BITCOIN IN 10 MINUTI

Tutto quello che avete sempre voluto sapere sul Bitcoin

Brought to you by Relai

CHE COS'È IL BITCOIN?

Il Bitcoin, la criptovaluta di maggior successo a livello globale, sta facendo parlare di sé in tutto il mondo. Molti vogliono approfittare del suo successo, altri sono indifferenti o addirittura scettici. La moneta digitale ha suscitato innumerevoli discussioni su denaro, investimenti e tecnologia. Alcuni vedono Bitcoin come puro veicolo di speculazione o lo denunciano come una bolla, mentre altri parlano di innovazione, rivoluzione monetaria o addirittura di riscatto dall'attuale sistema monetario.

Diversi Paesi, tra cui la Cina, vedono il Bitcoin come una minaccia e hanno dichiarato guerra alla criptovaluta. Altri governi, come quello di El Salvador, hanno introdotto il Bitcoin come mezzo di pagamento ufficiale nella speranza di una crescita economica.
Ma cos'è il Bitcoin? È denaro? Oro digitale? Una moda per informatici e speculatori? O qualcosa di completamente diverso? Nei paragrafi che seguono, andremo a fondo nelle risposte a queste domande e daremo un'occhiata più da vicino alla moneta digitale per capire meglio sia la filosofia sia le funzionalità che

la caratterizzano. Per farlo è però importante partire dal principio: la storia delle origini del Bitcoin.

LA STORIA DI BITCOIN

Gli inizi di Bitcoin risalgono ai primi anni Novanta. Nel 1992 un gruppo di scienziati informatici in California creò una mailing list per scambiare idee con persone che la pensavano allo stesso modo su crittografia, matematica, politica e filosofia. Decisero di chiamarsi „Cypherpunks“ - un gioco di parole tra cyberpunk (personaggio della letteratura fantascientifica che è scettico, e a ragione, nei confronti della società) e cipher (criptare).

I Cypherpunks

I Cypherpunks si trasformarono presto in un gruppo eterogeneo. Nonostante i loro diversi background, erano uniti dalla convinzione che Internet sarebbe diventata presto una delle arene più contestate per la libertà umana.
Per difendersi dalla minaccia del controllo, della sorveglianza e della censura di Internet e preservare un Internet libera e aperto, i Cypherpunks hanno usato un'arma potente: la crittografia, ovvero la cifratura delle informazioni.

Nel loro manifesto del 1993 hanno dichiarato: „I cypherpunk scrivono codice [informatico]. Sappiamo che qualcuno deve scrivere software per difendere la privacy, e [...] noi lo scriveremo.

Ma la crittografia da sola non sarebbe sufficiente per un Internet libero. Perché, e i Cypherpunks ne erano convinti, Internet non può essere veramente libero se non ha il proprio denaro. Un denaro indipendente da Stati, banche centrali e aziende; una criptovaluta equa e decentralizzata come Internet stessa.

Esperimenti Monetari

Ma la creazione di denaro digitale e indipendente ha posto i Cypherpunk di fronte a sfide tecniche. Già nel 1990 il crittografo David Chaum aveva creato eCash, la prima criptovaluta della storia, che non era decentralizzata ma garantiva l'anonimato grazie alla crittografia. Tuttavia eCash non fu in grado di affermarsi nei confronti di altri sistemi di pagamento online. La società dietro al progetto dovette dichiarare bancarotta dopo otto anni di servizio ed eCash scomparve.

Seguirono altri tentativi tra i quali spiccava E-Gold. E-Gold era una criptovaluta sostenuta dall'oro e aperta a tutti. Fondata nel 1996, durante l'era delle dot-com, l'azienda sbaragliò i suoi concorrenti elaborando, al suo apice, transazioni per oltre due miliardi di dollari all'anno.

Purtroppo E-gold era controllata da un'istituzione centrale e quindi vulnerabile agli attacchi. Sorsero immediatamente problemi legali tanto che il governo degli Stati Uniti intraprese un'azione legale contro E-Gold. Nel 2008 fu dichiarata colpevole di riciclaggio di denaro e di violazione del Patriot Act da un tribunale statunitense. Tutti i beni furono congelati e E-Gold dovette cessare l'attività.

Questi tentativi falliti hanno dimostrato ai Cypherpunks due fatti. Primo, sia eCash che E-gold erano sostenute da una garanzia collaterale. Questo collaterale si è rivelato un punto debole in quanto poteva essere sequestrato dagli Stati. Conseguentemente una criptovaluta libera non dovrebbe avere punti di attacco centrali, come una società registrata, un conto bancario o un server centralizzato. In secondo luogo, sia i governi sia le autorità di regolamentazione, non hanno interesse a una moneta digitale indipendente dallo Stato.

Per i Cypherpunks la domanda di fondo, per la quale non era ancora stata trovata una soluzione, rimaneva: come può funzionare una moneta digitale indipendente senza un'entità centrale che tenga la contabilità e che si assicuri che il denaro non venga speso due volte? Dopotutto se fosse possibile risolvere il problema della doppia spesa senza affidarsi a una entità centrale, sarebbe possibile creare una moneta digitale libera e che sia nativa di Internet.

Un Atto di Creazione Mistico

Per queste ragioni i Cypherpunks hanno iniziato a discutere su progetti per una criptovaluta senza un'entità centrale e senza garanzie. Due dei concetti più importanti sono stati b-money (1998) e BitGold (2005). Queste idee teoriche, che non sono mai state realizzate nella pratica, erano già molto simili a Bitcoin nella loro concezione. Era prevista una coppia di chiavi pubblica/privata per la crittografia e una Proof-of-Work per la creazione di ulteriori monete digitali, come nel caso del Bitcoin. Nel suo

Whitepaper, l'inventore del Bitcoin ha anche confermato che era a conoscenza di b-money e BitGold.

Tuttavia poiché b-money e BitGold si basavano su un sistema di voto per il consenso (l'accordo su chi possiede quali unità monetarie in un determinato momento), erano vulnerabili ad attacchi malevoli che avrebbero potuto manipolare tali votazioni e quindi distorcere i valori di proprietà.

A quest'ultimo problema, che ancora ostacolava la creazione di una nuova moneta su Internet, è stata presentata una soluzione venerdì 31 ottobre 2008. Quel giorno il Whitepaper di Bitcoin, in cui Satoshi Nakamoto spiega il suo concetto di rete di pagamento decentralizzata, venne inviato via e-mail ai Cypherpunks. Due mesi dopo, il 3 gennaio 2009, la rete Bitcoin è entrata in funzione.

Sebbene le reazioni iniziali alla nuova rete siano state piuttosto fredde, alcuni appassionati iniziarono a testarla ed a segnalare errori. All'inizio, tuttavia, fu soprattutto Satoshi Nakamoto a mantenerla in funzione. Poi, lentamente, la notizia della nuova moneta di Internet si diffuse nei forum di informatica e tecnologia e l'interesse per la rete crebbe. Dopo un anno la rete Bitcoin contava già diversi utenti. Il bitcoin stesso, tuttavia, non aveva ancora valore.

Chi è Satoshi Nakamoto?

Il Whitepaper di Bitcoin, così come la comunicazione via e-mail dell'inventore di Bitcoin, sono stati entrambi firmati con il nome di Satoshi Nakamoto. Tuttavia la vera identità dell'inventore dei Bitcoin rimane tuttora sconosciuta poiché il suo nome sembra essere uno pseudonimo. Per rivolgersi ai suoi sodali e successivamente alla comunità degli sviluppatori di Bitcoin, Nakamoto ha utilizzato almeno tre diversi indirizzi e-mail che criptava accuratamente per nascondere la vera identità del mittente.

Diverse persone hanno già affermato di essere Satoshi Nakamoto ma fino a oggi nessuno di loro è riuscito a dimostrarlo. La prova definitiva, ovvero l'invio di bitcoin da uno degli indirizzi dei portafogli che molto probabilmente appartengono a Satoshi, non è stata ancora fornita da nessuno.

Inoltre il gruppo di coloro che hanno comunicato „personalmente" con Satoshi Nakamoto via Internet è molto ristretto. Satoshi Nakamoto ha scritto il suo ultimo messaggio alla comunità Bitcoin il 12 dicembre 2010 ma non si trattava affatto di un messaggio d'addio: Satoshi ha semplicemente smesso di comunicare.

Il suo ritiro, tuttavia, è stato solo nei confronti della comunità più ampia. Nakamoto ha continuato a riunire intorno a sé un gruppo di programmatori che teneva informati sugli ulteriori sviluppi della rete Bitcoin ma, nell'aprile 2011, ha inviato un ultimo messaggio anche a questo gruppo.

Così come era apparso misteriosamente nel 2008, Nakamoto scomparve altrettanto misteriosamente tre anni dopo.

