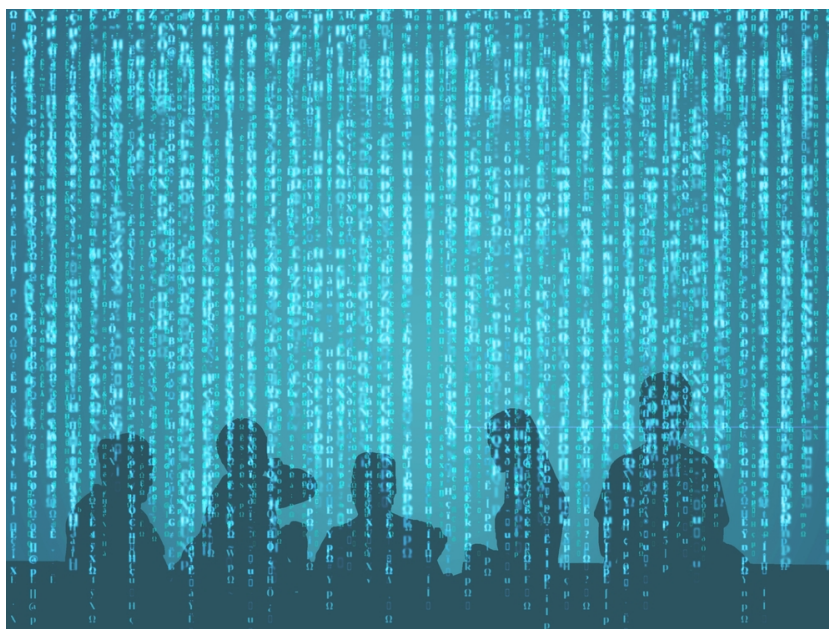

Come la tecnologia blockchain può cambiarci la vita



ANALISI APPROFONDATA

EPRS | Servizio Ricerca del Parlamento europeo

Autore: Philip Boucher

Unità Prospettiva scientifica (STOA)

PE 581.948

IT

Come la tecnologia blockchain può cambiarci la vita

Analisi approfondita

Febbraio 2017

AUTORI

Philip Boucher,	Unità Prospettiva scientifica (STOA), Direzione generale dei Servizi di ricerca parlamentare, Parlamento europeo
Susana Nascimento,	Unità Prospettiva, comprensione comportamentale e concezione delle politiche, Direzione generale del Centro comune di ricerca, Commissione europea (capitoli 6-8)
Mihalis Kritikos,	Unità Prospettiva scientifica (STOA), Direzione generale dei Servizi di ricerca parlamentare, Parlamento europeo (sezioni Politica lungimirante)

VERSIONE LINGUISTICA

Originale: EN
DE, ES, FR, IT, PL, PT

INFORMAZIONI SULL'EDITORE

Per contattare STOA o ricevere la sua newsletter scrivere a: STOA@ep.europa.eu
Il documento è disponibile sul seguente sito Internet: <http://www.ep.europa.eu/stoa/>

Manoscritto ultimato nel febbraio 2017
Bruxelles, © Unione europea, 2017

LIMITAZIONE DELLA RESPONSABILITÀ

Il presente documento è stato preparato per i membri e il personale del Parlamento europeo ed è ad essi destinato come materiale di background a supporto del loro lavoro parlamentare. Il contenuto del presente documento è di responsabilità esclusiva dei suoi autori e i pareri ivi espressi non vanno interpretati come rappresentativi della posizione ufficiale del Parlamento europeo.

Riproduzione e traduzione autorizzate, salvo a fini commerciali, con menzione della fonte, previa informazione del Parlamento europeo e con invio di una copia a quest'ultimo.

Fotografia: ©Montri Nipitvittaya

PE 581.948
ISBN 978-92-846-1042-6
doi: 10.2861/13366
QA-02-17-043-IT-N

Indice

Come la tecnologia blockchain può cambiarci la vita	4
Come funziona la tecnologia blockchain?.....	5
1 Valute: l'avanguardia della tecnologia blockchain.....	6
2 Contenuti digitali: blockchain e gestione dei diritti	8
3 Brevetti: protezione degli innovatori congiunta all'incentivazione dell'innovazione.....	10
4 Voto elettronico (e-voting): una rivoluzione del sistema elettorale?	12
5 Smart contract: se il codice fosse legge.....	14
6 Catene di approvvigionamento: finalmente trasparenza e responsabilità?.....	16
7 Stati e blockchain: ripensare i servizi pubblici	19
8 Blockchain per tutto? Organizzazioni autonome decentralizzate.....	21
Conclusioni.....	24

Come la tecnologia blockchain può cambiarci la vita

Le blockchain (letteralmente "catene di blocchi") rappresentano una modalità particolarmente trasparente e decentralizzata per la registrazione di elenchi di transazioni. Il caso d'uso più noto è quello nel campo delle valute digitali come il Bitcoin, che portò alla ribalta mondiale la tecnologia blockchain con il clamoroso aumento di valore del 1 000 % riportato nel corso di un solo mese nel 2013. La bolla scoppiò ben presto ma, grazie alla costante crescita registrata dal 2015, oggi i Bitcoin hanno un valore senza precedenti.

