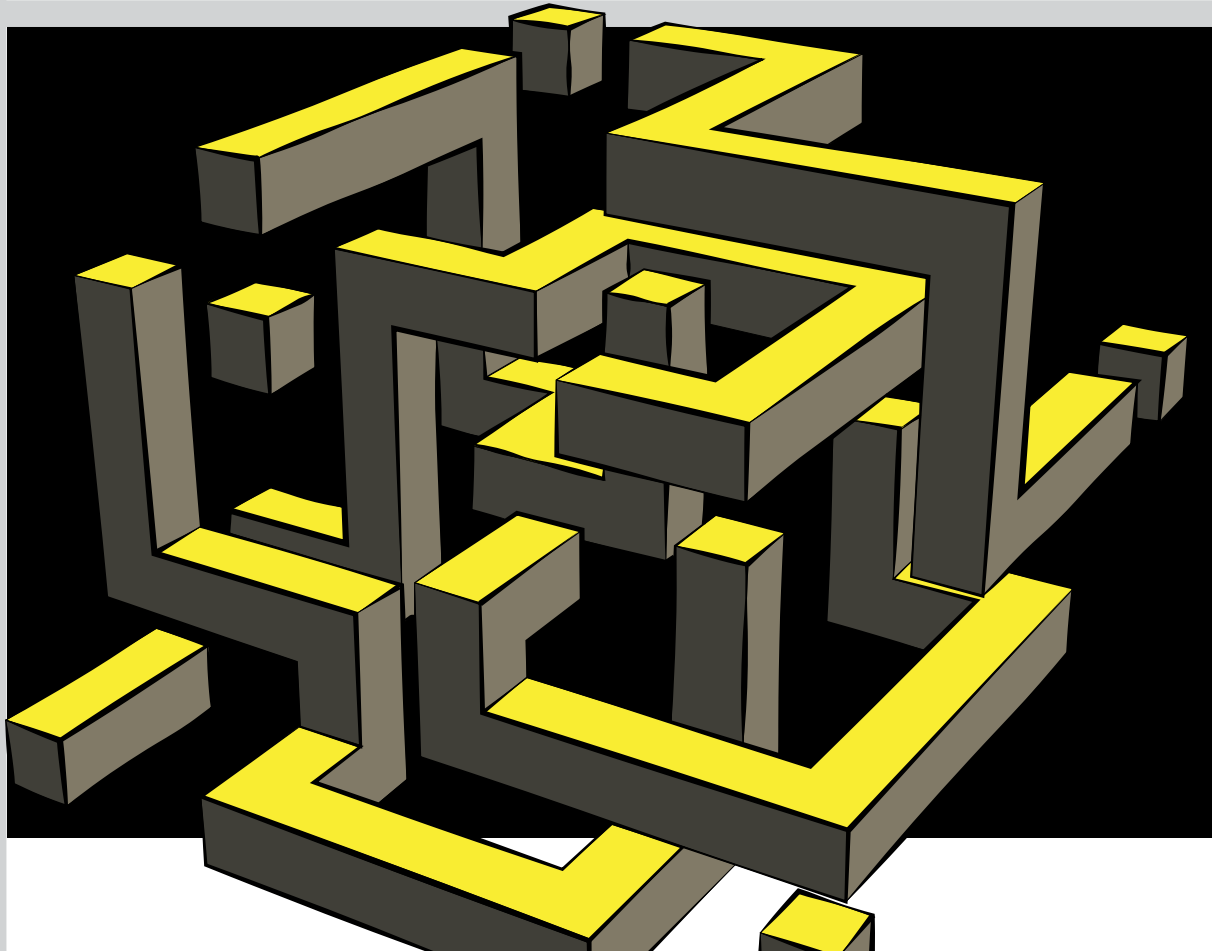
ZeroUno

WHITE PAPER 2018

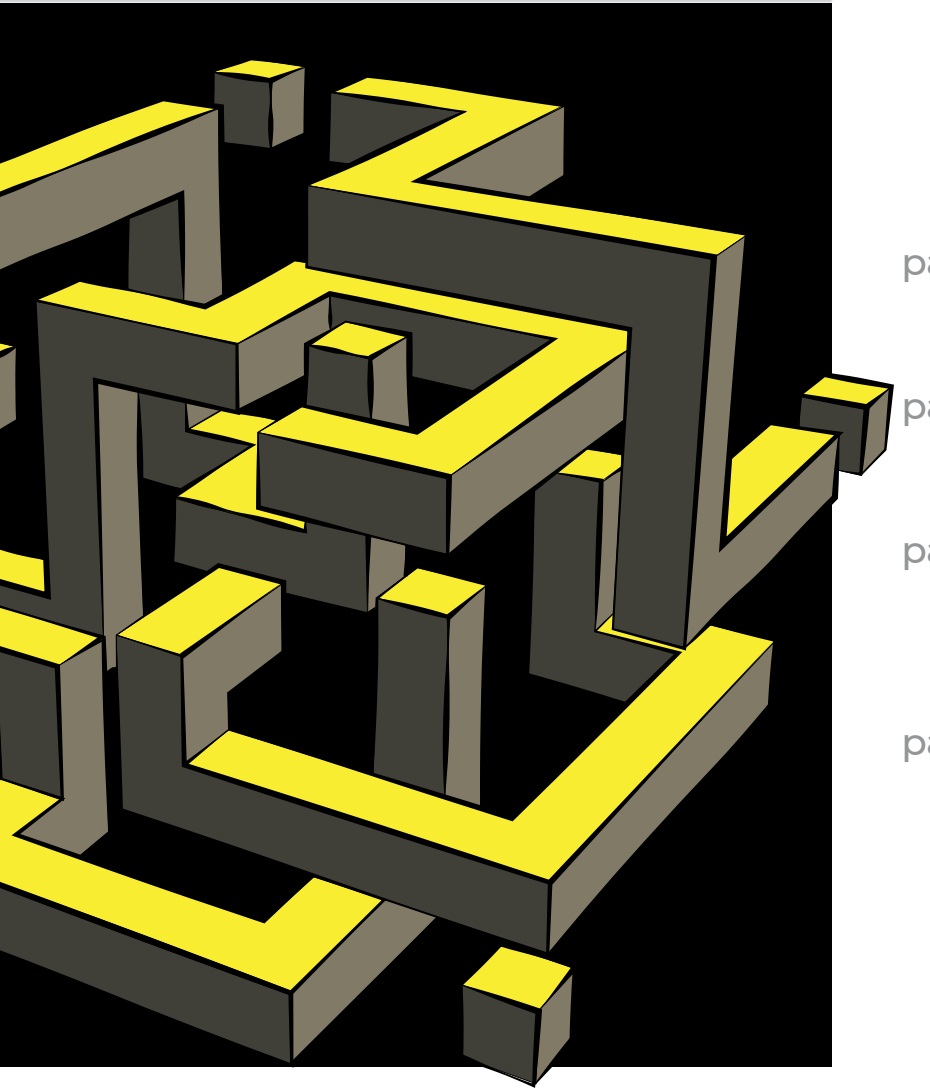
Blockchain

Cos'è, come funziona e vantaggi per il business



I meccanismi che regolano la tecnologia emergente degli ultimi anni. Il funzionamento dei protocolli di validazione e le caratteristiche distintive delle blockchain pubbliche e di quelle private. Smart contract, token e fork: alcune parole chiave che bisogna conoscere.
E ancora, le opportunità per il business ei consigli degli analisti.