Il „Pizza Day“ di Bitcoin

Ma come ha fatto il Bitcoin ad acquisire valore? All‘inizio i bitcoin potevano essere estratti e inviati tra i membri della rete ma le unità digitali non avevano valore. Inoltre, il gruppo di coloro che conoscevano il Bitcoin, per non parlare della possibilità di inviarlo e riceverlo, era ancora molto ristretto.

La situazione è cambiata il 22 maggio 2010 quando una richiesta insolita è apparsa sul forum Internet bitcointalk.org. Un uomo della Florida di 28 anni, di nome Laszlo Hanyecz, offrì 10.000 bitcoin a chi avesse ordinato due pizze da far consegnare al proprio domicilio. Uno studente californiano accettò l‘offerta e così gli furono consegnate a casa due pizze grandi del valore di 41 dollari. In cambio Hanyecz inviò allo studente i 10.000 bitcoin.

Da quel giorno, il 22 maggio viene celebrato ogni anno dai Bitcoiners come il „Pizza Day“ di Bitcoin.
La data è diventata popolare perché illustra tre cose:

- i bitcoin hanno valore
- i bitcoin sono adatti come mezzo di scambio e di pagamento
- il bitcoin come valuta è deflazionistico. Il numero di bitcoin aggiuntivi messi in circolazione diminuisce costantemente, caratteristica questa che può portare a un aumento del valore.

Le due pizze sono entrate nei libri di storia come le più costose al mondo. Calcolando il loro costo con il prezzo dei bitcoin del dicembre 2021, sono state pagate ben 460 milioni di dollari USA. Si tratta di un sacco di soldi. Ma chi ha ricevuto i 10.000 bitcoin li ha già spesi. In un‘intervista lo studente ha dichiarato di aver venduto i bitcoin non molto tempo dopo per poter fare un viaggio - al prezzo odierno dei bitcoin probabilmente il viaggio più costoso della storia dell‘uomo.

Il „Pizza Day“ del Bitcoin illustra anche in modo impressionante il motivo per cui l‘ ‘hodling’ - derivato da ‘to hold’ - è così popolare tra i Bitcoiners. ‘Hodling’ significa conservare i propri Bitcoin per lunghi periodi con l‘intento di non venderli (possibilmente) mai. Dopo tutto chi vuole spendere i propri bitcoin oggi quando potrebbero valere il doppio, il triplo o addirittura dieci volte tanto negli anni a venire?

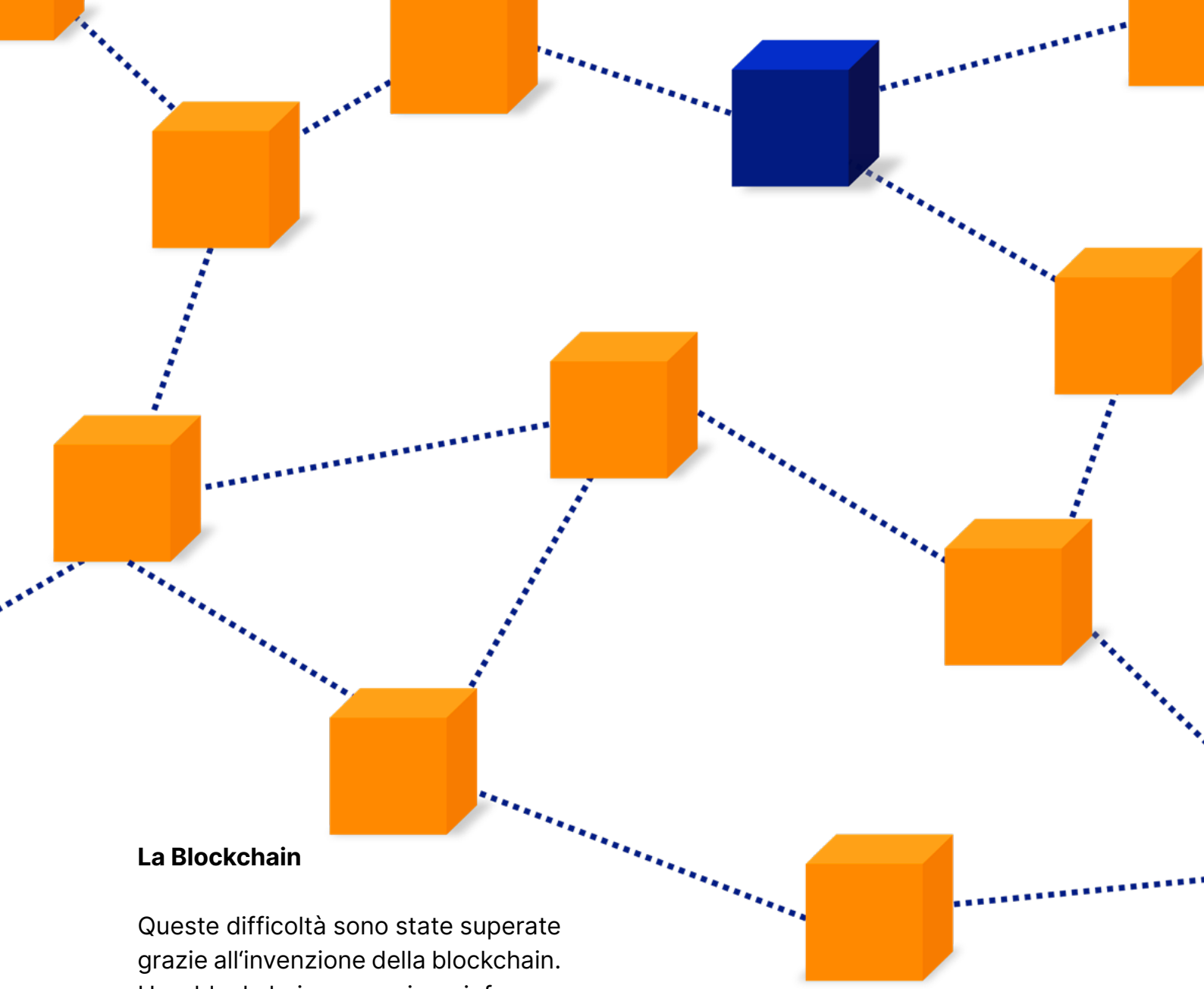
COME FUNZIONA BITCOIN?

Dopo aver appreso la storia del Bitcoin ci addentreremo ora nel suo funzionamento. L'obiettivo è capire come funziona la rete Bitcoin, quali problemi risolve e quali sono i suoi vantaggi pratici.

L'intento di Bitcoin è quello di essere una rete decentralizzata. Nessun partecipante alla rete dovrebbe essere in grado di governarla da solo: il potere decisionale e la supervisione sono distribuiti tra tutti i partecipanti. Questo aspetto è importante perché nessun individuo, nessun governo e nessuna azienda può cambiare la rete in modo indipendente, i cambiamenti sono possibili solo collettivamente.

Bitcoin funziona in modo tale che ogni partecipante alla rete abbia sempre una copia identica del registro di proprietà più aggiornato - di conseguenza tutti sanno sempre chi possiede quali bitcoin. Pertanto nessuno può affermare di possedere più bitcoin di quanti ne possieda perché ogni partecipante alla rete può verificare questa affermazione con la propria copia del registro di proprietà e dimostrarla falsa.

