TechnoScope
by satw 4/21

Blockchain

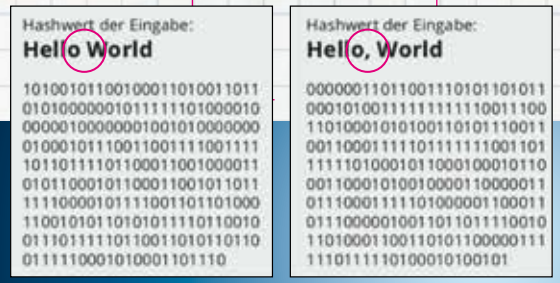
Opportunità e rischi

www.satw.ch/technoscope

Quanto è sicura la blockchain?

La blockchain è considerata inattaccabile perché viene distribuita fra innumerevoli computer. Inoltre la sicurezza è ulteriormente garantita grazie a diverse procedure crittografiche. Il termine crittografia deriva dal greco (kryptos: nascosto; graphein: scrivere) e significa «scrittura segreta» o cifratura. Nella blockchain l'hash ricopre un ruolo di rilievo. È composto da un algoritmo che comprime un file digitale di qualunque lunghezza e tipo, ad esempio un testo, un video o un file audio, convertendolo in una sequenza di caratteri di lunghezza fissa – l'hash (cifra di controllo). Nell'algoritmo SHA-256, il più usato nell'universo blockchain, l'hash è formato sempre da 256 caratteri. Ogni minuscolo cambiamento nell'inserimento genera un risultato completamente diverso. Cosa succede anche aggiungendo una sola virgola, è illustrato nell'esempio in basso.

Infine, tutti i partecipanti alla blockchain necessitano di un software di accesso, composto da due chiavi, una pubblica e una privata. Con la chiave pubblica è possibile visualizzare tutti i dati memorizzati nella blockchain. Ma solo con la chiave privata si possono firmare le transazioni. La chiave privata è una sequenza segreta di cifre. Chi la possiede ha accesso a tutti i valori firmati con la chiave in questione e può trasferirli ad esempio ad altri soggetti. La coppia di chiavi viene conservata in un wallet, un «portamonete digitale»: online, con l'aiuto di un programma di software, oppure offline, su disco rigido o stampato su un pezzo di carta come «paper wallet». I wallet possono rivelarsi punti deboli pericolosi: possono venire hackerati, mentre password e disco rigido possono andare persi. È questo il rovescio della medaglia dei bitcoin: chi non riesce più ad accedere alla sua chiave privata, non può più accedere neanche ai suoi valori memorizzati nella blockchain. Si calcola che da tre a cinque milioni di bitcoin siano bloccati nel cyberspazio.



BLOCKCHAIN

Fiducia digitale

La blockchain non è altro che una banca dati sotto forma di una catena di blocchi di dati che si susseguono uno dopo l'altro. Ciascun blocco contiene informazioni crittografate e ogni nuovo blocco fa riferimento al precedente. Pertanto ogni singolo blocco può essere connesso solo ad altri due blocchi specifici: quello precedente e quello successivo nella catena. In questo modo è impossibile modificare, manipolare o hackerare i blocchi una volta scritti.

La blockchain è nota come registro digitale incorruttibile. Ne esistono innumerevoli copie identiche, interconnesse tra loro. Se si modifica una voce in uno dei registri, la modifica viene automaticamente riportata in tutti gli altri. Ecco perché la tecnologia blockchain è anche definita tecnologia basata su un registro distribuito o Distributed-Ledger-Technologie (DLT).

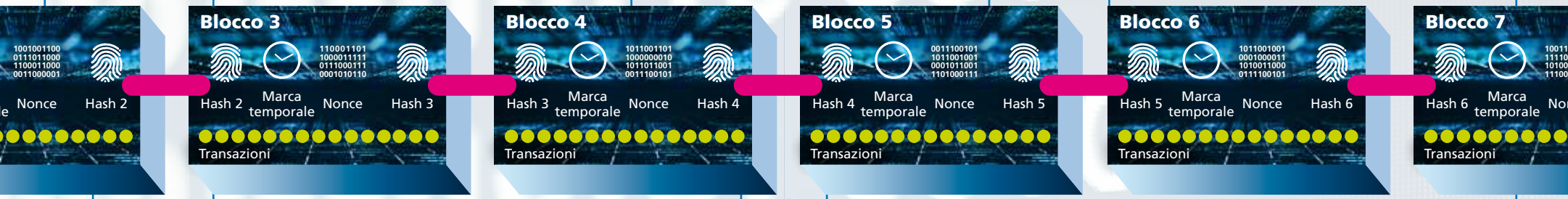
Nella catena non sono necessari organismi di controllo. Con la blockchain i passaggi attraverso intermediari come banche o assicurazioni diventano superflui. Grazie al suo carattere non modificabile, la blockchain crea fiducia e trasparenza. Alcuni la considerano una promessa, altri una minaccia di procedure e meccanismi di controllo consolidati. Non è ancora chiaro quale delle due parti abbia ragione. Ciò spiega il battage attorno alla tecnologia blockchain.