SOMMARIO



pag. 3 **TECNOLOGIA**
Trust machine: come funziona il processo di validazione

pag. 8 **TECNOLOGIA**
Le parole da conoscere: smart contract, fork e token

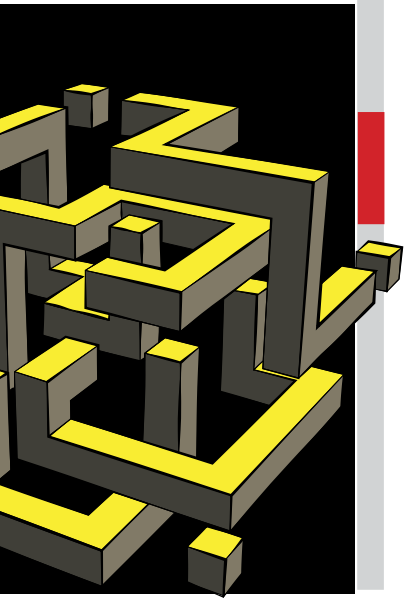
pag. 12 **TREND**
Dalle blockchain pubbliche a quelle private:
le evoluzioni possibili

pag. 16 **TREND**
Le opportunità della blockchain per il business:
i consigli di Gartner

Trust machine: come funziona il processo di validazione

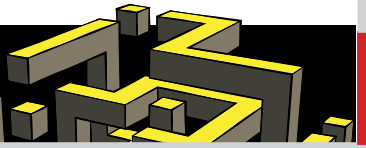
TECNOLOGIA

Un database distribuito composto da blocchi di dati crittografati che memorizzano transazioni: in estrema sintesi questa è la blockchain, il cui valore è dato dal meccanismo di consenso decentralizzato sull'inserimento di ciascun nuovo blocco nella catena. Il processo di validazione è dunque il cuore di una blockchain, vediamo come funziona



La definizione di blockchain è ormai ben nota: si tratta di un data base distribuito (una sorta di registro delle transazioni dove i dati non sono memorizzati su un solo computer, ma su più macchine collegate tra loro via Internet, attraverso un'applicazione dedicata che permette di interfacciarsi con la "catena") fatto di blocchi di dati che memorizzano transazioni; per essere consolidato all'interno di un blocco, ogni dato, e successivamente ogni blocco prima di essere inserito nella "catena", viene sottoposto a un processo di validazione.

Ed è proprio su questo processo di validazione che si basa un concetto fondamentale della blockchain, ossia il meccanismo di consenso decentralizzato che garantisce la sicurezza dell'intera catena: ogni blockchain è, di fatto, un'applicazione open source"decentralizzata" che rappresenta un contratto tra una rete (nel suo insieme) e i suoi utenti. La particolarità di questa applicazione è che il protocollo che la governa e i dati delle transazioni vengono archiviati nel database distribuito (quindi sui computer della "catena") e nessuna organizzazione ne detiene il controllo (proprio come succede per tutte le applicazioni peer to peer): ogni decisione (dalla singola transazione ad adattamenti del protocollo) viene presa con il consenso degli utenti (automatizzato



Trust machine: come funziona...

clicca per guardare il video

attraverso il processo di validazione).

È grazie a questo processo di validazione crittografato che la blockchain diventa una "trust machine" (per utilizzare la definizione di un celebre servizio di The Economist): di fatto, **la crittografia rimpiazza l'intermediazione di una terza parte che faccia da garante in una transazione** (la banca per le transazioni finanziarie, il notaio per la registrazione di un atto ecc.).

I differenti protocolli

Ma se non esiste un supercomputer centrale nel quale questi dati siano archiviati, dove avviene il processo di validazione? È proprio questo l'elemento distintivo di una blockchain: il processo avviene nei computer distribuiti della rete, ma come?

Prima di procedere dobbiamo prendere dimestichezza con due termini: nodi della blockchain e miner. I primi sono i computer della rete che hanno scaricato la blockchain nella loro memoria; chiunque può diventare un nodo, tramite l'apposito programma (Bitcoin Core per esempio per Blockchain Bitcoin). I miner sono coloro che effettuano il controllo delle transazioni, grazie a computer molto potenti e attraverso un protocollo di validazione piuttosto complesso (spiegato più avanti), e il cui lavoro viene ripagato con un premio (il termine ormai condiviso per questa operazione è "minare", italianizzando il termine inglese to mine ossia estrarre).

Il protocollo di validazione (che definisce gli algoritmi validanti e chi può essere un miner) rappresenta dunque l'elemento vitale principale della blockchain perché è proprio da questo che dipendono sostanzialmente la velocità della catena e la sua sicurezza (gli algoritmi che governano questo processo non solo validano che ogni nuova immissione risponda a determinati criteri, ma impediscono anche che possano essere manomessi i dati già presenti nella catena). È dunque in questo ambito che si vedono le principali evoluzioni e che si differenziano, dal punto di vista tecnologico, le diverse blockchain. È comunque importante sottolineare che non necessariamente un protocollo è

migliore di un altro: l'utilizzo dell'uno o dell'altro dipende anche dal tipo di applicazione per la quale viene utilizzata la blockchain.

