CAMERA DI COMMERCIO MONTE ROSA LAGHI ALTO PIEMONTE
punto impresa digitale

NOTIZIE DIGITALI

PID - Punto Impresa Digitale / #12 - 10.2022

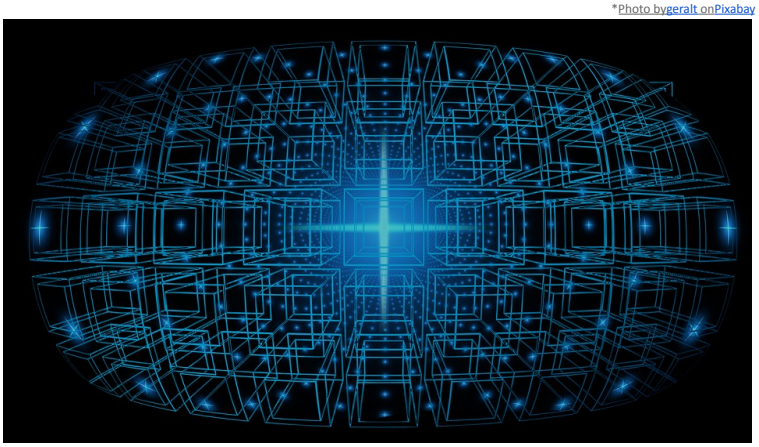
FOCUS 4.0

BLOCKCHAIN:

la tecnologia della sicurezza

Con questi registri, è possibile registrare e condividere dati in maniera sicura e tracciabile

*Photo bygeralt onPixabay



La **Blockchain** ("catena di blocchi") è una tecnologia informatica basata sul "consenso tra i partecipanti": in pratica, le informazioni vengono registrate su un **database condiviso** da una rete di computer, e proprio tale rete funge da "messa in sicurezza dei dati". Infatti, ogni singolo nodo di questo network svolge un ruolo di **verifica** delle informazioni prima di passarle al nodo successivo, in quella che si configura come una vera e propria catena di blocchi (da qui il nome). Tutte le operazioni effettuate sono confermate da blocchi tramite **crittografia**, e un **marcatore temporale** impedisce la loro modifica o annullamento. La verifica, quindi, non avviene grazie ad un ente centrale, bensì dal contributo di tutti i partecipanti alla catena per ogni singola transazione.

TERMINOLOGIA COLLEGATA ALLA BLOCKCHAIN

- **Hash** = funzione algoritmica informatica non invertibile che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita.
- **Bitcoin** = criptovaluta basata sulla tecnologia Blockchain.
- **Timestamp** = marcatore temporale.
- **Smart Contract** = software che automatizza compiti pre-assegnati da una o più parti.
- **Ledger** = libro contabile/registro.
- **Records** = aggiornamenti.
- **Mining** = processo di consenso distribuito.
- **Miners** = coloro che svolgono il Mining.

🔒 **Blockchain Private** (Permissioned): il mining è svolto solamente dall'autorità che attiva la Blockchain, alla quale si può partecipare solo tramite permessi.

🔓 **Blockchain Pubbliche** (Permissionless): il mining è svolto da qualsiasi partecipante alla Blockchain, che si configura come senza permessi, aperta a tutti e senza particolari criteri di certificazione dell'identità dell'utente della rete (ma non per questo non sicura).

🚀 **Blockchain Consortium**: la Blockchain può essere pubblica o privata, ma il mining è svolto da un numero prestabilito di nodi (quindi, ad esempio, affinché un blocco sia valido, deve essere validato dal 50% + 1 dei nodi).

La Blockchain viene normalmente definita "**a Ledger distribuiti**", poiché prevede che tutti i partecipanti a una rete Blockchain conservino una copia identica di un Ledger che a sua volta contiene le transazioni collegate a quella specifica implementazione. Il modello si basa sulla combinazione tra **firma digitale** (la quale garantisce che mittente e destinatario di un messaggio siano identificati in modo certo) e **marca temporale** (il quale permette che un insieme di messaggi, validato con la marca temporale da parte di un nodo scelto casualmente da un robusto modello matematico, venga comunicato e scritto nel registro di tutti gli altri nodi della rete e reso irreversibile). Tutte le operazioni sono confermate dai Miners attraverso il Mining.

PERCHÉ LA BLOCKCHAIN È COSÌ SICURA?

La Blockchain è una base di dati fatta di blocchi, che memorizzano blocchi di transazioni valide correlate da un Timestamp. Ogni blocco include l'hash del blocco precedente, collegandoli insieme: tali collegamenti formano una catena, con ogni blocco addizionale che rinforza quelli precedenti. Quando una transazione (o un blocco) si aggiunge a una Blockchain, viene replicata in tutti i ledger del sistema. Quindi, diventa impossibile modificare una transazione senza che il resto del sistema lo ignori: modificando una transazione, infatti, si modifica un blocco, che varia il suo codice hash (variando un blocco si invalidano tutti quelli seguenti).

In pratica, la correttezza del blocco di operazioni immesse nella rete viene verificata dai computer dei partecipanti al network, confrontandolo con la versione più aggiornata della blockchain.

Un elemento accessorio ma importante della tecnologia blockchain sono gli **Smart Contract**, contratti che si possono attivare da soli quando si verificano determinate condizioni nella catena delle transazioni (ad esempio, generare una transazione automatica se il conto di un determinato utente scende sotto una certa soglia). La vera novità che lega tali contratti alla Blockchain è che questi sono **veri contratti**, hanno cioè un valore legale tra le entità contraenti anche se esistono solo digitalmente.

CARATTERISTICHE

Decentralizzazione
Trasparenza
Affidabilità
Convenienza
Solidità
Irrevocabilità

ESEMPI DI UTILIZZO DELLA BLOCKCHAIN

BANKING/FINANCE Depositi e trasferimenti sicuri di valuta	**INTERNET OF THINGS** Maggiore autonomia dei singoli dispositivi (senza controllo centrale)	**PA** Spoglio sicuro e trasparente nelle elezioni (eVote)	**CYBERSECURITY** Comunicazioni verificate e cifrate
RETAIL Collegamento diretto tra acquirente e venditore	**SUPPLY CHAIN MANAGEMENT** Controllo più sicuro e trasparente delle operazioni	**REAL ESTATE** Identificazione di controparti e dettagli e velocizzazione	**HEALTHCARE** Conservazione e accesso a documenti

di Nicolò Mora e Giulia Bernini

Camera di Commercio Monte Rosa Laghi Alto Piemonte
Servizio PID - Punto Impresa Digitale
www.pno.camcom.it/digitale/pid - pid@pno.camcom.it