Blocco di genesi: Il primo blocco della blockchain contiene il protocollo di consenso concordato da tutti i partecipanti. Il protocollo determina la frequenza di registrazione nella catena di un nuovo blocco e le sue dimensioni, cioè il numero di transazioni che possono venire memorizzate al suo interno. Inoltre stabilisce chi ha il potere di controllare i nuovi blocchi e i compiti da svolgere a tale scopo.

Blocco 1, 2, 3....: Il contenuto di ogni blocco è composto dal valore di hash (cifra di controllo o impronta digitale, per i dettagli v. AHA!) di tutte le informazioni memorizzate nel blocco. Inoltre comprende anche una marca temporale e un numero casuale (nonce), richiesto per la validazione del blocco. E infine il valore di hash del blocco precedente. Da tutti questi elementi viene calcolato l'hash del nuovo blocco, che rappresenta per così dire la sua carta d'identità digitale, ovvero garantisce che venga generato un'unica volta (e ad esempio che i valori monetari in esso contenuti non possano venire conteggiati più volte). Inoltre dall'hash risulta evidente l'esatta sequenza del blocco all'interno della catena.

Mining: Prima che un nuovo blocco venga aggiunto alla catena, entrano in gioco i miner, i contabili della catena, che hanno il compito di verificare la validità delle nuove transazioni, collegarle e sigillarle mediante un codice cifrato. Il processo di verifica (proof of work) consiste nella risoluzione di un puzzle crittografato. Ciascun miner, in gara con gli altri, tenta di risolvere un complesso enigma matematico che richiede una straordinaria capacità di calcolo. Chi riesce a risolvere l'enigma per primo può collegare il blocco alla catena e ricevere così una ricompensa per il suo operato. Nel caso dei bitcoin, i miner vengono premiati con nuovi bitcoin. Nelle altre blockchain vengono generate altre forme di valori digitali (token). Il procedimento può essere paragonato alla tradizionale corsa all'oro.

Accesso consentito solo alle persone autorizzate: Le blockchain private hanno un numero ristretto di partecipanti. I partecipanti, i soggetti aventi diritto di accesso e i processi di validazione applicabili vengono decisi da un'autorità centrale. Le blockchain private quindi sono meno trasparenti rispetto a quelle pubbliche. In genere perseguono anche finalità diverse: si servono della tecnologia per memorizzare dati sensibili senza rischi di falsificazione. Le blockchain private vengono create soprattutto da imprese e autorità pubbliche.



Blockchain pubbliche: Nelle blockchain pubbliche è sufficiente scaricare il protocollo open source. Non è richiesta la prova dell'identità. Tutti i partecipanti hanno gli stessi diritti, possono vedere tutte le transazioni e prendere parte al processo di verifica. La blockchain pubblica è completamente trasparente per tutti i partecipanti.

Nodi: Ogni computer che partecipa alla blockchain è un nodo. Ogni nodo memorizza e gestisce una copia completa e costantemente aggiornata della blockchain. La memorizzazione ripetuta dei dati rende la rete stabile e affidabile, in grado di sopportare agevolmente l'eventuale perdita di uno o più nodi.