Molti sono i modi in cui è possibile utilizzare le blockchain per creare nuove valute. Sono state create centinaia di valute di questo tipo con caratteristiche e finalità differenti. Le transazioni valutarie basate sulle blockchain, poiché creano registri pubblici rapidi, economici e sicuri, possono essere utilizzate anche per molte attività non finanziarie, ad esempio per esprimere preferenze elettorali o provare che un documento esisteva in un dato momento. Le blockchain sono particolarmente indicate nelle situazioni in cui è necessario conoscere la cronologia della proprietà. Possono ad esempio aiutare a gestire meglio le catene di approvvigionamento per offrire la certezza che i diamanti siano di origine etica, che gli abiti non siano confezionati in fabbriche che sfruttano i lavoratori e che lo champagne provenga dalla regione da cui prende il nome. Le blockchain potrebbero aiutare a risolvere finalmente il problema della pirateria audiovisiva, consentendo al tempo stesso di acquistare, vendere ed ereditare a titolo legittimo i contenuti digitali e di cederli come accade per i libri, i dischi in vinile e i videonastri. Offrono inoltre opportunità in tutti i tipi di servizi pubblici, quali i pagamenti in ambito sanitario e assistenziale, mentre alle frontiere dello sviluppo della blockchain figurano i contratti ad esecuzione automatica, che stanno spianando la strada alle aziende che si gestiscono da sole senza l'intervento umano.

Le blockchain sottraggono alle élite centrali parte del controllo sulle interazioni quotidiane con la tecnologia, ridistribuendolo tra gli utenti. In questo modo, rendono i sistemi più trasparenti e, forse, più democratici. Ciò detto, è probabile che non assisteremo a una vera rivoluzione. Infatti, i governi e i grandi colossi che stanno realizzando ingenti investimenti nel campo della ricerca e dello sviluppo delle blockchain non stanno cercando di rendersi obsoleti, quanto piuttosto di potenziare i loro servizi. Occorre inoltre tenere conto di altre questioni di portata generale. Ad esempio, la trasparenza della blockchain risulta appropriata in settori di pubblico dominio quali i registri catastali, ma si può dire lo stesso per quanto concerne i saldi bancari e altri dati sensibili? È possibile (anche se solo a volte e con un notevole sforzo) identificare le persone associate alle transazioni, il che potrebbe lederne la riservatezza e l'anonimato. Benché alcune blockchain garantiscano effettivamente un totale anonimato, sarebbe opportuno evitare di utilizzarle per la distribuzione di informazioni sensibili. Tuttavia, malgrado non costituiscano la risposta a tutti i problemi e non rivoluzionino ogni aspetto delle nostre vite, le blockchain potrebbero avere un'incidenza significativa in molti ambiti e, pertanto, è necessario essere preparati alle sfide e alle opportunità che presentano.

La presente analisi offre un agevole punto di accesso a tutti coloro che, in seno al Parlamento europeo e non solo, siano interessati a saperne di più sullo sviluppo della blockchain e sulle sue potenziali ripercussioni. L'obiettivo è stimolare la riflessione e la discussione su questa complessa e controversa tecnologia in rapida evoluzione. L'analisi non è sequenziale e, pertanto, si invitano i lettori a scegliere le sezioni di loro interesse e a leggerle in qualsiasi ordine. La sezione a seguire presenta un'introduzione alla modalità di funzionamento della tecnologia blockchain. Ognuna delle successive otto sezioni presenta una sintesi di due pagine sui settori in cui è possibile applicare tale tecnologia, sulle sue potenziali ripercussioni e sulle sue implicazioni per la politica europea. Infine, la sezione conclusiva riassume alcune osservazioni di carattere generale e le potenziali risposte allo sviluppo della blockchain.

Come funziona la tecnologia blockchain?

