di Bitcoin Core, tra i suoi contributori con il maggior numero di revisioni figurano un buon numero degli sviluppatori più importanti di quella prima implementazione, tra cui van der Laan, Wuille, Andresen, Fields, Corallo, Schnelli, Falke e Maxwell.
Tuttavia, sono rimasti in gran parte inattivi sin dalla creazione di Bitcoin Cash, una criptovaluta che incarna gli ideali di BU. Al contrario, gli sviluppatori più attivi ultimamente sono Peter Tschipper e Andrew Stone.

Chi paga le bollette?

Se Bitcoin fosse un'azienda tipica, sarebbe facile capire da dove provengono gli stipendi degli sviluppatori e le attrezzature necessarie. Tuttavia, Bitcoin è un sistema open source e decentralizzato, quindi...

In realtà, la stragrande maggioranza dei suoi sviluppatori mette a disposizione il proprio talento e le proprie attrezzature volontariamente.

Questo non significa che Bitcoin non abbia finanziamenti. Infatti, il primo tentativo di garantirseli è stata la Bitcoin Foundation, creata da Andresen, che ha contribuito a "pagare i conti" fino al 2015. A partire dall'anno successivo, Bitcoin Core ha istituito il suo Programma di Sponsorizzazione, attraverso il quale aziende e organizzazioni possono candidarsi per diventare sponsor, a condizione che siano disposte a rispettare gli ideali di Bitcoin.

Nel corso degli anni sono apparse in questo panorama diverse aziende e organizzazioni, tra cui possiamo evidenziare le seguenti:

Blockstream

È un'azienda dedicata specificamente allo sviluppo di sidechain fin dalla sua fondazione nel 2014. Quasi tutti i suoi co-fondatori fanno parte di Bitcoin Core e, di conseguenza, ricevono o hanno ricevuto i loro stipendi

da lì. Tra questi, Corallo, Maxwell, Dasjr e Wuille, quest'ultimo dedicato a tempo pieno allo sviluppo di Bitcoin.
È interessante notare che questa azienda include una clausola etica nei contratti dei suoi sviluppatori, in cui si afferma che se viene chiesto loro di fare qualcosa che va contro gli interessi di Bitcoin, hanno il diritto di rifiutare e continuare a essere pagati.

Laboratori Chaincode

Fondata nello stesso anno di Blockstream, secondo il suo sito web, "Chaincode Labs esiste per supportare e sviluppare Bitcoin e altri sistemi P2P decentralizzati". Questa affermazione acquista ulteriore peso se si considera che l'intero gruppo è composto da sviluppatori di Bitcoin Core, tra cui Corallo, Newberry, Yanofsky e Falke.

Ciphrex

È stata fondata nel 2014 dallo sviluppatore Core Eric Lombrozo e i suoi prodotti di punta sono il portafoglio multi-firma sicuro per le aziende mSigma e CoinSocket, una piattaforma di sviluppo di applicazioni.
Lombrozo ha dichiarato in passato di collaborare con Core perché crede nel potenziale della tecnologia e perché questa rappresenta una grande opportunità

anche per lui.

L’iniziativa sulla valuta digitale del MIT Media Lab

La Digital Currency Initiative, parte del Media Lab del Massachusetts Institute of Technology (MIT), ha la missione, secondo quanto dichiarato sul suo sito web, di "creare un futuro in cui trasferire valore su Internet sia intuitivo ed efficiente quanto trasferire informazioni". Il suo attuale direttore è Neha Narula.
Come accennato in precedenza, dal 2015 ha assunto Wladimir van der Laan, Gavin Andresen (ora in pensione) e Cory Fields per lavorare a tempo pieno su Bitcoin in completa libertà. Possono persino lavorare su altre implementazioni al di fuori di Bitcoin Core.
Vale la pena notare, tuttavia, che gli stipendi di questi sviluppatori non provengono effettivamente dal MIT. Questa particolare iniziativa è sponsorizzata da diverse aziende e individui, tra cui BitFury, Bitmain, Circle, Chain, Nasdaq, il venture capitalist Fred Wilson e il fondatore di LinkedIn Reid Hoffman.

BTCC

È l'exchange più longevo dell'ecosistema, sebbene l'azienda disponga anche di un pool di mining. Nel 2018 è stato acquisito da un fondo di investimento di Hong Kong, presumibilmente con l'intento di aggirare le rigide misure adottate dalle autorità cinesi in materia

di criptovalute.
Nel 2016, BTCC ha assunto Peter Todd per lavorare allo sviluppo di Bitcoin per un minimo di 14 ore al mese per sei mesi.

Altri

Gregory Maxwell ha affermato che anche Coinbase, Bitmain e Blockchain sono tra i finanziatori di Core. Inoltre, come abbiamo visto con le implementazioni alternative, diverse aziende stanno investendo risorse umane e fondi nello sviluppo di Bitcoin in generale, anche se non specificamente per il ramo Core. Tra queste, BitPay, Purse e Decred.
In ogni caso, l'elenco è tutt'altro che esaustivo, soprattutto considerando l'anonimato che molti sviluppatori hanno scelto di mantenere.
In conclusione, per quanto riguarda chi c'è dietro lo sviluppo di Bitcoin: centinaia di individui, organizzazioni e aziende in tutto il mondo, che contribuiscono con talento e risorse finanziarie. E questo numero continuerà a crescere allo stesso ritmo di Bitcoin stesso.