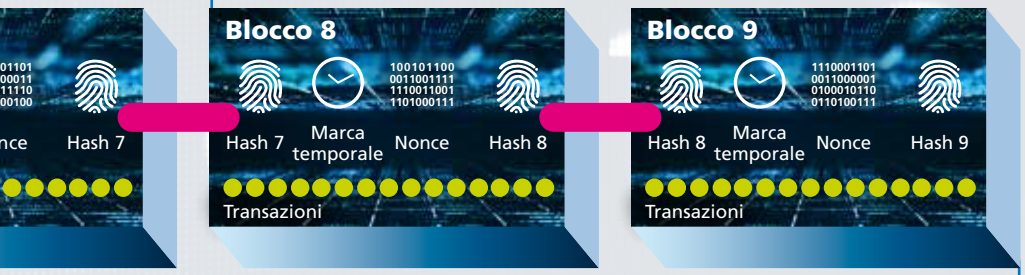
Vantaggi della blockchain:

- Dato che tutte le informazioni vengono memorizzate con codici cifrati, e che la blockchain è distribuita tra tanti computer, il rischio di manipolazione dei dati è praticamente inesistente.
- La blockchain è completamente trasparente. Crea fiducia tra le parti contrattuali che si conoscono poco o non si conoscono affatto.
- Le transazioni vengono elaborate direttamente tra i partecipanti. L'assenza di intermediari le rende più rapide, più convenienti e meno suscettibili di errore.
- Nei Paesi con scarsa certezza del diritto la blockchain contribuisce a garantire i diritti di proprietà.

Pseudonimizzazione: In una blockchain pubblica ogni transazione è assegnata a un indirizzo pubblico che non consente di identificare la persona interessata. Tuttavia, poiché non è da escludere che qualcuno riesca a indovinare l'identità di tali soggetti in base alle transazioni registrate, la blockchain ricorre alla pseudonimizzazione dei dati anziché all'anonimizzazione. Per questo motivo non è particolarmente adatta per le transazioni fraudolente – anche se questa cattiva fama le grava ancora addosso.

Rischi della blockchain:

- La blockchain si basa sulla gigantesca capacità di calcolo di tanti computer collegati in rete, il che si traduce in enormi consumi energetici.
- Il fatto che gli utenti partecipino alle blockchain pubbliche con uno pseudonimo può venire strumentalizzato per scopi criminali.
- Se diventa nota l'identità della persona che si cela dietro uno pseudonimo, è possibile ricostruire tutte le transazioni che questa ha eseguito sulla blockchain, contravvenendo dunque al diritto all'oblio sancito dalla legislazione in materia di protezione dei dati.
- La blockchain promette maggiore trasparenza, ma allo stesso tempo è talmente complessa che rimane ancora un mistero impenetrabile per la maggior parte delle persone.



Chi ha inventato la blockchain? Nel 2008, nel mezzo della crisi bancaria, una persona o un gruppo di persone sconosciute pubblicava un articolo scientifico con lo pseudonimo di Satoshi Nakamoto. Si trattava di un nuovo sistema elettronico chiamato Bitcoin, in grado di trasferire valori monetari senza un'autorità centrale di controllo, in forma anonima e senza rischio di falsificazione. A tutt'oggi nessuno sa chi sia Satoshi Nakamoto e come gli – o le – vadano le cose. Ma per tanti la sua idea rimane rivoluzionaria: un sistema di pagamento libero, aperto, autogestito dalla società digitale. In alternativa al sistema finanziario, spesso incomprensibile e soggetto a crisi.

COS'ALTRO PUO FARE LA BLOCKCHAIN?

I bitcoin e le altre criptovalute – attualmente ne esistono più di 6000 – sono solo una delle tante applicazioni della blockchain. L'incorruttibile registro digitale in linea di principio può venire utilizzato in tutti i casi in cui i rapporti di proprietà devono essere documentati in maniera trasparente, pubblica e senza rischio di falsificazione: attestati, diplomi, iscrizioni nel Registro Immobiliare, testamenti. Un esempio concreto: da circa un anno la maison orologiera svizzera Breitling vende tutti i nuovi modelli con un pass digitale basato su blockchain. Il pass documenta tutte le informazioni essenziali (modello, data di fabbricazione, numero di serie, data di acquisto, garanzia, riparazioni, ecc.) in maniera sicura e non modificabile, e garantisce l'autenticità dell'orologio. Le soluzioni blockchain risultano particolarmente efficienti se abbinate ai contratti smart (smart contract). Si tratta di codici di programmazione if-then-else memorizzati nella blockchain che attivano automaticamente le operazioni concordate non appena vengono soddisfatte determinate condizioni. Ad esempio la serratura smart della casa vacanze rimane chiusa il giorno di arrivo finché l'ospite non ha depositato la cauzione.