Prima di provare a comprendere come funzionano i libri mastri blockchain, vale la pena dare un'occhiata ai libri mastri tradizionali. Per secoli, le banche hanno utilizzato i libri mastri per tenere basi di dati delle transazioni contabili e i governi li hanno utilizzati per tenere registri della proprietà fondiaria. Le modifiche alla registrazione delle transazioni sono gestite da un'autorità centrale, sia essa una banca o un ufficio governativo, in modo da poter identificare chi possiede cosa, in qualsiasi momento. In questo modo, è possibile controllare che le nuove transazioni siano legittime, che gli stessi cinque euro non siano spesi due volte e che le case non siano vendute da chi non le possiede. Poiché gli utenti confidano nel fatto che chi gestisce il libro mastro verifichi in maniera adeguata le transazioni, le persone possono comprare e vendere anche senza essersi mai incontrati prima e in assenza di fiducia reciproca. Anche l'intermediario controlla l'accesso alle informazioni contenute nel libro mastro. Può decidere che chiunque possa accedere all'identità del proprietario di un edificio, ma che solo i titolari di un conto possano controllarne il saldo. Detti libri mastri sono **centralizzati** (esiste un intermediario, di cui tutti gli utenti si fidano, che ha pieno controllo sul sistema e che funge da mediatore in ogni transazione) e **a scatola chiusa** (il funzionamento del libro mastro e i suoi dati non sono pienamente visibili ai suoi utenti). La digitalizzazione ha reso i libri mastri più rapidi e facili da usare, ma continuano a essere centralizzati e a scatola chiusa.

La blockchain offre la stessa funzionalità di mantenimento dei registri, ma senza un'architettura centralizzata. Il problema è verificare la legittimità di una transazione in assenza di un'autorità centrale che effettui i dovuti controlli. Le blockchain risolvono questo problema decentralizzando il libro mastro, in modo che ogni utente sia in possesso di una copia. Chiunque può chiedere che una transazione sia aggiunta alla blockchain, ma tale richiesta sarà accettata solo se tutti gli utenti concordano in merito alla sua legittimità, vale a dire che la richiesta provenga dalla persona autorizzata, che il venditore di un immobile ne sia ancora il proprietario e che l'acquirente disponga ancora della somma necessaria. Questo controllo viene eseguito in modo affidabile e automatico per conto di ciascun utente, creando un sistema di libro mastro molto rapido e sicuro, fortemente in grado di resistere a eventuali manomissioni.

Ogni nuova transazione da registrare è unita ad altre nuove transazioni per formare un "blocco", che viene aggiunto come ultimo anello di una lunga "catena" di transazioni cronologiche. Tale catena forma il libro mastro blockchain detenuto da tutti gli utenti. Questo lavoro è detto "mining". Chiunque può diventare un "miner" e competere per essere il primo a risolvere il complesso problema matematico legato alla creazione di un blocco di transazioni valido e crittografato da aggiungere alla blockchain. Esistono diversi modi per incentivare le persone a dedicarsi a tale compito. Nella maggior parte dei casi, il primo miner che crea un blocco valido e lo aggiunge alla catena viene ricompensato con la somma delle commissioni per le sue transazioni. Le commissioni sono attualmente pari a circa 0,10 euro a transazione, ma i blocchi vengono aggiunti regolarmente e contengono migliaia di transazioni. I miner possono inoltre ricevere nuove valute create e messe in circolazione come meccanismo di inflazione.

Aggiungere un nuovo blocco alla catena significa aggiornare il libro mastro detenuto da tutti gli utenti. Gli utenti accettano un nuovo blocco solo dopo che è stata verificata la validità di tutte le sue transazioni. Se viene rilevata una discrepanza, il blocco viene rifiutato. Altrimenti, il blocco viene aggiunto e rimarrà nella catena come record pubblico permanente; nessun utente può rimuoverlo. Mentre per distruggere o danneggiare un libro mastro tradizionale è necessario attaccare l'intermediario, nel caso di una blockchain è necessario attaccare ogni copia del libro mastro simultaneamente. Non può esistere un "falso libro mastro" poiché tutti gli utenti sono in possesso di una versione autentica che possono impiegare per un confronto. La fiducia e il controllo nelle transazioni basate su blockchain non sono centralizzati e a scatola chiusa, ma **decentralizzati** e **trasparenti**. Queste blockchain sono definite come "senza autorizzazioni" (permissionless) perché non

esiste un'autorità speciale che possa negare l'autorizzazione a partecipare al controllo e all'aggiunta di transazioni. Tali blockchain possono anche essere descritte come l'incarnazione di valori sociali e politici quali la trasparenza e la redistribuzione del potere.

È inoltre possibile configurare blockchain "con autorizzazioni" (permissioned), in cui un limitato gruppo di attori mantiene il potere di accesso, controllo e aggiunta di transazioni nel libro mastro. In questo modo, gli attori "tradizionali" come le banche e i governi possono mantenere un controllo sostanziale sulle loro blockchain. Le blockchain con autorizzazioni sono meno trasparenti e decentralizzate rispetto alle loro controparti senza autorizzazioni e, pertanto, incarnano valori sociali e politici per certi versi differenti.