• **Proof of Work** – È il protocollo di validazione primigenio, sul quale si è basata la prima blockchain, Bitcoin, e a tutt'oggi ancora il più diffuso (figura 1). Ogni 10 minuti un nuovo blocco, contenente migliaia di transazioni, viene immesso nella blockchain seguendo questo protocollo:

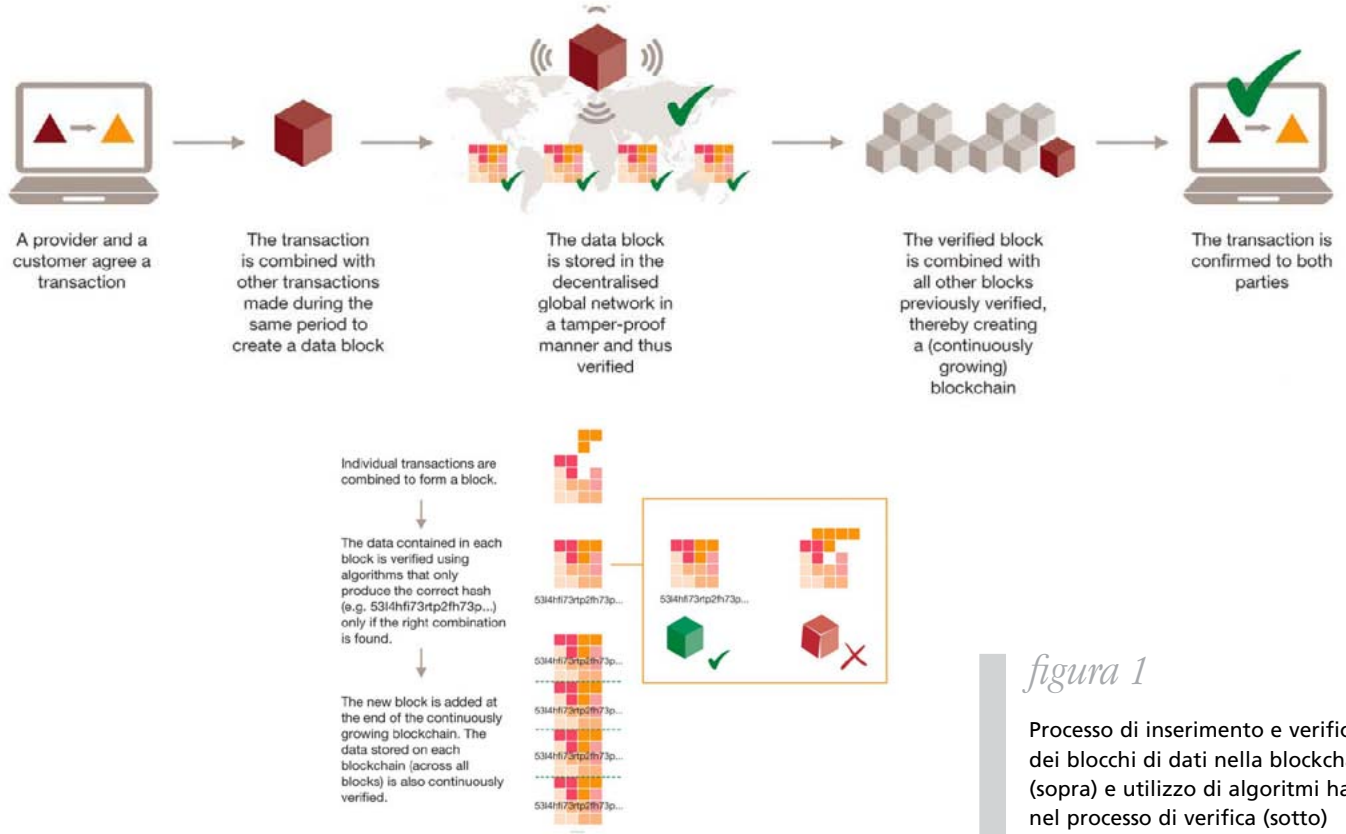
- ogni transazione viene trasformata, utilizzando un algoritmo hash, in una stringa univoca che contiene tutti i dati della transazione precedente (pseudonimo del venditore e dell'acquirente, ammontare, orario ecc.) e quelli della transazione in oggetto;

- tutte le migliaia di transazioni che avvengono nell'arco dei 10 minuti vengono inserite in un blocco che viene sottoposto al processo di verifica dei miner;

- per poter minare il blocco, i miner devono risolvere un calcolo computazionale molto complesso, calibrato per essere risolto in 10 minuti (ogni due settimane viene rivisto il grado di difficoltà del calcolo ed eventualmente ricalibrato);

- il primo che risolve il calcolo (e se la soluzione è validata dal 51% dei miner) "sblocca" (in gergo, "mina") il blocco che viene inserito nella catena e il miner riceve oggi, nel caso della blockchain Bitcoin, per esempio, un premio di 12,5 bitcoin di nuova emissione;

- mentre il processo di "sblocco" dura appunto circa 10 minuti, il processo di verifica da



fonte: Pwc

figura 1

Processo di inserimento e verifica dei blocchi di dati nella blockchain (sopra) e utilizzo di algoritmi hash nel processo di verifica (sotto)

parte degli altri miner che la soluzione del calcolo sia corretta impiega pochi secondi.

La criticità di questo meccanismo risiede nella velocità per minare un blocco perché è un protocollo che, al crescere della blockchain, richiede sempre maggiore potenza elaborativa nei computer dei miner. Il tempo di validazione di una transazione (10 minuti) è uno dei motivi dal quale derivano le maggiori criticità in termini di scalabilità della tecnologia.

Esiste poi il problema che possano di fatto riprodursi meccanismi di concentrazione, con la creazione di enormi data center che centralizzano la funzione di mining (mining farm).

- **Proof of Stake** – Questo protocollo nasce per far fronte al problema della scalabilità del precedente protocollo, semplificando il processo di mining: mentre nel proof of work un vasto numero di miner deve verificare contemporaneamente gli hash da introdurre nella catena, il proof of stake assegna il processo di verifica ai membri della catena in base alle quote di partecipazione alla catena stessa (nel caso di criptovalute, per esempio, se si possiede il 10%, possesso dimostrabile attraverso il protocollo stesso, si può minare il 10% dei blocchi ecc.). Il protocollo prevede inoltre che quando viene aggiunto un nuovo blocco venga automaticamente scelto il creatore del blocco successivo (che non può essere l'account che ha una posizione dominante nella catena come, per esempio, chi possiede la maggior quantità di criptovaluta dato che altrimenti sarebbe colui che può creare tutti i blocchi); per effettuare questa operazione di selezione vengono oggi utilizzati metodi diversi:

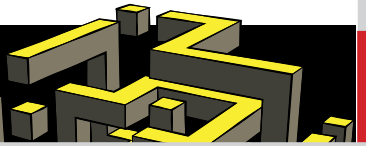
  - *Nxt e BlackCoin*: una funzione casuale randomizzata con una formula che cerca il valore hash più basso rapportato alla dimensione della somma in gioco;

  - *Peercoin*: effettua una selezione casuale abbinandola al concetto di anzianità:numero di giorni di possesso delle monete virtuali;

  - *Redcoin*: utilizza un algoritmo basato sulla

Chi sono i miner?