Le criptovalute sono come le carte dei Pokemon

Intervista con l'esperto di blockchain Bernd Lapp

Pagare con bitcoin

In Svizzera nella vita di tutti i giorni pagare con le criptovalute è ancora un evento raro, fatta eccezione per singoli caffè e shop online, o assicurazioni. Nella città di Zugo dal 2016 è possibile pagare le tasse con bitcoin, mentre a Zermatt da inizio anno l'amministrazione comunale accetta bitcoin per le transazioni allo sportello – con scarsa eco mediatica. Un ponte tra valuta digitale e valuta reale (il franco) è la carta di credito in bitcoin, che per i pagamenti funziona esattamente come una normale carta prepagata ricaricabile.

Technoscope: Ci spieghi in termini semplici cos'è una blockchain.

Bernd Lapp: La blockchain è come un foglio di carta su cui scriviamo. Una volta riempito, il foglio deve essere archiviato in un libro. Non appena la nuova pagina è stata archiviata, tutti quelli che si ritrovano il libro in mano possono leggerne il contenuto. E in giro per il mondo, tutti quelli che possiedono lo stesso libro trovano esattamente la stessa pagina nella loro copia.

Come sono interconnessi i blocchi all'interno della catena?

Si sommano tutte le informazioni di una pagina. Il risultato viene crittografato mediante un codice cifrato. Il risultato, l'hash, diventa la prima voce della pagina successiva. Se conosco il meccanismo di cifratura, grazie a questo hash sono in grado di ricostruire da solo la pagina precedente e di risalire fino all'inizio dell'intera catena. È questa trasparenza il principale punto di forza della blockchain.

Perché?

Esistono grandi società di revisione che vivono di questo: analizzano i libri contabili di banche e altre società per controllare che tutte le voci siano state contabilizzate al valore corretto. Quando spiego loro cos'è una blockchain, prima o poi arriva il momento in cui cala un profondo silenzio. Perché capiscono che questa

Dove ci portano i bitcoin?

Per possedere bitcoin serve un portamonete (wallet) digitale. Fino a poco tempo fa aprirne uno era una procedura abbastanza complicata. Ora, grazie a diverse app, è diventato un gioco da ragazzi.

Risparmiare in bitcoin

La start-up svizzera relai.ch è convinta che i bitcoin siano particolarmente adatti come salvadanaio. Con la sua app diventa tutto più semplice.

Acquistare bitcoin

Nella hall del Parkhotel Beau Site Zermatt è stato installato il primo bancomat per bitcoin dell'intero comprensorio alpino elvetico. Ma chi preferisce pagare con bitcoin o investire in bitcoin, deve prima acquistarli. Cosa che è possibile fare ad esempio in tutte le biglietterie automatiche delle FFS. Un servizio che secondo le FFS ogni mese viene utilizzato da 1500 utenti. E da qualche tempo Manor e Valora, più altri shop delle aree di servizio, propongono i buoni acquisto in bitcoin, che si possono cambiare online (da franchi a bitcoin).

« Tutti possono dare un'occhiata ai registri, nessuno può più falsare qualche elemento. »

nuova tecnologia rende superfluo il loro modello di business. Ciò che fanno abitualmente, ora grazie alla blockchain possono farlo tutti: tutti possono dare un'occhiata ai registri, nessuno può più falsare qualche elemento. Semplicemente non funziona così. Non appena una pagina viene crittografata, è come se fosse scolpita nella pietra.

Cosa è in grado di fare in più la blockchain rispetto all'e-banking?

Con l'online banking sono registrato presso una banca a cui do l'accesso al mio denaro. Con la blockchain sono l'unico a poter accedere ai miei fondi e nel momento in cui trasferisco a qualcun altro una somma in bitcoin o in altre criptovalute, non vengono coinvolti terzi. Ciò comporta anche commissioni inferiori e una maggiore efficienza dell'intera procedura.

Le criptovalute riusciranno a imporsi?

Le criptovalute sono come le carte dei Pokemon. Alcune valgono di più perché riportano una figura che vogliono tutti, altre sono meno rare e di conseguenza meno ambite. Con le criptovalute funziona in maniera analoga. Il numero dei loro estimatori è in crescita, addirittura tra gli stati: grazie alle criptovalute le transazioni finanziarie sono più semplici e convenienti, richiedono meno tecnologia, meno fasi intermedie e meno intermediari. Ecco perché stiamo assistendo a un crescendo per quanto riguarda la loro accettazione. Di recente El Salvador è stato il primo Paese al mondo a riconoscere i bitcoin come valuta ufficiale.