1. Valute: l'avanguardia della tecnologia blockchain

Pur essendo solo uno dei possibili ambiti di applicazione della tecnologia blockchain, il settore delle valute è di gran lunga quello più conosciuto. Analogamente, benché sia solo una delle numerose valute messe a punto attraverso la tecnologia blockchain, Bitcoin è indiscutibilmente quella più nota. Molte iniziative recenti si sono concentrate sulle possibilità più ad ampio raggio della tecnologia blockchain, ma è raro trovare una discussione convenzionale in materia di blockchain che non includa riferimenti a Bitcoin o, come minimo, alle valute abilitate alla blockchain. Considerando che le applicazioni valutarie dominano i dibattiti sulla blockchain e rappresentano gli ambiti di applicazione più maturi e noti, esse hanno una grande influenza sullo sviluppo delle tecnologie blockchain in generale. Di seguito si analizzano brevemente il funzionamento delle applicazioni blockchain nel caso delle valute nonché alcune loro implicazioni. Tuttavia, poiché sull'argomento è già disponibile un considerevole numero di guide e discussioni di facile reperibilità, ci si concentrerà sul modo in cui il predominio di Bitcoin nel campo delle blockchain può influenzare un più ampio sviluppo della tecnologia e altre applicazioni dei libri mastri distribuiti.

Come funzionano?

Bitcoin è stato lanciato da Satoshi Nakamoto, pseudonimo del misterioso ed elusivo editore (o editori) di un articolo che descriveva in che modo la crittografia, combinata con un libro mastro distribuito, poteva essere utilizzata per implementare una valuta digitale senza un'autorità centrale che autenticasse i pagamenti. Tradizionalmente, lo scambio di denaro tra due sconosciuti è possibile perché entrambi gli attori si fidano di una terza parte, di solito la validità di una banconota o di un intermediario, come una banca o un cambiavalute. Il sistema di Nakamoto non prevede contanti e intermediari ma crea un sistema affidabile grazie all'uso innovativo della crittografia e del networking peer-to-peer. Quando un utente invia Bitcoin a un altro utente, i dettagli della transazione (come gli indirizzi del mittente e del destinatario e l'importo dei fondi trasferiti) vengono trasmessi alla rete Bitcoin in modo che la transazione possa essere convalidata da tutti i "peer" (pari) della rete stessa. Dopo essere stata convalidata dalla rete, la transazione viene inserita in un "blocco" di transazioni e aggiunta, tramite il processo di "mining", al sempre crescente elenco di blocchi che formano il libro mastro blockchain. Questo elenco viene conservato dai pari nella rete. Bitcoin presenta anche una funzione per mezzo della quale vengono generati e aggiunti al sistema nuovi Bitcoin, con un effetto inflazionario. Vengono distribuiti ai miner (oltre alla somma delle commissioni delle transazioni nel blocco) come ricompensa per essere riusciti ad aggiungere le transazioni alla blockchain. Il mining può essere eseguito da qualsiasi utente dotato di un computer ma è emerso un settore di miner professionisti che utilizzano computer dedicati sviluppati appositamente per tale attività. La struttura distribuita del sistema, insieme alla sua funzionalità crittografica, rende Bitcoin incredibilmente solido. La fiducia richiesta per abilitare le transazioni viene raggiunta grazie alla consapevolezza che tutte le transazioni – passate, presenti e future – sono attestate (seppur automaticamente) da tutti gli utenti.

Bitcoin è in assoluto la valuta basata sulle blockchain più diffusa, anche se ne esistono diverse altre con caratteristiche tecniche leggermente differenti. Le differenze spesso concernono il processo di mining, che può richiedere notevoli risorse computazionali. Alcune valute, ad esempio, utilizzano algoritmi che richiedono meno risorse rispetto a Bitcoin. L'algoritmo di Peercoin è progettato per arrivare a utilizzare meno risorse man mano che viene sviluppato. Le valute possono essere differenti anche per quanto riguarda la frequenza e il meccanismo con cui la nuova valuta viene generata e distribuita (e, pertanto, anche per quanto riguarda le loro politiche inflazionistiche). Molte hanno un numero massimo predefinito di "coin" e, quando questo limite viene raggiunto, non vengono generati nuovi coin e i miner trarranno profitto solo dalle commissioni relative alle transazioni. Alcune valute utilizzano algoritmi progettati per evitare che emergano "miner professionisti" che utilizzano apparecchiature specifiche per il mining.