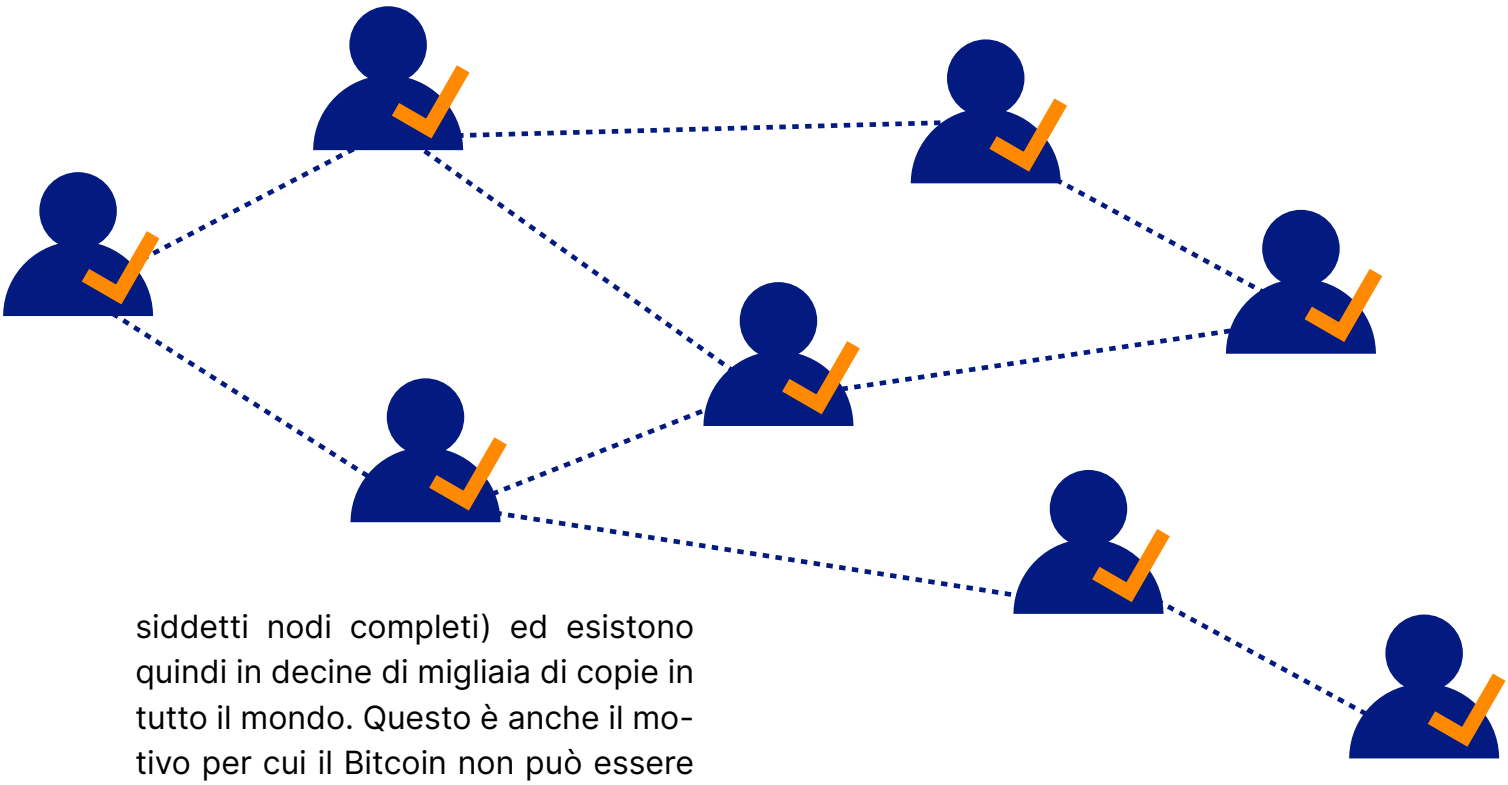
Prima del lancio del Bitcoin le reti decentralizzate dovevano affrontare due grandi sfide. In primo luogo come assicurarsi che tutti i partecipanti ricevano gli ultimi aggiornamenti sui cambiamenti di proprietà, cioè le informazioni su quali bitcoin sono stati trasferiti e a chi. In secondo luogo, come possono i partecipanti verificare con assoluta certezza che le informazioni ricevute siano corrette.
.



La Blockchain

Queste difficoltà sono state superate grazie all'invenzione della blockchain. Una blockchain memorizza informazioni e dati in ordine cronologico. Nel caso di Bitcoin tutte le transazioni effettuate dalla creazione sono archiviate in ordine cronologico in decine di migliaia di blocchi che insieme formano la blockchain di Bitcoin. Qualsiasi partecipante alla rete che voglia sapere chi possiede quali bitcoin può tracciare la cronologia delle transazioni sulla blockchain e determinare con esattezza chi possiede quanti bitcoin in quel preciso momento. In questo modo, se qualcuno vuole inviare un bitcoin, chiunque può verificare se questo bitcoin appartiene veramente alla persona in questione.

Fino a questo punto questo meccanismo non rappresenta una novità poiché le banche utilizzano già un processo simile. Se un cliente vuole spendere un franco svizzero, la banca consulta la cronologia delle transazioni per vedere se il franco appartiene ancora al cliente o se è già stato speso (inviato a qualcun altro). La caratteristica unica di una blockchain, tuttavia, è che queste informazioni non sono memorizzate su un server della banca centrale ma sui computer di tutti i partecipanti alla rete (i co-



siddetti nodi completi) ed esistono quindi in decine di migliaia di copie in tutto il mondo. Questo è anche il motivo per cui il Bitcoin non può essere semplicemente cancellato: per farlo bisognerebbe eliminare nello stesso momento la copia della blockchain da tutti i computer dei partecipanti in tutto il mondo.

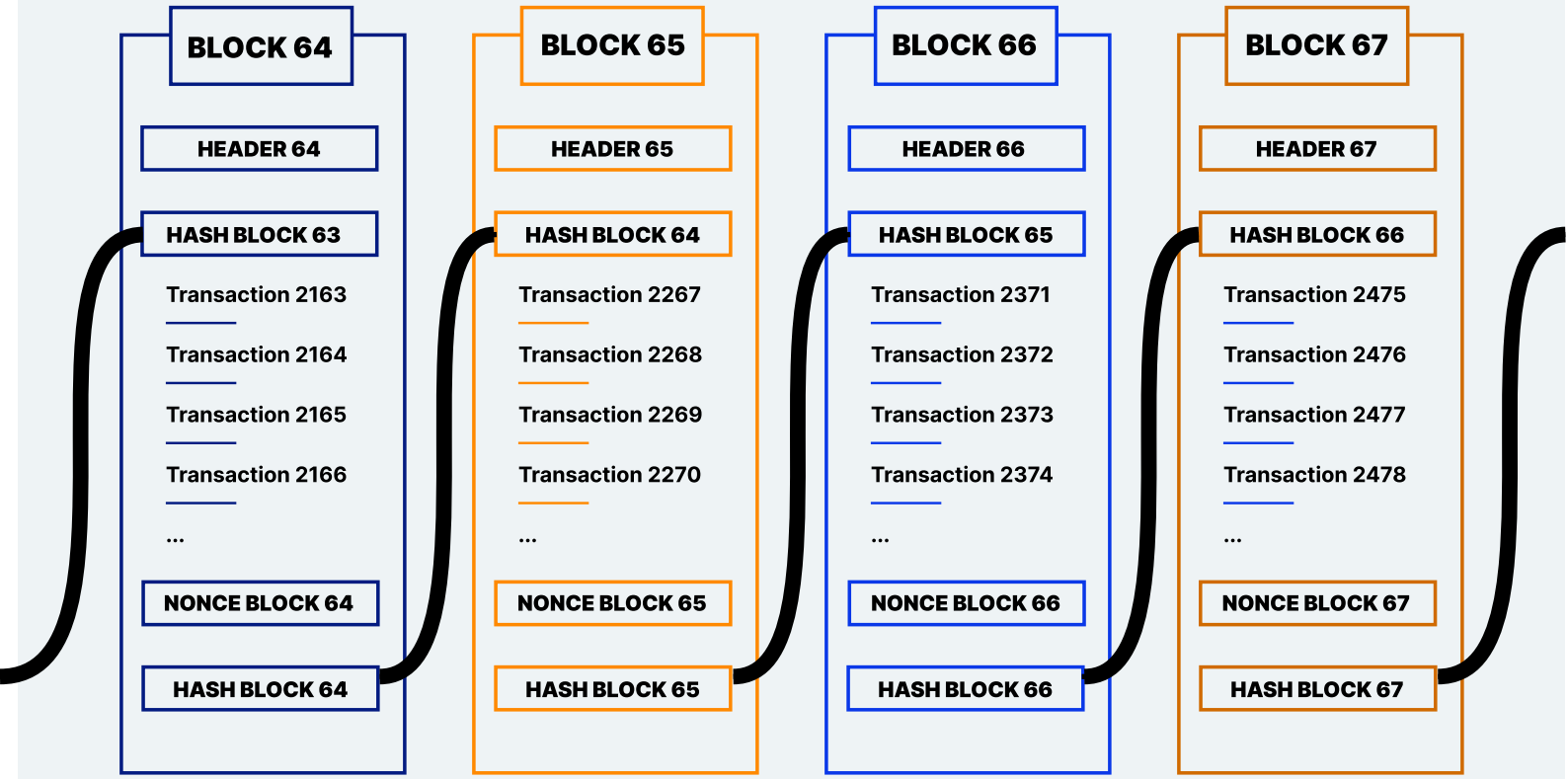
Tuttavia la sfida che le blockchain si trovano ad affrontare è che ogni partecipante alla rete deve essere in grado di determinare con assoluta certezza che la propria copia della blockchain sia corretta e che non vi siano transazioni errate o fraudolente nella propria copia del libro mastro. Poiché alla blockchain vengono aggiunti nuovi blocchi con nuove transazioni ogni 10 minuti circa, la blockchain cresce costantemente e deve essere aggiornata continuamente su tutti i computer dei partecipanti in tutto il mondo.

Questi nuovi blocchi devono essere verificabili da tutti. La verifica viene effettuata utilizzando regole immutabili definite nel codice informatico della rete Bitcoin. Queste regole definiscono esattamente quali transazioni sono consentite e quali no. Ogni utente che scarica la copia della blockchain può quindi verificare se tutte le transazioni sono conformi alle regole stabilite. Se una transazione viola le regole, cioè se è errata o fraudolenta, viene rifiutata dai partecipanti alla rete (nodi completi) e non viene inclusa nella blockchain.