Il Blockchain miner è un "personaggio" clou della blockchain essendo colui che, attraverso un protocollo di validazione, consente l'inserimento di un nuovo blocco di dati all'interno della catena.
Le virgolette sono d'obbligo perché se all'inizio si trattava effettivamente di persone fisiche che "smanettavano" per fare mining, cioè aggiungere blocchi alla catena Bitcoin e guadagnare così criptovaluta, oggi con questo termine si intendono vere e proprie batterie di computer o addirittura mining farm che svolgono questa attività.
Quando nacque Bitcoin, nel 2009, il Blockchain mining (cioè il processo di validazione di un blocco all'interno della blockchain Bitcoin) era un'operazione relativamente semplice e nel mondo i Blockchain miner erano poche decine che utilizzavano la potenza di calcolo della CPU del proprio computer. Si è poi passati a sfruttare la potenza di calcolo delle GPU (Graphics Processing Unit) e di FPGA (Field Programmable Gate Array, circuiti integrati le cui funzionalità sono programmabili via software) per poi passare a hardware dedicato basato su ASIC (Application Specific Integrated Circuit, circuiti integrati creati appositamente per risolvere un'applicazione di calcolo ben precisa).
La potenza di calcolo oggi necessaria per minare un blocco è talmente elevata da richiedere risorse computazionali irraggiungibili per un singolo operatore; ne consegue la nascita di mining pool o mining farm. Il valore dell'attività di sblocco diminuisce all'aumentare dei blocchi creati e, di conseguenza, il "premio" che spetta al Blockchain miner che per primo mina il singolo blocco si riduce: Bitcoin prevedeva inizialmente 50 bitcoin di nuova emissione per questa attività, ma il sistema è programmato per diminuire nel tempo secondo una progressione geometrica che dimezza il premio ogni 4 anni, divenuto 25 bitcoin a partire dal 2012 e 12,5 oggi. È questo un altro elemento che favorisce la concentrazione elaborativa: più si dispone di sistemi potenti e più ci si "arricchisce".



Trust machine: come funziona...

vai al sito Blockchain4Innovation

Realizzato dal Gruppo Digital360, è il primo sito in Italia dedicato interamente alla blockchain per il business e a come le aziende possono sfruttarla per crescere.

velocità delle transazioni per incoraggiare la movimentazione di criptovaluta piuttosto che il suo possesso.

Da questi esempi (che mostrano come non sia stato ancora identificato un metodo univoco e condiviso per questa delicata operazione) si evince che si tratta di un protocollo ancora non stabile e in continua evoluzione, oggetto di numerose critiche (la più grave di tutte addirittura relativa alla possibilità di "inquinare" la blockchain con autorizzazioni non legittime), ma resta una prima risposta alle problematiche di scalabilità del proof of work dato che la potenza elaborativa richiesta è molto inferiore (su questi temi, alla fine del 2015 Bitfury Group ha rilasciato un White Paper, che ha avuto un'ampia eco tra gli sviluppatori che si occupano dei vari protocolli blockchain, nel quale vengono sottolineate le differenze tra i due protocolli ed evidenziate le criticità del secondo. Il documento Proof of Stake vs Proof of Work, insieme ad altri molto interessanti sul tema, è disponibile su http://bitfury.com) .

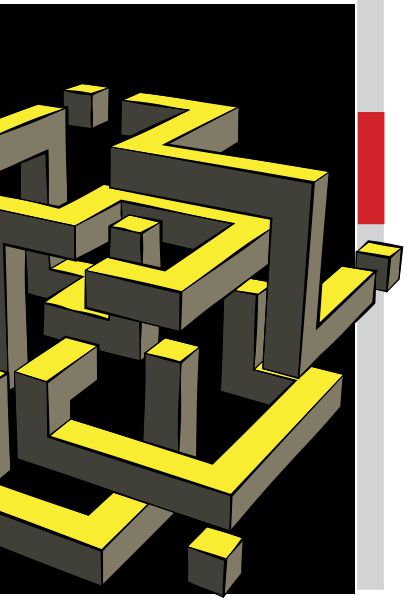
È quindi in corso una grande attività da parte della comunità open source per sviluppare proof of stake affidabili: il progetto più importante è Casper Ethereum, sul quale stanno lavorando diversi sviluppatori, tra i quali anche Vitalik Buterin, uno dei fondatori della blockchain Ethereum; per essere aggiornati sul progetto si può seguire il blog.

- **Federated Byzantine Agreement** (FBA) – Se quelli descritti sono i due protocolli principali, ne sono stati poi creati altri, in parte derivazione di questi, in parte con elementi totalmente nuovi. Tra i più interessanti segnaliamo Federated Byzantine Agreement (FBA), sviluppato da Stellar Development Foundation (e utilizzato dalla seconda metà del 2015 dalla blockchain Stellar) basato su unità di fiducia (quorum slices) decise dai singoli server che insieme stabiliscono il livello di consenso del sistema: rispetto ai modelli di validazione totalmente decentralizzati questo protocollo richiede poche risorse di calcolo e di banda di rete, consentendo applicazioni a più basso costo. (P.F.) ■

Le parole da conoscere: smart contract, fork e token

TECNOLOGIA

Contratti sotto forma i codice che consentono di definire reciproci impegni tra le parti in modo automatico e sicuro (smart contract), strumenti per migliorare le performance delle blockchain e gestirne il protocollo (fork), rappresentazioni digitali di beni o servizi che possono essere scambiati in una blockchain (token). Terminologie con le quali bisogna familiarizzare per capire come le caratteristiche di una blockchain

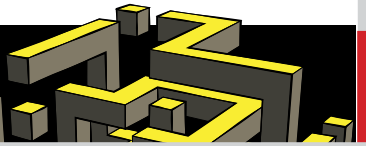


La blockchain è una tecnologia relativamente nuova e per capirne caratteristiche e potenzialità è necessario familiarizzare con acuni termini.

Smart contract, fork e token rientrano tra questi e in questo articolo ne andiamo a illustrare storia, caratteristiche e funzionalità.

Smart contract: quando il software diventa legge

Un contratto sotto forma di codice che rimanda l'esecuzione di alcune o tutte le sue clausole a un software: l'idea è di Nick Szabo, informatico esperto di crittografia e laureato in legge (americano di origine ungherese), che nella metà degli anni '90 si mise a lavorare a componenti hardware e software da installare su oggetti (per un'automobile, per esempio) che ne potessero modificare il funzionamento sulla base di condizioni previste nelle clausole di un contratto che ne regolasse l'uso: ripercorrendo l'esempio dell'automobile e immaginandone un acquisto rateizzato, il componente avrebbe potuto disabilitare la messa in moto in caso di mancato paga-



Le parole da conoscere...

clicca
per guardare
il video

mento di una o due rate. Szabo si è dimostrato un grande visionario perché, in pratica, ha immaginato l'Internet of Things quando Internet era agli albori.

Il concetto di smart contract si compone di tre parti:

- il **codice di un programma** che diventa l'espressione di una logica contrattuale (l'auto funziona se ne vengono pagate le rate);
- **messaggi inviati al programma** stesso che rappresentano gli eventi che devono far attivare il contratto (il mancato pagamento della rata);
- un **meccanismo** che ponga in essere gli effetti previsti dalla logica (all'auto viene inibita la messa in moto).