Poiché le transazioni hanno un costo molto basso (attualmente compreso tra 0 e 0,10 euro), ma offrono una registrazione sicura e permanente, è possibile utilizzare la blockchain Bitcoin per altre finalità non finanziarie. Servendosi di tale catena è possibile esplorare e lanciare diverse applicazioni non correlate alle valute, dalla votazione alla protezione brevettuale. Nonostante impedisca agli sviluppatori di attuare le funzioni su misura che avrebbero potuto introdurre in una loro attuazione blockchain, questo tipo di approccio fornisce una struttura a basso costo, facilmente accessibile e stabile, il che la rende un eccellente "ambiente isolato" per esplorare idee. Altre valute basate sulla blockchain sono state configurate pensando esplicitamente a campi d'uso più ampi. Ethereum è una configurazione blockchain che segue il libro bianco di Vitalik Buterin e una campagna di finanziamento collettivo. Include una valuta (ether, che è descritta come "carburante") e un codice che può essere utilizzato per attivare un'ampia gamma di funzioni non finanziarie (cfr. smart contract, gestione dei diritti digitali e organizzazioni autonome decentralizzate).

Potenziali impatti e sviluppi

Nel 2014, un parere espresso dall'Autorità bancaria europea ha evidenziato i diversi rischi posti dalle valute basate su blockchain, rifiutando altresì i loro vantaggi immediati, segnatamente i trasferimenti rapidi, sicuri ed economici, poiché sarebbero irrilevanti nell'UE, dove i trasferimenti convenzionali sono già relativamente rapidi, sicuri ed economici. Per molti utenti, i veri vantaggi delle valute basate su blockchain sono rappresentati, al di là dei risparmi in termini di tempo e costi, dalla funzionalità e dai valori non disponibili nelle valute convenzionali. Possono comprendere alcuni degli ampiamente pubblicizzati "problemi" di Bitcoin, come le sue enormi impennate di prezzo e l'uso nei mercati illeciti sul dark web, due aspetti che in realtà possono aver attirato molti nuovi utenti. Semplicemente, se non vi fossero vantaggi sostanziali derivanti dall'utilizzo di valute basate su blockchain in Europa, non se ne registrerebbe un uso sostanziale in Europa. L'adozione di valute basate su blockchain continua tuttavia a crescere, nonostante la grave violazione di sicurezza che ha messo alla prova le fondamenta ideologiche di Ethereum.

Tali valute sono già all'avanguardia dello sviluppo blockchain, il che potrebbe provocare una forte instabilità tecno-sociale. Se realizzano il loro pieno potenziale, potrebbero aprire la strada a un processo di decentralizzazione che ridurrebbe il potere delle istituzioni che tradizionalmente reggono le finanze, governi e banche compresi. D'altro canto, proprio i governi e le banche stanno attualmente promuovendo attività di ricerca e sviluppo nel campo della blockchain in direzioni che riflettono i loro interessi. Tali blockchain potrebbero rivelarsi meno decentralizzate e trasparenti delle altre.

Tuttavia, le valute basate su blockchain potrebbe forse avere una maggiore incidenza in altri ambiti che esulano dal sistema finanziario. Bitcoin e le altre valute forniscono un'ampia base di utenti, spazi fertili per la sperimentazione e "carburante" per dare slancio a nuove idee. Benché Bitcoin non rivoluzioni il sistema finanziario, potrebbe tuttavia spianare la strada ad altre applicazioni che potrebbero offrire notevoli vantaggi, ad esempio alle catene di approvvigionamento e ai servizi governativi. Anche se le discussioni sulla ricca serie di applicazioni della blockchain sono ora

all'ordine del giorno, le valute come Bitcoin hanno dominato la maggior parte dell'attenzione rivolta alla blockchain dai media e dal mondo politico negli ultimi anni e ciò potrebbe influenzare il modo in cui si svilupperà questa tecnologia. In altre parole, i frequenti riferimenti al valore fluttuante di Bitcoin e al suo utilizzo nei mercati neri potrebbero distrarre le parti interessate e il pubblico da un dibattito più produttivo sull'ampia gamma di opportunità e sfide attualmente presentata da tale tecnologia.

Politica lungimirante

Le valute basate su blockchain presentano molte sfide di natura giuridica e normativa, tra cui i meccanismi di protezione dei consumatori, i metodi di applicazione e le possibilità di intraprendere attività illegali quali l'evasione fiscale e la vendita di merci illecite. Presentano inoltre diversi potenziali vantaggi per i cittadini, tra cui una riduzione dei costi, una maggiore sicurezza e un sistema finanziario più accessibile e innovativo. Questi e altri aspetti sono emersi in una recente proposta di risoluzione approvata dal Parlamento europeo, in cui si evidenziava l'ampio potenziale della tecnologia blockchain "ben oltre il settore finanziario" e si auspicava un approccio normativo proporzionato nonché lo sviluppo di capacità e competenze adeguate a livello dell'UE.