Proof-of-Work (PoW) Mining

La rete Bitcoin dispone di un meccanismo per limitare l'aggiunta di nuovi blocchi. Se nuove transazioni e nuovi blocchi potessero essere aggiunti alla blockchain da chiunque, la rete finirebbe nel caos in quanto la blockchain non sarebbe in grado di aggiornarsi in tutto il mondo abbastanza velocemente.

Per evitare ciò Bitcoin funziona con un meccanismo di Proof-of-Work. Affinché qualcuno si guadagni il diritto di aggiungere un nuovo blocco alla



La cabecera, el resultado de la función hash del bloque anterior, todas las transacciones del bloque actual y un Nonce (número aleatorio) se introducen en una función matemática. El Nonce se cambia hasta que el resultado de la función hash tiene suficientes ceros precedentes. Este proceso se denomina minería.

blockchain deve fornire una prova di lavoro. Una semplice descrizione di questo processo può essere rappresentata da un gruppo di persone che cerca aghi in un pagliaio. Chi trova per primo un ago è autorizzato ad aggiungere un nuovo blocco alla blockchain. Inoltre chi lo trova viene ricompensato con nuove unità di bitcoin e con le commissioni di transazione contenute nel blocco. Non appena il blocco è stato aggiunto il processo ricomincia.

In realtà i minatori eseguono una funzione matematica di hash (algoritmo di hash SHA-256) alla ricerca di numeri specifici. L'hash del blocco precedente, le transazioni del blocco corrente e un numero casuale (nonce) vengono inseriti in un hash. Il numero casuale viene modificato finché la funzione hash non produce un risultato con un numero minimo di zeri iniziali. Ad esempio, il blocco #700000, creato l'11 settembre 2021, ha il seguente hash valido:

00000000000000000590fc0f3eba193a278534220b2b37e 9849e1a770ca959.

La ricerca di questo numero, chiamata anche mining, ha due funzioni principali: in primo luogo collega i blocchi in modo matematico-crittografico per fare in modo che tutti possano verificare facilmente l'ordine corretto. Allo stesso tempo, il meccanismo di Proof-of-Work, rende quasi

impossibile cambiare questo ordine. In secondo luogo questo meccanismo ritarda l'aggiunta di nuovi blocchi in modo tale che, in media, un nuovo blocco venga aggiunto alla blockchain solo ogni 10 minuti. In questo modo tutti i partecipanti alla rete mondiale hanno il tempo sufficiente per aggiornarsi all'ultimo stato della blockchain.

In sintesi, i minatori mantengono in funzione la rete Bitcoin. Grazie a loro le nuove transazioni vengono elaborate e aggiunte alla blockchain. I nodi completi mantengono le copie del libro mastro, si assicurano che le regole siano rispettate e assicurano che nessuna transazione errata o fraudolenta entri nella blockchain.

21 milioni di Bitcoin

Sebbene vengano costantemente aggiunti altri blocchi alla blockchain di Bitcoin e i minatori vengano ricompensati per questo lavoro con nuovi bitcoin, il loro numero totale è limitato a 21 milioni. Non ci saranno mai più di 21 milioni di bitcoin. Ma questi 21 milioni di monete non sono stati in circolazione fin dall'inizio. Piuttosto, vengono rilasciati dal codice Bitcoin secondo un rigoroso programma di emissione.

Quando il Bitcoin è stato lanciato, il codice rilasciava 50 nuovi bitcoin ai minatori ogni 10 minuti circa. Quattro anni dopo il lancio il numero di bitcoin rilasciati ogni dieci minuti si è dimezzato. Questo processo è chiamato 'dimezzamento' (halving) e descrive il fatto che la ricompensa dei blocchi per i minatori diminuisce della metà ogni quattro anni. Attualmente sono già in circolazione 19 milioni di bitcoin. I restanti saranno estratti fino all'anno 2140 dopodiché i minatori saranno ricompensati solo attraverso le commissioni di transazione.

La quantità strettamente limitata di unità di bitcoin è una delle proprietà fondamentali della criptovaluta e rende il Bitcoin un bene estremamente scarso. Questa assoluta scarsità digitale è anche un importante prerequisito per la funzione del Bitcoin come riserva di valore nel lungo periodo ed è il motivo per cui viene spesso definito oro digitale o oro 2.0.

Il risultato: Proprietà digitale

Esaminando insieme tutte le caratteristiche della rete Bitcoin si capisce l'importanza di questa invenzione. Per la prima volta nella storia esiste un bene digitale che è disponibile solo in un numero strettamente limitato. I bitcoin non possono essere copiati o duplicati.

Grazie a questo risultato il Bitcoin viene spesso definito proprietà digitale perché, proprio come ogni terreno del pianeta, è unico ed esiste una sola volta. Così come anche ogni unità di bitcoin è unica ed esiste una sola volta nello spazio digitale.

Queste unità bitcoin possono essere realmente possedute ma solo la persona proprietaria della corrispondente chiave privata, che è una combinazione di numeri e lettere composta da 64 caratteri, può muovere i bitcoin associati. In altre parole, senza questa chiave privata, i bitcoin non possono essere rubati, confiscati o bloccati. Questo permette al proprietario di avere un controllo assoluto sulle proprie risorse finanziarie, indipendentemente dal fatto che si tratti di un milionario, un rifugiato politico o un creditore perseguitato. Per la prima volta dall'invenzione del computer è possibile possedere veramente beni digitali.

PERCHÉ BITCOIN?

Ma perché tutto questo clamore intorno al Bitcoin? La possibilità di possedere veramente un bene digitale può essere rivoluzionaria. E perché qualcuno dovrebbe voler possedere i bitcoin?

Il Meglio dei Due Mondi

Nei secoli passati metalli preziosi e successivamente il denaro contante, sotto forma di monete e banconote, venivano usati come mezzi di pagamento. Questi ultimi avevano il vantaggio di poter essere conservati e spesi indipendentemente da terzi. Il detto „il contante è la libertà stampata“ riassume molto bene questo concetto. Tuttavia lo svantaggio dei metalli preziosi e del contante è che sono difficili da usare nello spazio digitale di Internet. Infatti, con l‘avvento dello shopping online, le carte di debito e di credito si sono affermate tra la popolazione.

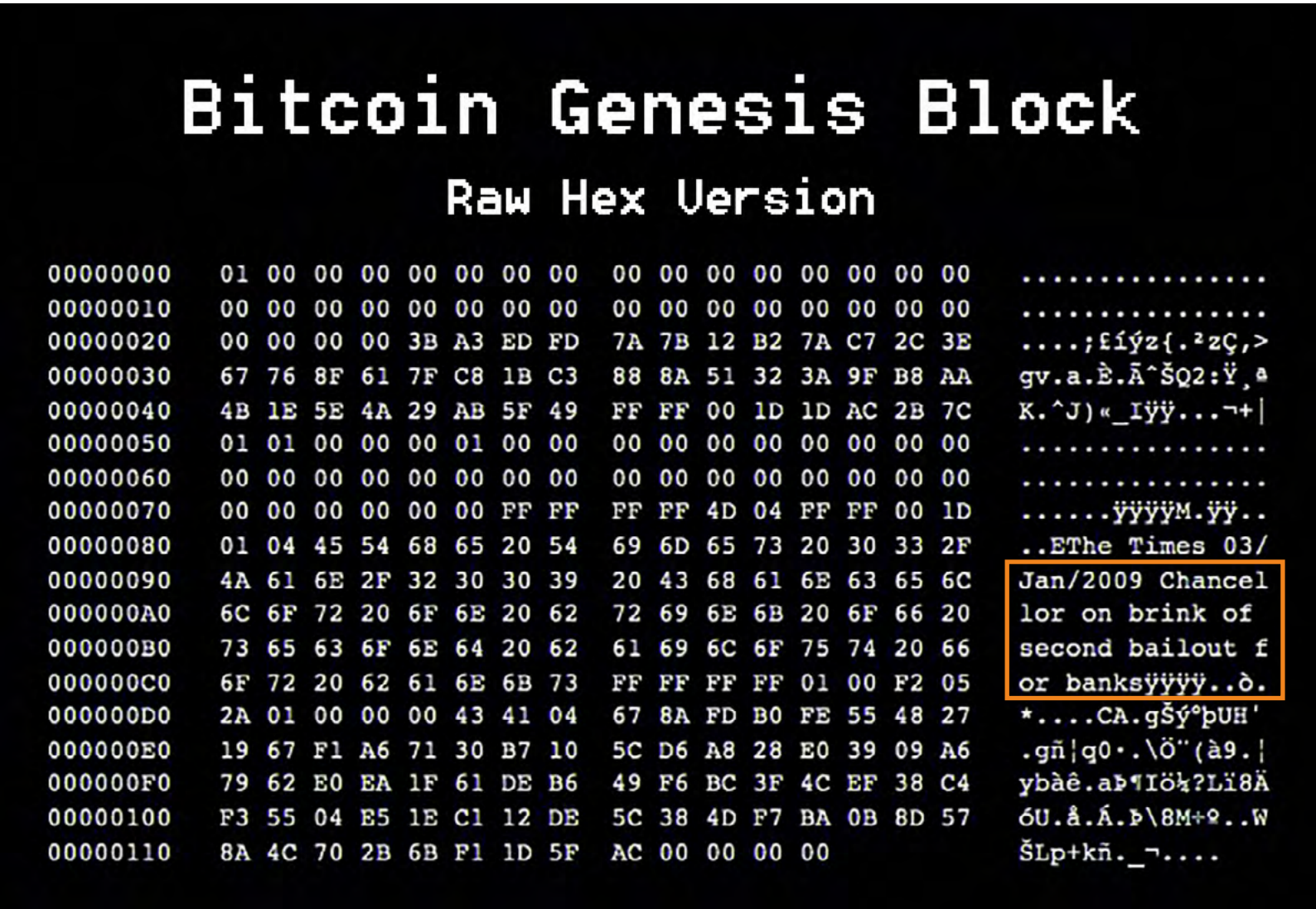
Ma ora che la maggior parte delle persone utilizza il denaro digitale attraverso i propri conti bancari al posto del contante, i rischi di controparte a cui vanno incontro aumentano. Se, per esempio, un‘istituzione finanziaria si dichiara insolvente, i risparmi dei clienti potrebbero andare persi. Oppure, come è successo a Cipro nel 2013, se vengono fortemente limitati i prelievi di contante , se sono messi in atto i controlli sui capitali e se si verifica un‘espropriazione forzata dei conti di risparmio, allora vuol dire che le persone non hanno più il controllo del proprio denaro. Oppure ancora, come avviene attualmente in molti paesi occidentali, se ai clienti delle banche non è permesso di inviare denaro ai parenti perché vivono a Cuba o in Iran, significa che si stanno affidando a una terza parte per l‘approvazione di tutte le loro transazioni. Con il passaggio dal denaro cartaceo a quello digitale, memorizzato nei conti bancari, in definitiva non abbiamo più il controllo del nostro denaro. Finora, tuttavia, questo aspetto negativo è stato il prezzo da pagare per partecipare a una vita digitalizzata.
Bitcoin offre una soluzione a questo dilemma. Come moneta digitale