Lei vive e lavora nella Crypto Valley di Zugo. Perché la Svizzera attira così tante società di blockchain?

La blockchain si concilia alla perfezione con il sistema federalistico decentralizzato e con l'autonomia dei cittadini, abituati a partecipare attivamente al processo decisionale. Questa è esattamente la filosofia alla base della blockchain.

A: **Laura Braga**

Cc:

Oggetto: **Scelta degli studi e del lavoro**

Sono molto interessato alla sicurezza informatica. Attualmente frequento l'apprendistato come informatico al secondo anno. Sono particolarmente attratto da tutto ciò che ruota attorno alla cyber security e mi piacerebbe proseguire i miei studi in questo settore. Quali possibilità di formazione ci sono in Svizzera, soprattutto a livello universitario professionale, che ti permettono di lavorare in questo ambito? (Oscar, 16 anni)

Caro Oscar,
Il tirocinio che stai seguendo, oltre all'attestato federale di capacità, ti consente di ottenere la maturità professionale con indirizzo tecnico che ti permetterà di accedere alle scuole universitarie professionali (SUP) che citi nella tua domanda.

In Ticino, la SUPSI offre un bachelor in ingegneria informatica e un bachelor in scienza dei dati e intelligenza artificiale. Questi due curricoli di studio sono una buona base di partenza per occuparsi in seguito di sicurezza informatica. Nel caso del bachelor in scienza dei dati, per esempio, nell'ultimo semestre di studio viene approfondito il tema della cyber security e della blockchain.

Laura Braga, Servizio documentazione, Ufficio dell'orientamento scolastico e professionale, Bellinzona

Se invece sei disposto a seguire un percorso di studi in tedesco, la SUP di Lucerna offre un bachelor più specifico in Information and Cyber security. Questo nuovo corso di laurea mira a colmare le lacune di una sempre maggior domanda di esperti nel campo della sicurezza informatica. Il bachelor in questione fornisce le competenze necessarie per specializzarsi sugli attacchi informatici e sui test anti-intrusione.

Preferiresti invece una formazione nella Svizzera francese? La SUP di Ginevra propone un bachelor in informatica e sistemi di comunicazione. Qui studenti e studentesse, già dal secondo anno, si specializzano in un settore preciso scegliendo tra 5 orientamenti, uno dei quali è proprio la sicurezza informatica. In seguito, le offerte di formazione continua che danno la possibilità di specializzazione nel campo della sicurezza sono numerose. In Ticino, per esempio, la SUPSI propone il MAS in ICT Systems, Security and Cybercrime.

Il tema della sicurezza informatica come sai non riguarda solo la Svizzera, bensì tutto il mondo. Esistono delle community internazionali che organizzano conferenze, approfondimenti e ingaggiano i cosiddetti hacker etici. Questi «pirati buoni» hanno il compito di cercare di violare un sistema informatico con lo scopo di individuare delle possibili falle.

Link utili

Per informazioni sugli studi in sicurezza informatica: **www.orientamento.ch/informatica**
Per informazioni sulla formazione continua: **www.orientamento.ch/formazioni**
Per informazioni sugli studi in Ticino alla SUPSI-DTI: **www.supsi.ch/dti/bachelor**
Per informazioni sugli studi alla SUP di Lucerna: **www.hslu.ch/informatik**
Per informazioni sugli studi alla SUP di Ginevra: **www.hesge.ch/hepia/bachelor**

Colophon
SATW Technoscope 04/21 | Dicembre 2021 | www.satw.ch/technoscope
Idea e redazione: Ester Elices | **Collaboratori di redazione:** Christine D'Anna-Huber | **Grafica:** Andy Braun | **Foto:** Adobe Stock, Bernd Lapp | **Foto di copertina:** Adobe Stock | **Traduzione:** Ars Linguae | **Stampa:** Egger AG

Abbonamento gratuito e ordini supplementari
SATW | St. Annagasse 18 | CH-8001 Zurigo | technoscope@satw.ch | Tel +41 44 226 50 11

Il prossimo Technoscope uscirà ad aprile 2022 sul tema «Musica»

satw it's all about technology

Hai domande o suggerimenti per il team Technoscope? Scrivici! **technoscope@satw.ch**