2. Contenuti digitali: blockchain e gestione dei diritti

I falsi e le truffe nel campo della produzione artistica sono pratiche con una lunga tradizione ma, nell'era di Internet, basta fare un copia e incolla e il gioco è fatto. Da quando i sistemi hi-fi domestici hanno reso estremamente semplice copiare dischi in vinile e trasmissioni radio su audiocassetta, i contenuti multimediali sono stati ampiamente copiati e condivisi, spesso illegalmente. Internet ha reso la pirateria ancora più facile. I primi utenti organizzavano reti globali per condividere CD copiati caricandoli in rete. Con l'ampliarsi delle larghezze di banda e la nascita dei formati elettronici, le reti di file-sharing hanno portato la pirateria al grande pubblico. Attualmente, la pirateria multimediale è prevalentemente organizzata tramite servizi di torrent e, in misura crescente, streaming. Nonostante questo tipo di distribuzione di contenuti multimediali sia spesso illegale, tale pratica è così diffusa e l'applicazione delle normative vigenti è così difficile che spesso il rispetto delle norme viene considerato come qualcosa di volontario. Di recente, i servizi di abbonamento legittimi hanno sostituito in parte la pirateria fornendo accesso ai contenuti multimediali tramite il pagamento di royalty ai titolari dei diritti, utilizzando i ricavi pubblicitari o quelli derivanti dai canoni versati dagli abbonati. Tuttavia, nessun modello di distribuzione, fino forse alla nascita della blockchain, è riuscito a rispondere in modo efficace alla realtà del traffico illegale di contenuti digitali nell'era di Internet, riuscendo al tempo stesso a trovare un equilibrio tra gli interessi dell'autore originale, del cliente e dei diversi intermediari.

Con l'acquisto di libri e dischi, i consumatori diventano proprietari di un oggetto fisico che possono poi vendere, regalare o lasciare in eredità. Esistono limitazioni ai loro diritti, ad esempio non devono distribuire copie e devono pagare royalty se trasmettono i contenuti. Acquistando l'equivalente digitale dello stesso prodotto, i consumatori sanno che non entreranno in possesso di un oggetto fisico, sebbene molti non si rendano conto che non entreranno neanche in possesso dei contenuti. Stipulano piuttosto un accordo di licenza valido per un periodo di tempo o per un numero fisso di ascolti/visualizzazioni. Tali licenze non possono essere vendute, regalate o lasciate in eredità. Creare una raccolta di musica, testi, giochi e film in formato digitale acquistati legittimamente spesso costa quanto una raccolta di dischi e libri con gli stessi contenuti. Parliamo di un investimento cospicuo e che dura una vita ma che non può essere trasferito e che scade alla morte del legittimo proprietario. Mentre le generazioni precedenti potevano dilettersi a rivivere i gusti e le esperienze dei loro cari grazie agli scatoloni di dischi in vinile, libri e giochi ora in loro possesso, i bambini di oggi potrebbero non godere dello stesso accesso ai contenuti digitali dei loro genitori. La tecnologia blockchain potrebbe aiutare a risolvere questo e altri problemi relativi ai contenuti digitali?

Come potrebbero essere gestiti i diritti digitali nella blockchain

La tecnologia blockchain può essere utilizzata per gestire i diritti dei consumatori associati ai prodotti digitali. Nella maggior parte dei casi, si tratterà di opere riprodotte in serie, l'equivalente digitale di CD, DVD e libri, vendute in molte copie dagli artisti originali. È tuttavia pertinente anche per il settore emergente delle opere d'arte digitali uniche, ovvero l'equivalente digitale, ad esempio, di un dipinto. In questo caso, l'acquirente non sta acquistando una versione derivata, come un MP3 di una canzone, bensì diritti esclusivi sull'opera originale stessa. La blockchain potrebbe proteggere i consumatori e i creatori di opere digitali di tutti i tipi registrando l'avvicinarsi cronologico della proprietà di un bene digitale e, magari, addirittura applicando diritti digitali.