è ideale per l'uso nello spazio digitale e allo stesso tempo può essere conservato come proprietà digitale senza dover dipendere da terze parti (banche) per la custodia in sicurezza. I possessori di bitcoin possono quindi conservare le proprie monete - sotto forma di chiavi private - sotto il materasso o dove ritengono sia più sicuro.

Tempismo Perfetto

Il Bitcoin è stato creato nel corso della crisi finanziaria mondiale del 2008/09. Nel primo blocco della blockchain - chiamato anche blocco Genesi - Satoshi Nakamoto ha lasciato un messaggio forte e chiaro. Ha citato un titolo pubblicato sul quotidiano The Times che recitava: „Il cancelliere sull'orlo di un secondo salvataggio per le banche".

Con questo gesto Satoshi ha espresso la filosofia critica dei Cypherpunks nei confronti dello Stato. Nella crisi finanziaria del 2008 le banche centrali hanno messo in circolazione grandi quantità di nuovo denaro per salvare le banche. Alla fine, però, a pagarne le conseguenze sono stati i risparmiatori che hanno visto diminuire il valore del loro denaro a causa della diluizione della massa monetaria. Questo fatto consolidò ulteriormente la sfiducia dei Cypherpunks nei confronti dello Stato e delle banche centrali e rafforzò la loro convinzione che un denaro indipendente dallo Stato fosse necessario e urgente.



La stessa procedura, ma su scala più ampia, si è ripetuta allo scoppio della pandemia di Covid-19. Nel solo anno 2020, l'offerta di moneta statunitense è stata ampliata del 50% e in altri paesi, tra cui la Svizzera, la macchina da stampa digitale continua a funzionare costantemente. Una conseguenza diretta sono i tassi d'interesse ai minimi storici, addirittura negativi in Svizzera, e una forte inflazione degli asset.

Copertura contro la Svalutazione Monetaria

Il Bitcoin è stato quindi lanciato nel momento migliore. Rispetto al momento attuale, raramente la questione del denaro è stata più rilevante e i punti interrogativi più grandi. Con la sua offerta limitata a 21 milioni di unità, Bitcoin rappresenta un piacevole contrasto con la crescita infinita dei bilanci delle banche centrali. La sua offerta limitata costituisce una protezione contro la diluizione del proprio capitale, al contrario di quanto è avvenuto con tutte le valute del mondo negli ultimi decenni.

Grazie alla sua specifica configurazione, il bitcoin è stato progettato per garantire la conservazione del potere d'acquisto per lunghi periodi. Essendo scarso, il bitcoin dovrebbe svolgere questo compito meglio dell'oro che ha un afflusso netto dell'1-2% ogni anno. Inoltre i costi di immagazzinamento e trasporto del bitcoin sono significativamente inferiori rispetto all'oro, aspetto che consente una migliore conservazione del valore nel tempo..

Protezione della proprietà

Un altro problema che il Bitcoin attenua è la protezione della proprietà. Mentre l'oro o il denaro contante devono essere conservati in modo sicuro e con grandi spese per proteggerli dal furto, il bitcoin può essere conservato e trasportato praticamente a costo zero. Anche importi consistenti possono essere portati in qualsiasi parte del mondo utilizzando solo un codice composto da dodici o ventiquattro parole. Una volta memorizzato e distrutto fisicamente, questo codice non può essere rubato da nessuno al punto da permettere al suo proprietario di portare i suoi bitcoin con sé nella tomba, se lo desidera.

ACQUISTARE BITCOIN

Ci sono due modi per entrare in possesso di bitcoin. O si guadagnano come minatori o si acquistano da un'altra persona. Dal momento che il mining con i dispositivi domestici è diventato virtualmente impossibile, l'unico modo che rimane ai nuovi arrivati è quello di acquistarli.

Crypto Exchanges & Brokers

Il modo più semplice per acquistare bitcoin è attraverso un crypto exchange o un broker. Questi funzionano in modo simile alle piattaforme di trading azionario. Dopo aver aperto un conto personale è possibile trasferire Franchi Svizzeri, Euro o Dollari USA tramite bonifico o carta di credito. Una volta che il denaro è arrivato sul conto personale, bitcoin può essere acquistato al prezzo di mercato corrente 24 ore su 24, 7 giorni su 7, con pochi clic. In Europa è possibile acquistare bitcoin senza registrazione, né verifica, né deposito di denaro, con la popolare app di investimento per soli bitcoin Relai.

Peer-to-peer

In alternativa ai crypto exchange, i bitcoin possono anche essere acquistati direttamente da altri operatori di mercato tramite piattaforme peer-to-peer senza dover ricorrere a un exchange. Questo permette un maggiore anonimato poiché nel processo non si rivelano dati personali.

ATM Bitcoin

Esiste anche la possibilità di prelevare bitcoin tramite appositi bancomat.

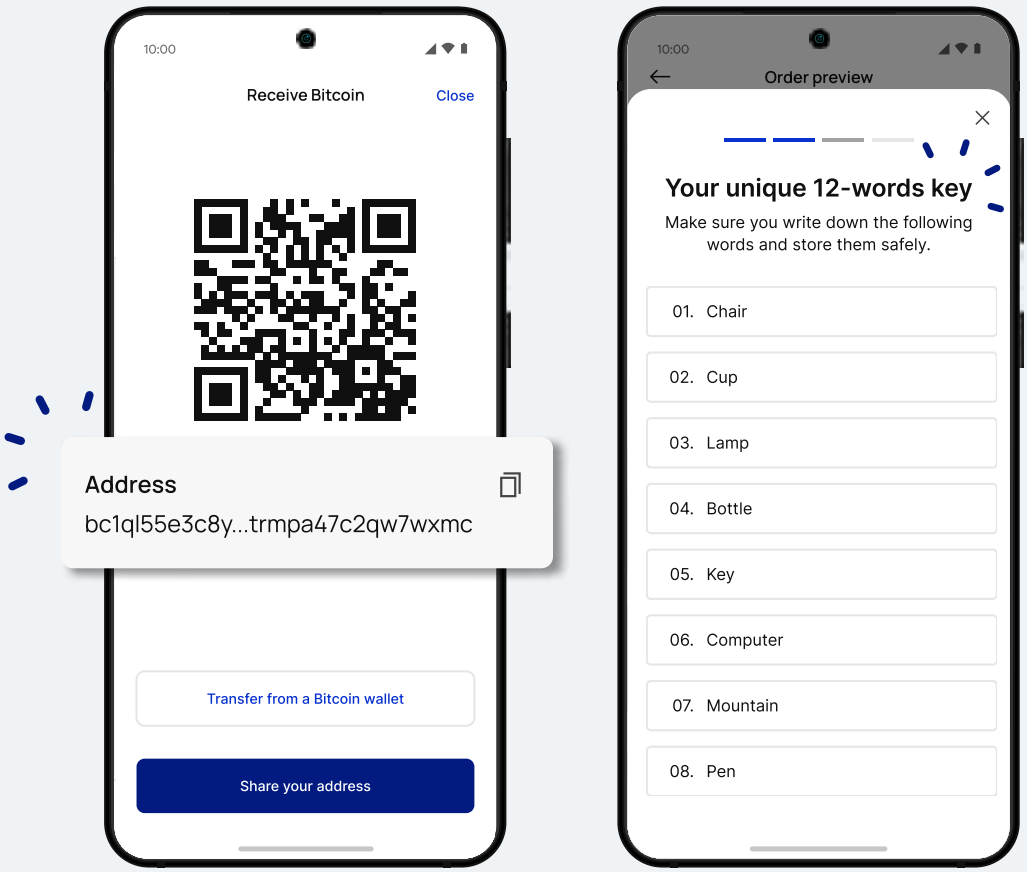
Questi sono già disponibili in molti paesi tra cui Svizzera, Germania, Austria e Italia. Presso gli sportelli bancomat Bitcoin è possibile prelevare in modo anonimo con contanti o carta di credito. Non è necessario essere già registrati o avere un portafoglio crypto esistente.