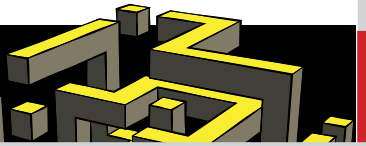
Semplice a dirsi, ma non altrettanto a farsi perché, affinché uno smart contract funzioni, è indispensabile:

1) il consenso tra le parti e, quindi, la presenza di un intermediario che ne garantisca l'affidabilità e impedisca manomissioni;

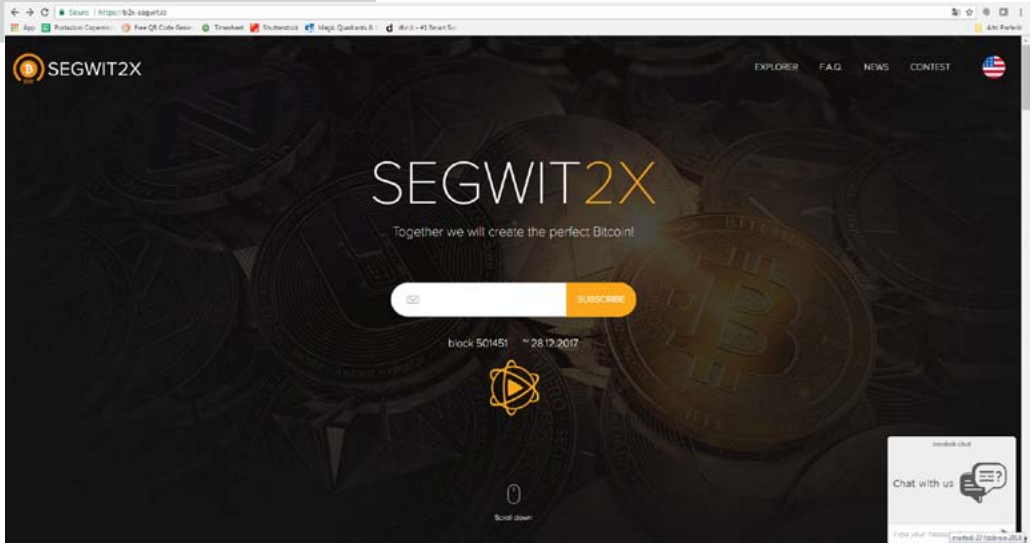
2) oppure di un meccanismo che, in modo automatico e via software, si sostituisca a questo intermediario.

Un esempio del primo caso è quello di eBay che incorpora degli smart contract, sotto forma di procedure automatizzate che eseguono le clausole del contratto che i contraenti sottoscrivono quando si affidano a eBay; questi smart contract vengono eseguiti sui server della società di aste e vendite online.

Per l'applicabilità del secondo caso, negli anni '90 la tecnologia non era ancora ancora pronta, mentre oggi, grazie all'Internet of Things (che consente alle "cose" di comunicare direttamente) e alle tecnologie blockchain con i vari meccanismi di validazione, la geniale idea di Nick Szabo abilita l'utilizzo delle tecnologie blockchain in una varietà di ambiti.



Le parole da conoscere...



vai al sito del progetto SegWit2x, fork di Bitcoin

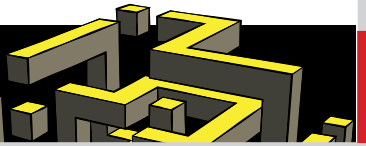
Migliorare le performance della blockchain grazie ai fork?

Fork significa biforcazione e infatti, nell'ambito dell'ingegneria del software, indica lo sviluppo di un nuovo progetto software che parte dal codice sorgente di un altro già esistente; analogamente il termine viene utilizzato nella tecnologia blockchain quando si presenta la necessità di un aggiornamento del protocollo che regola la blockchain (per una normale evoluzione o per risolvere eventuali bug). Questo aggiornamento determina una separazione della blockchain che può essere (da tener presente che, anche se concettualmente può applicarsi a tutti i tipi di blockchain, oggi questa tematica riguarda sostanzialmente le criptovalute):

- una hard fork, ossia una divergenza permanente nella blockchain: i nodi che non si sono aggiornati al nuovo protocollo non possono validare i blocchi creati con il nuovo protocollo; in pratica la nuova versione del software non è compatibile con quella vecchia e in sostanza questo significa che viene creata una nuova blockchain;
- una soft fork è invece una divergenza temporanea dove la nuova versione del software è compatibile con le vecchie, e i vecchi nodi (non aggiornati) saranno in grado di validare i nuovi blocchi.

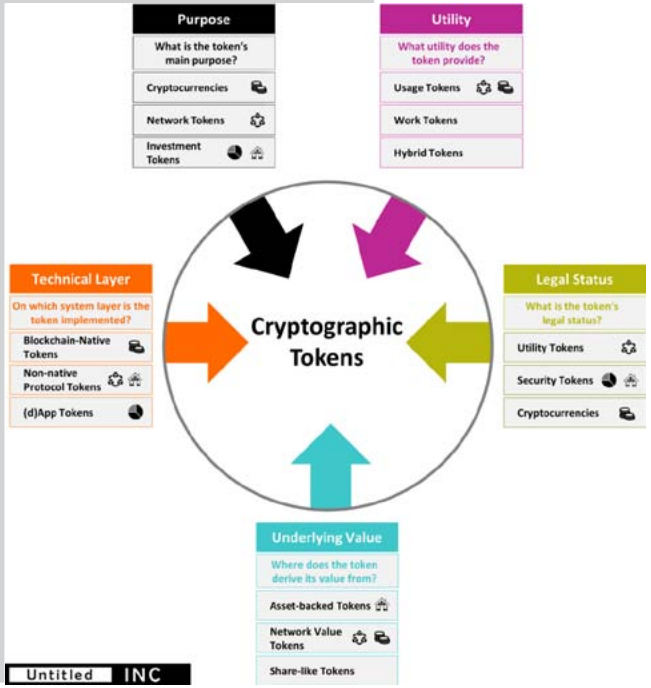
L'esigenza di un fork nasce dalla necessità di migliorare le performance della blockchain dato che uno dei problemi principali di questa tecnologia è la scalabilità: maggiore è il successo di una blockchain e maggiore è il rischio di un rallentamento nella validazione e nel consolidamento dei blocchi.

Il tema è comunque molto delicato ed è stato negli ultimi mesi oggetto di un acceso dibattito relativamente agli hard fork di Bitcoin (in particolare, per SegWit2x che ha lo scopo di migliorare la scalabilità della blockchain Bitcoin, consigliamo la lettura dell'articolo A forza di fork...).