La blockchain potrebbe essere utilizzata per registrare ogni vendita, prestito, donazione o altri trasferimenti analoghi dei singoli manufatti digitali. Tutte le transazioni sono ratificate e concordate da tutti gli utenti. Analogamente alle transazioni in un conto bancario o un registro catastale, i manufatti possono essere trasferiti solo dai legittimi proprietari. Gli acquirenti possono verificare che stanno acquistando copie legittime di MP3 e file video. Infatti, la cronologia delle transazioni permette a chiunque di verificare che i diversi trasferimenti di proprietà consentono di risalire fino al proprietario originale, ossia il creatore dell'opera. Il concetto potrebbe essere combinato con gli smart contract in modo da poter cedere l'accesso ai contenuti ad altre persone per periodi fissi prima che sia restituito automaticamente al cedente, o per consentire l'esecuzione automatica delle disposizioni testamentarie all'atto di registrazione di un certificato di morte. Una condizione necessaria perché applicazioni del genere funzionino è che, all'atto del trasferimento della proprietà dei contenuti da una persona a un'altra, chi cede la proprietà perda l'accesso, proprio come succederebbe se vendesse un disco in vinile sul mercato dell'usato. In effetti, sapere quando terminano i diritti di un utente è importante proprio come sapere quando iniziano quelli di un altro utente. In questo caso, la blockchain permetterebbe di controllare sia chi era il proprietario dei contenuti sia la cronistoria della proprietà. Ciò consentirebbe ai clienti di essere certi di acquistare beni legittimi piuttosto che copie illegittime e potrebbe anche consentire ai titolari dei diritti di farli valere. Sarebbe anche possibile attuare, grazie all'uso della tecnologia, controlli della legittima proprietà ricorrendo a dispositivi che controllano la proprietà sulla base del profilo dell'utente prima di consentire la riproduzione audio/video. Ciò richiederebbe lo sviluppo di nuovi codec e standard del settore, oltre che di formati di file che integrano i contenuti con le autorizzazioni.

Oltre a comprare copie con licenza di opere digitali, come ad esempio brani in formato MP3, è anche possibile acquistare e vendere opere originali, ossia il brano stesso. Proprio come l'acquisto di un dipinto garantisce più diritti dell'acquisto di una sua copia, l'acquirente delle opere digitali originali acquista anche il diritto esclusivo di trasmissione dei contenuti, della vendita di copie e di azione contro terzi che utilizzano tali contenuti in modo illegittimo. Per gli acquirenti, è fondamentale sapere se stanno acquistando la proprietà dell'opera stessa con il valore e i diritti associati o solo una riproduzione concessa in licenza per uso personale. In questo caso, la blockchain potrebbe essere utilizzata per verificare chi è l'effettivo proprietario dei contenuti, siano essi la versione originale o una copia legittima, e l'insieme di diritti connessi a tali contenuti.

Oltre ai diritti di venditori e acquirenti, la blockchain potrebbe essere utilizzata per proteggere i diritti dei creatori originali delle opere, che potrebbero continuare a detenere alcuni diritti dopo la vendita dei loro contenuti. Tali creatori originali possono includere una complessa rete di attori che rivendicano una proprietà parziale e il diritto al pagamento di royalty nel caso in cui i contenuti vengano utilizzati per finalità commerciali. Per i brani musicali, ad esempio, tale inclusione potrebbe annoverare autori, musicisti e altri artisti, oltre che tecnici del suono, manager e tutta una gamma di intermediari specializzati. I diritti di ciascuno di questi attori, oltre che i termini e le modalità del compenso loro spettante, possono essere codificati digitalmente, consentendo un pagamento più affidabile ed efficiente. I pagamenti di royalty possono anche essere eseguiti automaticamente ricorrendo agli smart contract.

Potenziali impatti e sviluppi

L'utilizzo della tecnologia blockchain in questo modo potrebbe, per la prima volta, consentire ai consumatori di acquistare e vendere copie digitali di seconda mano, regalarle o donarle a negozi gestiti da enti di beneficenza, prestarle ad amici in via temporanea o lasciarle in eredità, proprio come accadeva un tempo con il vinile e i libri, garantendo nel contempo che non siano distribuite molteplici copie senza licenza. Per diventare la base di un metodo di gestione dei diritti digitali, riuscendo laddove molti altri hanno fallito, la blockchain dovrebbe essere in grado di bilanciare i diritti di venditori e acquirenti, di una rete di attori che comprende il proprietario originale dei contenuti, nonché di un'ampia gamma di altri intermediari, compresi coloro che sviluppano e gestiscono la blockchain stessa. Con reti di interessi così complesse in gioco, sarebbe poco realistico sperare che emerga una soluzione rapida e senza controversie, anche se c'è chi suggerisce che, entro un orizzonte temporale di 10-15 anni, la tecnologia blockchain potrebbe essere riuscita ad avere un impatto reale sul settore musicale, con opportunità più immediate per quelli che si saranno mossi per primi.