Conservare Bitcoin in modo sicuro

Una volta acquisiti i bitcoin, si pone il problema della loro gestione e conservazione sicura. I bitcoin e le criptovalute sono governati dal principio: „non le tue chiavi, non le tue monete“. Per possedere effettivamente i propri bitcoin è necessario avere il controllo delle relative chiavi private. Questa espressione un po' tecnica significa che si ha realmente il controllo sui propri bitcoin solo se li si memorizza in un portafoglio digitale personale di cui si possiedono le chiavi private. Finché i bitcoin sono depositati su un crypto exchange sono sotto il controllo di quest'ultimo. Se l'exchange viene violato o va in bancarotta, i bitcoin potrebbero essere persi per sempre.

Auto-custodia

A differenza di un conto bancario, Bitcoin offre la possibilità di conservare le proprie unità monetarie in un portafoglio personale. Questo vi permette di essere la vostra banca e ha il vantaggio di farvi avere il controllo assoluto sui vostri bitcoin. D'altro canto ciò comporta anche delle responsabilità. La chiave privata, che spesso si presenta sotto forma di dodici o ventiquattro parole, deve essere conservata e tenuta al sicu-



ro dal proprietario stesso dei bitcoin. Una gestione errata o negligente può portare alla perdita irrevocabile dei bitcoin.

Portafogli: Portafogli digitali

I portafogli digitali (wallet) aiutano a conservare in modo sicuro i bitcoin o, più precisamente, le chiavi private. I bitcoin sono sempre memorizzati sulla blockchain e non possono essere trasferiti a un portafoglio. Solo le chiavi di accesso ai bitcoin possono essere memorizzate in un portafoglio.

I portafogli sono stati quindi creati per conservare le chiavi private in modo sicuro e semplice. Inoltre essi consentono di inviare e ricevere bitcoin con pochi clic. I portafogli sono quindi uno strumento utile per gestirli.

Portafogli Software

I portafogli più comuni sono i portafogli software. I portafogli software possono essere configurati come applicazioni desktop o come applicazioni per smartphone. Durante la configurazione le chiavi private del portafoglio sono elencate sotto forma di dodici o ventiquattro parole (seed phrase).

Queste parole sono l'equivalente dei bitcoin in quel portafoglio. Chiunque conosca queste parole ha il controllo sulle monete, pertanto le parole devono essere trascritte in modo fedele, preferibilmente su carta, in segreto e tenute al sicuro. Se il computer o lo smartphone dovessero essere smarriti o rubati, il portafoglio può essere ripristinato in qualsiasi momento grazie a queste parole.

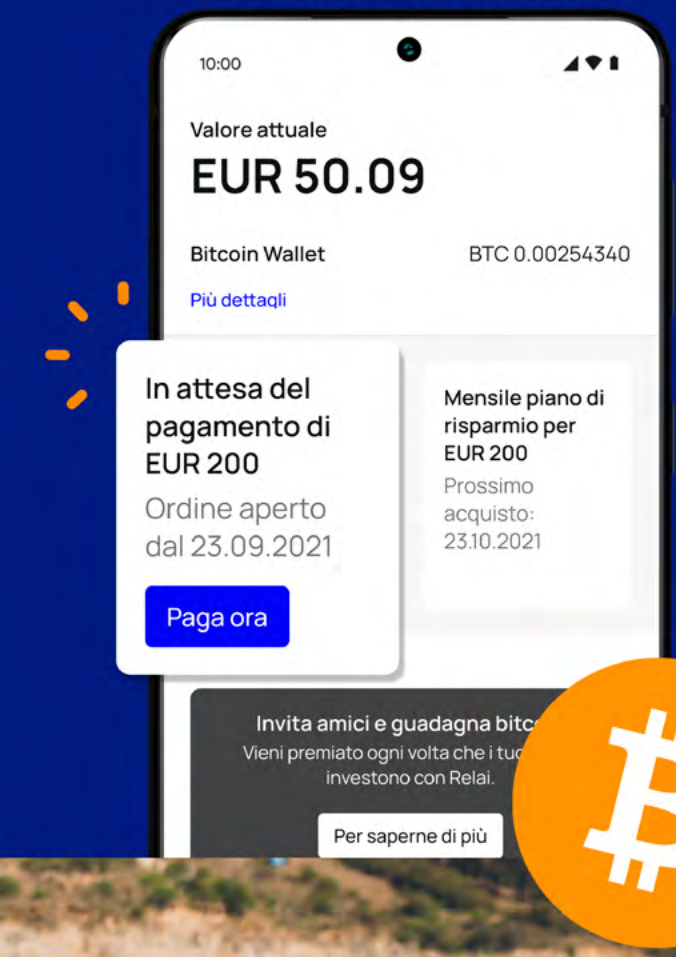
I portafogli software hanno il vantaggio di poter essere configurati rapidamente e di essere facili da usare. Tuttavia, poiché i portafogli software sono programmi informatici installati su un dispositivo e collegati direttamente a Internet, c'è sempre il rischio di attacchi da parte di hacker.

Portafogli Hardware

Se tenete alla sicurezza dovreste invece utilizzare un portafoglio hardware. Questi piccoli dispositivi memorizzano i codici di accesso per i bitcoin su un dispositivo simile a una chiavetta USB che viene collegato al computer solo quando è necessario. Il dispositivo è progettato in modo tale che anche un computer infettato da malware o virus non possa compromettere l'accesso ai codici.

Quando si configura un portafoglio hardware vengono generate dodici o ventiquattro parole (seed phrase) che devono essere trascritte fedelmente e conservate al sicuro. Se il portafoglio hardware viene perso può essere ripristinato con l'aiuto delle parole. Esempi di portafogli hardware sono BitBox e Trezor.