Le parole da conoscere...

vai sul blog della community Untitled INC per vedere il Token Classification Framework



Diritti di proprietà rappresentati dai token

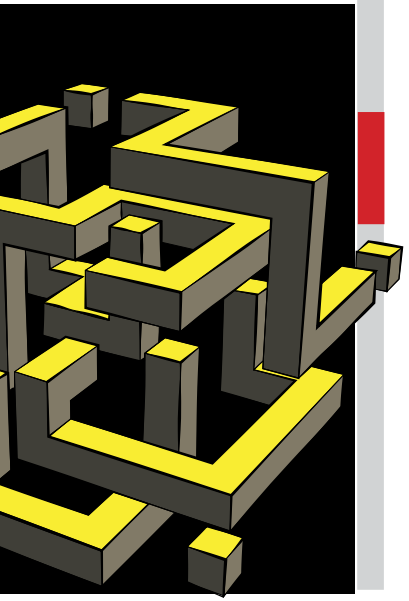
Token significa letteralmente “gettone” e, in ambito blockchain, il termine era strettamente legato al concetto di ICO (Initial Coin Offering), sistema di raccolta fondi non regolamentato per nuove criptovalute, assimilabile all’OPA (Offerta Pubblica di Acquisto) che è invece regolamentata. Nel 2013 fu fatta la prima ICO per il lancio della criptovaluta Mastercoin e l’anno successivo il sistema venne utilizzato per raccogliere fondi per Ethereum. Ma, come la blockchain è una tecnologia che si è andata sempre più allontanando dalle criptovalute, anche il significato di token è nel corso del tempo mutato per andare a definire un **insieme di informazioni digitali che conferiscono un diritto di proprietà a un soggetto all’interno di una blockchain**. Il token può contenere altri diritti e il loro insieme viene governato da smart contract.

Esistono oggi diverse tipologie di token in base al diverso approccio tecnologico o all’utilizzo cui sono destinati. Non esiste attualmente una classificazione standard condivisa, il team di Untitled INC (network nato nel 2001 che riunisce vari esperti di blockchain) ha presentato nel gennaio 2018 un’ipotesi di classificazione (vedi a fianco). (P.F.) ■

Dalle blockchain pubbliche a quelle private: le evoluzioni possibili

TREND

Nata per lo scambio di criptovalute, la blockchain originale è di tipo pubblico (l'ingresso è quindi aperto a tutti), ma con l'estensione di questa tecnologia ad altri ambiti si sono sviluppate blockchain permissioned (che necessitano di permessi, ossia private). Sono queste ultime che avranno un importante impatto sul business scardinando non pochi modelli consolidati



Oggi le applicazioni blockchain possono essere suddivise in tre macrocategorie in base allo stadio di sviluppo delle tecnologie utilizzate.

La categoria **Blockchain 1.0** riguarda tutte le applicazioni di carattere finanziario per la gestione di criptovalute (indipendentemente dal protocollo di validazione utilizzato) a partire dalla storica (e che attualmente detiene ancora la leadership delle criptovalute) Bitcoin che nel corso del 2017 ha vissuto alterne vicende, con picchi di crescita e improvvise discese di valore. Per quanto sia la più famose, si tratta dell'applicazione di questa tecnologia meno interessante dal punto di vista del business.

Verso le blockchain permissioned: vantaggi e criticità

La categoria **Blockchain 2.0** estende la blockchain a settori diversi dal finanziario grazie all'implementazione degli smart contract: protocolli per computer che facilitano, verificano o fanno rispettare la negoziazione o l'esecuzione di un

contratto. In pratica si tratta di contratti che si auto-eseguono e applicano in automatico le proprie clausole. Non una novità, dato che la loro ideazione risale alla seconda metà degli anni '90 del secolo scorso; l'idea innovativa è avere abbinato gli smart contract alla logica della blockchain, idea messa in pratica dal gruppo di sviluppatori guidati da Vitalik Buterin che ha creato la piattaforma Ethereum (basata su blockchain sullo stile di Bitcoin, con una propria criptovaluta denominata Ether, e che, come abbiamo visto, è in prima linea per ridefinire il protocollo di validazione proof of stake) che consente l'esecuzione di piccoli programmi che incorporano una logica di business, ossia degli smart contract.

Nella blockchain Ethereum, gli smart contract sono micro-programmi con associato un database in miniatura:

- la modifica del database è possibile solo da parte del programma che lo controlla (codice e dati sono incapsulati);
- il programma può ricevere dall'esterno messaggi che devono essere firmati digitalmente e che vengono esaminati dal programma che decide se e come agire (figura 1).

Gli smart contract in Ethereum vengono eseguiti in una macchina virtuale presente su ogni nodo della rete: ogni step (transazione) del contratto viene attivato da un messaggio (approvato secondo la procedura appena descritta) e si passa allo step successivo; questo avviene in modo automatico e indipendente in tutti i nodi della rete. Ogni step ha un costo in Ether e la piattaforma ha introdotto dei meccanismi per evitare che vengano lanciati programmi "senza fine" e per correggere altre anomalie che potrebbero verificarsi.

Infine ricordiamo che se la blockchain è nata come modalità pubblica per effettuare transazioni (si tratta delle cosiddette blockchain permissionless alle quali chiunque può accedere), Blockchain 2.0 vede il diffondersi di questa tecnologia (in ambiti diversi dalle criptovalute) sempre più all'interno di ecosistemi più o meno chiusi, con la conseguente nascita di blockchain private (denominate permissioned perché richiedono, appunto, una specifica au-

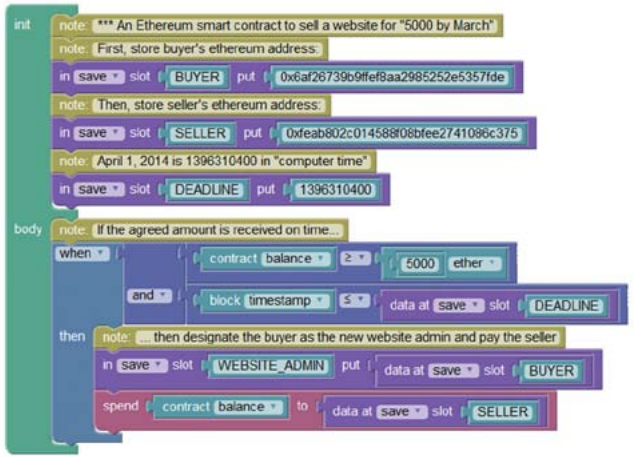
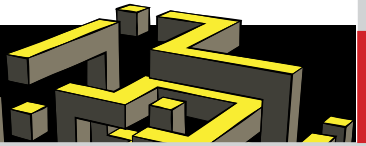