Made in Switzerland



L'APP BITCOIN PIÙ *SEMPLICE* D'EUROPA

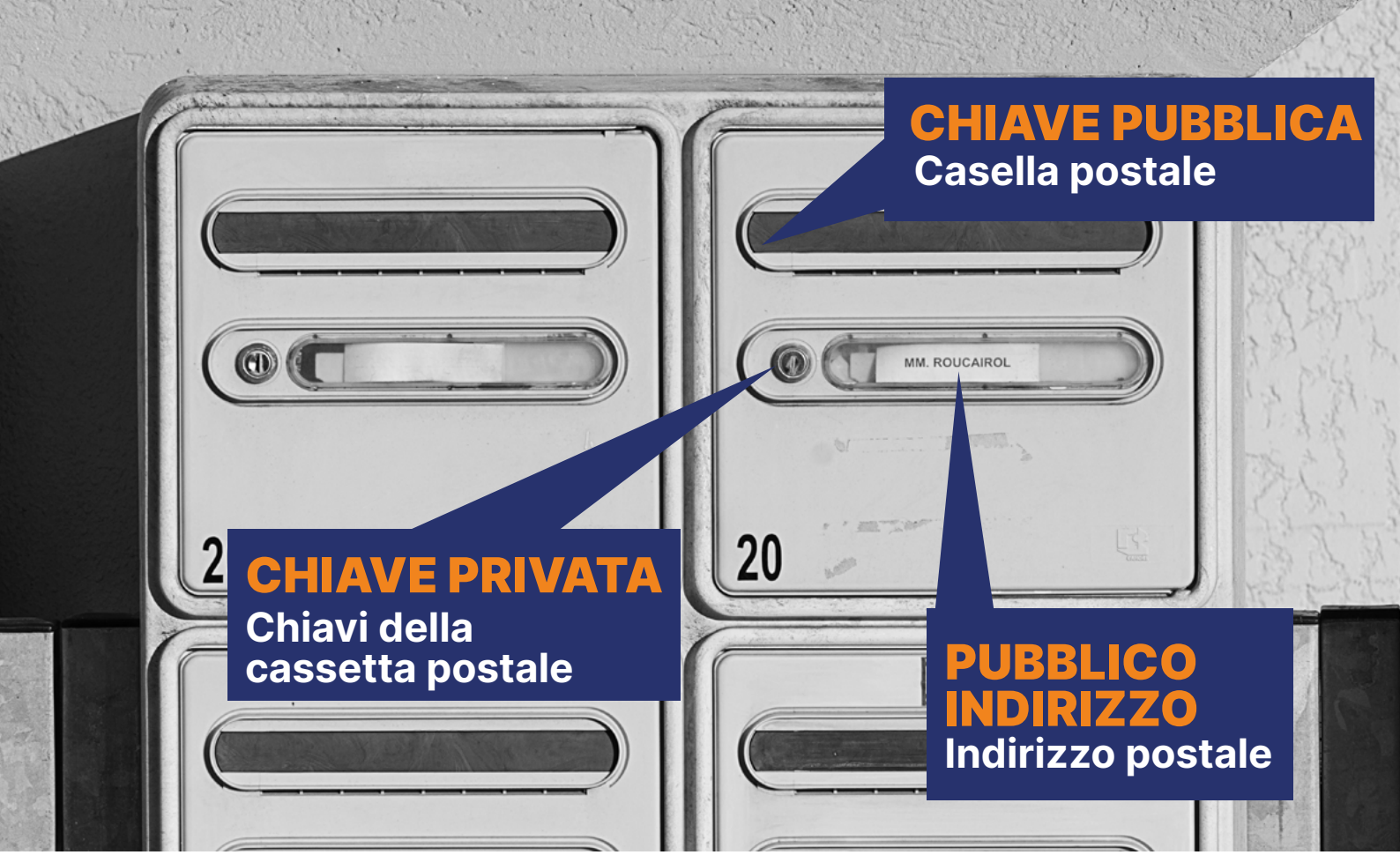
Bitcoin ricevuti	BTC 0.00254340
24.09.2021	CHF 50.65

Relai

Download on the App Store

GET IT ON Google Play

Acquistate bitcoin in 1 minuto da appena 10 EUR/CHF senza verifica.



Inviare e ricevere bitcoin

Inviare e ricevere bitcoin è molto semplice. Ogni portafoglio bitcoin ha il suo indirizzo pubblico generato dalla cosiddetta chiave pubblica. Questo serve come indirizzo di ricezione, simile a un IBAN. Chiunque sia in possesso di questo indirizzo può inviare bitcoin al portafoglio corrispondente. L'indirizzo viene spesso visualizzato come codice QR per semplificare ulteriormente la gestione.

Se si desidera inviare bitcoin a qualcuno è possibile inserire l'indirizzo bitcoin del destinatario nel proprio portafoglio alla voce „invia" oppure scansionare il codice QR corrispondente. Le spese di transazione vengono automaticamente detratte dal portafoglio del mittente. L'importo delle commissioni di transazione varia a seconda del carico della rete e può essere consultato qui. Sono necessari in media 10 minuti affinché il trasferimento raggiunga il destinatario. Tuttavia possono essere necessari anche tempi più lunghi a seconda dell'entità delle commissioni di transazione che si è disposti a pagare.

Pagare con Bitcoin

Quando il Bitcoin è stato creato, si sperava che un giorno potesse essere utilizzato per pagare i beni di uso quotidiano. In teoria oggi questo è già possibile. Alcuni dipartimenti fiscali governativi, organizzazioni no-profit e un numero crescente di aziende, accettano il bitcoin come mezzo di pagamento. Ma poiché le transazioni attraverso la rete Bitcoin possono costare diversi euro di commissione e richiedere almeno 10 minuti, ques-

to ha senso solo per importi elevati. Per inviare bitcoin in modo rapido ed economico è necessaria una soluzione alternativa.

La rete Lightning:
più veloce e più economica

E' stato quindi costruito un livello aggiuntivo sulla rete Bitcoin. Questa seconda rete, chiamata Lightning, permette di pagare in bitcoin in pochi secondi a un costo minimo. In paesi come El Salvador la rete Lightning è già utilizzata attivamente e con successo.
In futuro il pagamento di beni di uso quotidiano con bitcoin avverrà quindi in gran parte attraverso la rete Lightning. Gli sviluppi in questo settore procedono a pieno ritmo. Twitter, per esempio, ha recentemente introdotto una funzione di „mancia" che utilizza la rete Lightning. Anche l'app Strike offre pagamenti in tutto il mondo in varie valute a costo zero tramite la rete Lightning. È quindi prevedibile che in futuro solo gli importi più elevati saranno regolati direttamente tramite la rete Bitcoin mentre tutte le altre transazioni saranno effettuate tramite la rete Lightning.
Poiché attraverso la rete Lightning vengono inviati soprattutto importi di minore entità, come unità di conto vengono utilizzati i Satoshi, o in breve Sats, che sono utilizzati al posto dei bitcoin. 1 bitcoin equivale a 100.000.000 di sats. Per utilizzare la rete Lightning è necessario creare un portafoglio Lightning.

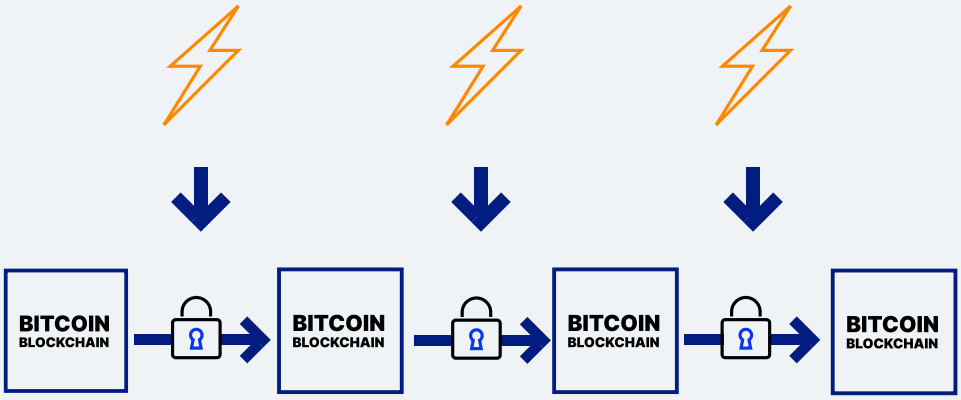
UNO SGUARDO AL FUTURO

Nei suoi oltre dieci anni di vita, il Bitcoin ha attraversato molti alti e bassi. Più volte la criptovaluta è stata dichiarata morta o è caduta nell'oblio del grande pubblico dopo pesanti perdite di valore. Tuttavia nell'ultimo decennio il Bitcoin si è diffuso inesorabilmente in tutto il mondo.

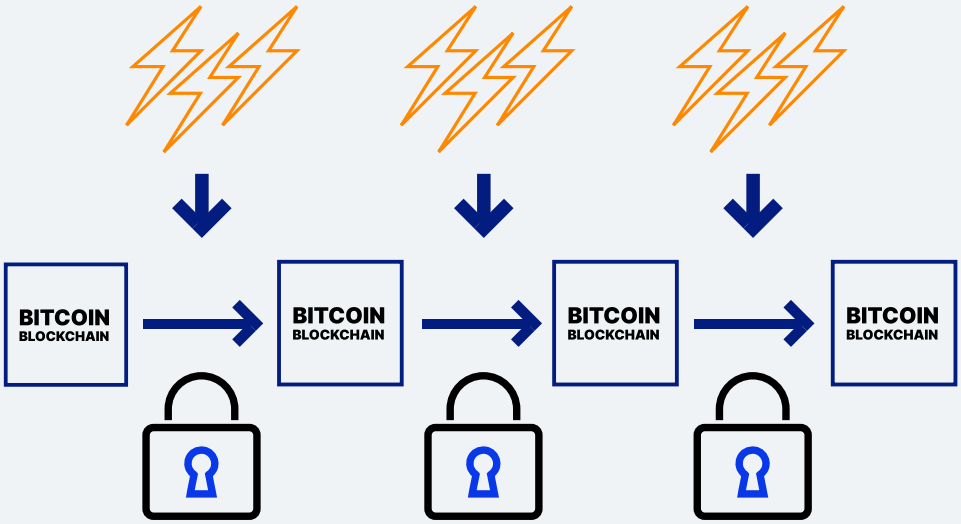
Bitcoin e Energia

Una delle prime obiezioni che vengono spesso sollevate riguardo allo sviluppo di Bitcoin è il consumo energetico della rete. Il mining di bitcoin consuma già una notevole quantità di elettricità in tutto il mondo e questo consumo è destinato ad aumentare in futuro man mano che sempre più persone si dedicheranno al mining di bitcoin.

Quando si parla di Bitcoin e di energia è importante però comprendere che la quantità di energia che fluisce nella rete Bitcoin è fondamentale per



Meno energia sotto forma di potenza di calcolo viene utilizzata per costruire la blockchain Bitcoin, più facile è modificarla in seguito.



Più energia sotto forma di potenza di calcolo viene utilizzata per creare la Blockchain Bitcoin, più è difficile modificarla in seguito.

la sua sicurezza. Più energia fluisce nella rete più questa è sicura. Questo perché per alterare la blockchain di Bitcoin, la stessa quantità di potenza di calcolo - e quindi di energia - che è stata investita per creare la blockchain, deve essere spesa di nuovo. Tuttavia, con milioni di computer in tutto il mondo che forniscono potenza di calcolo alla rete Bitcoin, è quasi impossibile per un individuo, un'organizzazione o uno Stato raccogliere abbastanza potenza di calcolo per apportare anche le più piccole modifiche alla blockchain. Pertanto, la potenza di calcolo e il consumo di energia, sono un'importante caratteristica di sicurezza della rete Bitcoin.

Altro aspetto importante è che i computer per il mining di bitcoin hanno il vantaggio di poter essere situati ovunque nel mondo. Poiché i minatori hanno bisogno dell'elettricità più economica possibile per essere redditizi, spesso si trovano in luoghi dove esistono molte eccedenze e quindi energia a buon mercato. A lungo termine è probabile che si troveranno in luoghi dove è presente molta energia rinnovabile, fatto questo che permetterà di disporre di elettricità a costi più contenuti.

Secondo il Bitcoin Mining Council, attualmente i minatori di bitcoin utilizzano circa il 56% di energia rinnova-

bile e la tendenza è in aumento. Molti esperti ritengono che in futuro fino al 100% del mining di bitcoin sarà alimentato da energia rinnovabile.

Finché non sarà così, tuttavia, il consumo energetico del Bitcoin si riduce alla questione se un denaro e una riserva di valore sicuri e non falsificabili valgano o meno questo dispendio di energia.

El Salvador - Bitcoin come Moneta Nazionale

Già qualche anno fa i visionari ritenevano possibile che un giorno il Bitcoin sarebbe stato riconosciuto come moneta legale dagli Stati nazionali. Nell'estate del 2021 il momento è arrivato: El Salvador è stato il primo Paese al mondo a introdurre il bitcoin come moneta legale. Nei negozi, ristoranti e presso i fornitori di servizi di ogni tipo, il pagamento può essere effettuato, oltre che con dollari USA, anche con bitcoin. A questo scopo ai cittadini è stato fornito un portafoglio bitcoin personalizzato che consente di effettuare pagamenti tramite la rete Lightning in pochi secondi e a un costo minimo.

Altri Paesi come l'Ucraina, il Brasile e Panama stanno discutendo progetti di legge simili. Se altri Paesi dovessero seguire l'esempio di El Salvador, ciò da un lato aumenterebbe ulteriormente la domanda di bitcoin e dall'altro rafforzerebbe la credibilità del bitcoin come „denaro". L'accettazione del bitcoin come moneta legale in un numero sempre maggiore di Paesi, quindi, rappresenta una fase decisiva nel processo di adattamento globale del Bitcoin.

Leggi e Regolamenti

Questi sviluppi hanno portato gli Stati nazionali, le banche centrali e le imprese a doversi occupare estensivamente di criptovalute. Diversi Stati, tra cui la Svizzera, hanno emanato regolamenti e linee guida sulle criptovalute. Questo passo è stato accolto con favore da molti operatori del mercato perché crea certezza giuridica sia per i progetti di criptovalute che per gli investitori coinvolti.

Anche negli Stati Uniti, che finora hanno adottato un approccio permissivo, si prospetta l'introduzione di una regolamentazione. La forma esatta che assumeranno queste nuove leggi negli Stati Uniti viene monitorata da vicino dalla comunità globale delle criptovalute poiché avranno un impatto notevole sull'intero settore.

Altre criptovalute

Il bitcoin non è di certo l'unica criptovaluta al giorno d'oggi. Esistono, infatti, oltre 16.000 criptovalute e asset diversi. Queste monete e token hanno caratteristiche e funzionalità diverse e non sono state tutte concepite come „valute" o denaro. Alcune sono più simili ad azioni in quanto il loro valore riflette il successo di un

progetto sottostante. Altre sono necessarie per usufruire di un particolare servizio. Altre ancora - i cosiddetti meme-token - sono principalmente valute giocattolo.

Per evitare perdite è quindi consigliabile dare un'occhiata più da vicino alla valuta e al rispettivo progetto che ne è alla base prima di effettuare qualsiasi investimento.

Central Bank Digital Currencies (CBDC)

Le criptovalute sono in transizione da una fase selvaggia e non regolamentata a un mondo di criptofinanza regolamentato. Questo sviluppo è sostenuto principalmente dalle banche centrali le quali sono in corsa per emettere le proprie criptovalute. Queste „Central Bank Digital Currencies" o CBDC, secondo i sostenitori combinerebbero la stabilità di una valuta statale con i vantaggi di una valuta basata sulla blockchain. In breve si può dire che creerebbero un nuovo tipo di contante digitale.

Tuttavia, a seconda della sua progettazione, una CBDC può assumere forme fondamentalmente diverse. Diversi Paesi hanno avviato test pilota con diversi tipi di CBDC ed in alcuni di essi le CBDC sono già in uso. Tuttavia si attende con impazienza di sapere se e in che forma le aree valutarie economicamente forti come gli Stati Uniti, l'UE o la Cina lanceranno le loro CBDC.

Competizione tra tipi di denaro

Negli ultimi decenni la nostra società si è abituata così tanto alle valute statali che per molti, fino a poco tempo fa, altri tipi di denaro erano difficilmente immaginabili. Ma in tempi non molto lontani la circolazione parallela di diversi tipi di denaro era parte della vita quotidiana. C'erano banconote emesse dalle banche, monete di metalli diversi e altri valori monetari che potevano essere utilizzati come mezzi di pagamento.

Con il Bitcoin le valute non statali sono ora nuovamente disponibili come alternativa alle valute statali. Finora la maggior parte dei governi ha tollerato il Bitcoin. In una certa misura questo potrebbe essere grazie alla sua natura decentralizzata che lo rende difficile da attaccare. Per i cittadini questo significa che un'alternativa digitale alla moneta di Stato, oltre all'oro e all'argento, è ora disponibile. Gli effetti di questa ulteriore concorrenza monetaria saranno interessanti da osservare in futuro.

BITCOIN, E ADESSO?

Se vi state chiedendo cosa dovreste fare con tutte queste informazioni, permettetemi di darvi un suggerimento. Entrare nel mondo dei Bitcoin non costa nulla, né tempo né denaro. Ma conoscerete una tecnologia che sta per cambiare il nostro mondo e il futuro.

Pertanto, create un conto su un crypto exchange o scaricate un portafoglio sul vostro smartphone e acquistate bitcoin per 50 Euro. Oppure chiedete a un collega di inviarvi dei bitcoin nel vostro portafoglio. Ma toccate con mano, almeno una volta, il Bitcoin.

Perché se il Bitcoin dovesse fare il salto di qualità e diventare onnipresente come è successo con Internet, non solo potrete avere una conoscenza dal punto di vista teorico ma avrete anche usato Bitcoin in prima persona. A volte questo fa la differenza, in quanto vi dà la possibilità di vedere e toccare con mano la tecnologia che vi mette in una posizione di vantaggio rispetto alla maggioranza delle persone.

CIRCA

NOTE SULL'AUTORE

Daniel Jungen è un economista e giornalista finanziario esperto di criptovalute. Daniel è cofondatore di InsightDeFi, una boutique di ricerca specializzata in tutto ciò che riguarda le criptovalute. Insieme ai suoi partner di InsightDeFi, pubblica una newsletter bisettimanale (in tedesco) su Bitcoin, DeFi e criptovalute.

RELAI

Fondata in Svizzera da Julian Liniger e Adem Bilican dopo aver faticato a trovare uno spazio sicuro, senza problemi per l'acquisto di bitcoin, Relai rende accessibile a tutti il risparmio e l'investimento in bitcoin. L'applicazione per soli bitcoin è stata progettata per essere semplice e intuitiva, consentendo a chiunque in Europa di acquistare e vendere bitcoin in pochi minuti, senza bisogno di registrazione, verifica o deposito. Sottoposta a revisione contabile indipendente e con oltre 35 milioni di CHF di bitcoin investiti attraverso la sua piattaforma, Relai sta dando ai consumatori la possibilità di utilizzare nuovi mezzi di risparmio e investimento.

Per saperne di più, visitate il sito Relai.app.

Grazie a @italiansatoshi per aver tradotto questo e-book dall'inglese all'italiano.