figura 1

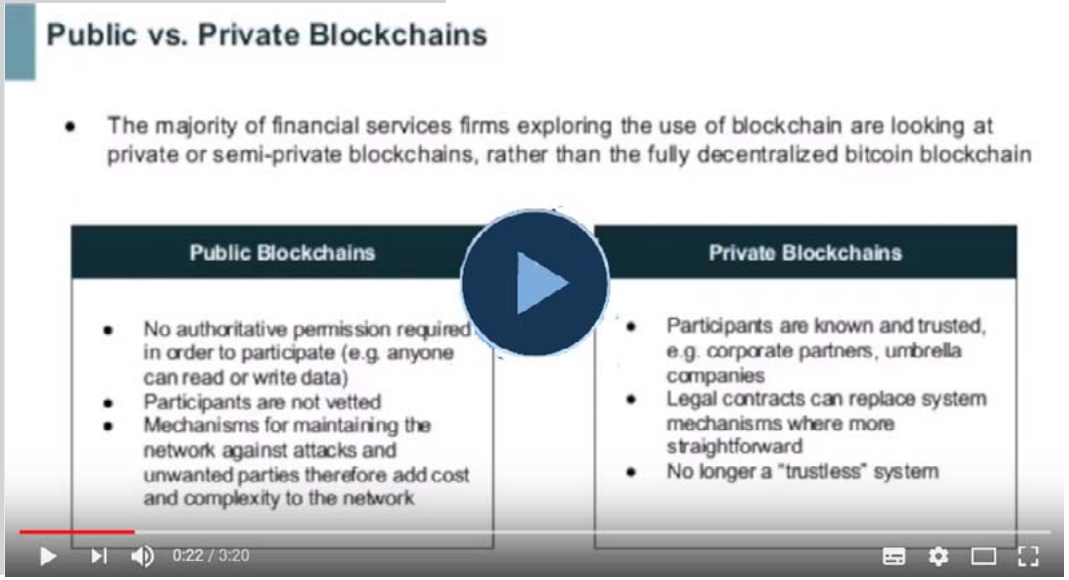
Esempio di smart-contract in Ethereum espresso in istruzioni di alto livello

fonte: Istituto Centrale delle Banche Popolari Italiane



Dalle blockchain pubbliche a...

clicca
per guardare
il video



torizzazione per accedervi).

"Invece di avere un network pubblico e non controllato, è possibile creare un sistema in cui i permessi per accedere sono strettamente controllati e in cui solo alcuni utenti hanno il diritto di leggere o modificare la catena, pur mantenendo alcune delle caratteristiche, in termini di autenticità e decentralizzazione, che la blockchain fornisce", così scriveva già nel 2015 Vitalik Buterin nel sul suo blog . Nell'ambito di quelle permissioned Buterin distingue tra blockchain realizzate da consorzi e blockchain completamente private, ossia gestite da una sola organizzazione. Butrin enuclea molto chiaramente i vantaggi di blockchain permissioned:

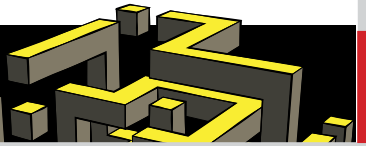
- i validatori sono soggetti noti, per cui il rischio di "attacchi" alla catena per prenderne il controllo viene meno;
- le transazioni diventano più economiche perché sarebbero verificate solo da pochi nodi;
- i nodi possono essere collegati in modo da ottimizzare la scalabilità e garantire la massima sicurezza;
- può essere garantito un maggiore livello di privacy.

Condensa in due principali i vantaggi delle blockchain unpermissioned (senza permessi, pubbliche):

- proteggono gli utenti di un'applicazione dagli sviluppatori, stabilendo che ci sono alcune cose che anche gli sviluppatori di un'applicazione non hanno autorità da fare
- essendo aperte possono essere accessibili a tutti senza alcun vincolo.

Quindi? Quindi tutto dipende dal tipo di applicazione e, come sempre, il tema non è tecnologico bensì di carattere sociale, etico ecc.

Se la blockchain nasce per semplificare e rendere più sicura la supply chain di un'azienda e del suo ecosistema, il suo carattere privato non ha alcuna implicazione etica o morale ed è



Dalle blockchain pubbliche a...

clicca
per guardare
il video

assolutamente logico che le regole che la governano siano stabilite dall'azienda in accordo con il suo ecosistema. Anche se in questo caso, ossia quello di una blockchain totalmente privata, si riduce la portata innovativa di questa tecnologia.

Se, sempre in ambito supply chain, l'intento è quello di migliorarne la gestione per un intero comparto (pensiamo, per esempio, al trasporto delle merci su container e a tutto quello che implica a livello di bolle di trasporto, documenti doganali ecc.), una blockchain permissioned gestita da un consorzio che riunisca tutti gli attori del processo è la soluzione più auspicata e vantaggiosa.

Ma che dire di blockchain che potrebbero gestire tematiche molto delicate dal punto di vista etico? Pensiamo a un database di donatori di organi e malati in attesa di trapianto: quale sarebbe la soluzione migliore? Una blockchain pubblica o gestita da un consorzio? Da chi dovrebbe essere composto questo consorzio? Come definirne un garante?

Le applicazioni decentralizzate

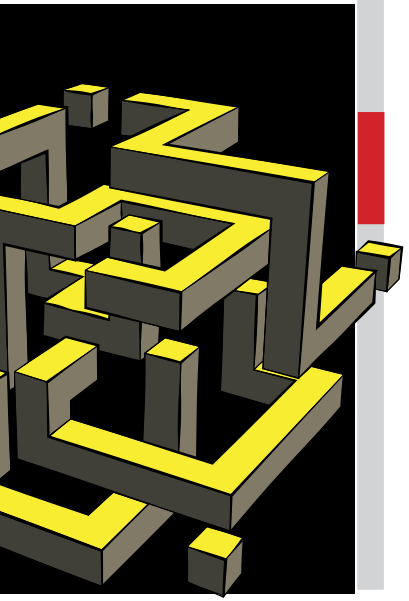
Il passo successivo sarà quello della Blockchain 3.0 con la diffusione delle Dapp (decentralized applications): un futuro in cui tutti noi utilizzeremo le tecnologie blockchain, probabilmente senza neanche rendercene conto, perché incapsulate nelle "cose" connesse tra loro, senza intervento umano, con applicazioni che si autocompileranno.

Ma per il momento questo futuro non sembra alle porte anche proprio per l'immaturità di protocolli e standard. (P.F.) ■

Le opportunità della blockchain per il business: i consigli di Gartner

TREND

L'impatto della blockchain sarà differente nei settori, con diversi livelli di disruption, portando sia opportunità sia rischi. Molti aspetti, soprattutto di carattere tecnologico e giuridico, sono ancora da definire, ma non si può attendere che tutto sia consolidato per occuparsi delle opportunità che la blockchain può offrire.
Nell'articolo i consigli di Gartner



Come devono comportarsi le aziende, per non perdere il treno di queste nuove piattaforme?

Gartner, pur sollecitando i CIO di tutti i settori a informarsi sulle tecnologie blockchain e a comprenderne i meccanismi perché questo modello "semplifica alla radice la governance di transazioni interaziendali e sociali fino a rimuovere la necessità di arbitraggi centrali", sottolinea come molte di queste tecnologie non siano ancora pienamente sviluppate e che, di conseguenza, **gli early adopters si troveranno a dover accettare livelli significativamente più elevati di rischio operativo nei prossimi cinque/sette anni**.

Sul versante dell'offerta, Gartner evidenzia che anche **l'e-**

cosistema dei vendor è ancora immaturo e mette in guardia dalle dichiarazioni di questi, affermando che per tutto il 2018, nell'85% dei casi i progetti che avranno il termine "blockchain" nella propria definizione, in realtà rappresenteranno più una dichiarazione d'intenti che un effettivo disegno strutturale che integra questa tecnologia.

Ma, indipendentemente dal fatto che possano essere vinte le sfide tecnologiche, Gartner sottolinea che persistono alcune considerazioni di carattere legale, per esempio, che richiedono molta attenzione, pertanto consiglia ai CIO e al top management di valutare con attenzione l'implementazione di progetti blockchain su vasta scala.

Diventa quindi quanto mai fondamentale analizzare tutti i fattori della matrice SWOT (Strengths, Weaknesses, Opportunities e Threats) predisposta dalla società di analisi (figura 5) e cercare una risposta a 6 domande strategiche poste dalla stessa Gartner:

1. Quali sono le piattaforme presenti oggi sul mercato, già disponibili per la sperimentazione o, addirittura, per andare in produzione?

2. In che modo il potenziale sviluppo o l'acquisizione di tecnologie blockchain possono influenzare l'attuale piano

LE CARATTERISTICHE DELLA BLOCKCHAIN CHE INTERESSANO AL BUSINESS

Digitale. Valuta, contratti, documenti... nella blockchain tutto diventa digitale e le transazioni inserite nella catena possono riguardare qualsiasi asset, qualsiasi diritto o contenitore di valore e informazione.

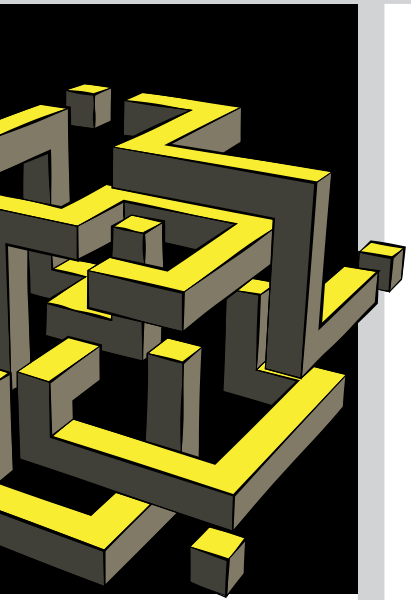
Sicura. Grazie al processo di crittografia che la caratterizza, non è possibile variare o apportare delle modifiche ai blocchi già inseriti nella catena; i dati in essa salvati sono quindi sicuri, certi e non manipolabili.

Attendibile. Essendo organizzata cronologicamente (i blocchi vengono aggiunti alla catena secondo un preciso ordine cronologico immodificabile) impedisce l'insorgere di contestazioni in merito all'esecuzione, per esempio, delle diverse fasi di un contratto.

Affidabile. Le sue caratteristiche tecniche impediscono qualsiasi perdita di dati o danneggiamento: se anche uno dei nodi nei quali è salvata la catena venisse danneggiato, gli altri seguiterebbero a funzionare tenendo stabile la catena, senza alcuna perdita di dati.

Veloce. Non richiede un'entità centrale che ne verifichi la congruità e validità, questa avviene per consenso del network, ed essendo una soluzione completamente digitale elimina tempi di esecuzione, controlli, carta, back-office e rischi operativi.

Le opportunità della blockchain per...



Strengths	Weaknesses
• Distributed resilience and control • Decentralized network • Open source • Security and modern cryptography • Asset provenance • Native asset creation • Dynamic and fluid value exchange	• Lack of ledger interoperability • Customer unfamiliarity and poor user experience • Lack of intraledger and interledger governance • Lack of hardened/tested technology • Limitation of smart contract code programming model • Wallet and key management • Poor tooling and poor developer user experience • Skills scarcity and cost • Immature scalability • Lack of trust in new technology suppliers
Opportunities	**Threats**
• Reduced transaction costs • Business process acceleration and efficiency • Reduced fraud • Reduced systemic risk • Monetary democratization • New business-model enablement • Application rationalization and redundancy	• Legal jurisdictional barriers • Politics and hostile nation-state actors • Technology failures • Institutional adoption barriers • Divergent blockchains • Ledger conflicts/competition • Poor governance

fonte: Gartner

figura 1

Matrice SWOT
per la blockchain elaborata
da Gartner

strategico IT (in termini di utilizzo di open source, API o integrazione)?

3. In che modo i registri distribuiti influenzano le strategie e le operazioni di gestione delle informazioni esistenti?

4. Quali sono le competenze necessarie per valutare lo sviluppo e l'implementazione di blocchi?

5. Quale sarà l'influenza della blockchain nei processi e nelle policy di gestione del rischio?

6. Quali architetture e modalità di implementazione dovrebbero essere considerate in base al contesto aziendale?

Riportiamo infine alcune domande che generano non banali spunti di riflessione espressi da Domenico Gammaldi, Direttore Superiore del Servizio Supervisione sui mercati e sul Sistema dei Pagamenti di Banca d'Italia, nel corso della presentazione dei dati dell'Osservatorio Digital Finance del Politecnico di Milano; Gammaldi sollecita a guardare ai progetti in corso da una prospettiva più ampia: blockchain smetterà di essere una tecnologia per diventare una infrastruttura? Come dovrà quindi essere affrontato il tema della governance dell'infrastruttura? Come fronteggiare il rischio di una frammentazione su più blockchain private e non interoperabili? È sufficiente la sola crittografia a garantire la sicurezza di un'infrastruttura sistemica? (P.F.) ■

direttore responsabile
Stefano Uberti Foppa
stefano.ubertifoppa@zerounoweb.it

articoli di
Patrizia Fabbri
editore
Ict & Strategy srl
società del Gruppo
DIGITAL 360 | Group
Digital360 Srl opera nell'offerta B2B di contenuti editoriali, servizi di comunicazione e marketing, lead generation, eventi e webinar, advisory, advocacy e coaching, nell'ambito della Trasformazione Digitale e dell'Innovazione Imprenditoriale