Politica lungimirante

La legge continuerà ad avere un ruolo importante nell'identificazione delle opere protette da diritti d'autore e nella risoluzione delle controversie. Lo sviluppo della blockchain in questo campo potrebbe favorire politiche di concessione di licenze multiterritoriali e rafforzare la certezza giuridica per i creatori e gli acquirenti, fornendo al tempo stesso efficaci meccanismi di risoluzione delle controversie, soprattutto in materia di tariffe, condizioni di concessione delle licenze, affidamento dei diritti online finalizzato alla loro gestione e ritiro dei diritti online.

3. Brevetti: protezione degli innovatori congiunta all'incentivazione dell'innovazione

I soggetti titolari di brevetto godono del diritto di utilizzo esclusivo delle innovazioni da loro create per uno specifico periodo di tempo. Il sistema dei brevetti è stato progettato per incentivare l'innovazione, mettendo gli innovatori in una posizione di vantaggio rispetto ai concorrenti che consenta loro di trarre profitto dalle loro idee. Dopo tutto, perché un inventore dovrebbe spendere tempo e denaro per sviluppare un'idea se altri soggetti possono copiarla e ricavarne soldi immediatamente, senza neanche contribuire ai costi di sviluppo? Tuttavia, proteggere gli innovatori e incentivare l'innovazione non sono la stessa cosa. Il sistema dei brevetti deve trovare un punto di equilibrio tra la protezione degli innovatori e quella dei concorrenti. Se gli innovatori non sono protetti, il rischio di essere esposti alla concorrenza di chi non ha dovuto sostenere alcun costo li scoraggerà dall'investire in nuove invenzioni. D'altro canto, senza protezione, i concorrenti saranno scoraggiati dall'investire per apportare miglioramenti e ridurre i costi e potrebbero anche non avere la possibilità di accedere al mercato e rompere così il monopolio dell'innovatore iniziale. Essenzialmente, il sistema dei brevetti può essere visto come uno scambio in cui da una parte il governo concede agli innovatori un monopolio (limitato nel tempo e nella portata) di sfruttamento delle loro innovazioni e dall'altra gli innovatori pubblicano i dettagli di funzionamento di dette innovazioni, aiutando chi lo vorrà a sviluppare miglioramenti e alternative.

Il sistema dei brevetti presenta diversi problemi ben noti. Può capitare, ad esempio, che i concorrenti sfruttino prima dell'innovatore un brevetto perché quest'ultimo non è abbastanza forte o perché i titolari non sono stati in grado di difendersi da violazioni illegali. Questo, combinato all'onere per ottenere una protezione brevettuale in diverse regioni, fa sì che alcune aziende preferiscano assumersi il rischio di lanciare sul mercato le loro innovazioni senza proteggerle con un brevetto. Un altro problema è rappresentato dalla complessità del sistema dei brevetti. Le politiche e i sistemi vigenti variano da paese a paese. Nonostante i recenti sviluppi, non esiste ancora un sistema dei brevetti UE unificato. Tuttavia, l'Ufficio europeo dei brevetti offre uno "sportello unico" per la registrazione di

brevetti nel sistema di ciascuno Stato membro, anche se il costo delle traduzioni, delle convalide e dei rinnovi in diversi sistemi rende il rilascio di brevetti in Europa relativamente costoso.

Un ulteriore problema per il sistema dei brevetti è identificato nella comparsa dei "troll dei brevetti", che non innovano in senso stretto bensì acquistano brevetti e chiedono risarcimenti per la loro violazione. Anche se le loro richieste di risarcimento non poggiano sempre su una solida base giuridica, spesso le aziende non possono o non vogliono sostenere le spese legali necessarie per difendersi e preferiscono accordarsi in sede extragiudiziale. Le autorità europee garanti della concorrenza stanno indagando in misura crescente riguardo all'abuso dei brevetti, in particolare nel settore dell'high-tech.

Anche se molti aspetti del sistema dei brevetti sono ora digitalizzati, non sono state apportate modifiche sostanziali alla sua struttura dai tempi della rivoluzione informatica. È stato suggerito che l'uso della blockchain invece dei brevetti tradizionali potrebbe consentire un'innovazione più fluida riducendo le controversie contrattuali e che la blockchain potrebbe offrire un'opportunità per correggere alcuni aspetti del sistema dei brevetti. Proviamo qui a spiegare in che modo la blockchain potrebbe avere un ruolo nel sistema dei brevetti e quali vantaggi potrebbe offrire, prima di prendere in considerazione alcune delle affermazioni più radicali, secondo cui potrebbe sostituire o anche "segnare la fine" del sistema dei brevetti.

Come la blockchain può aiutare il sistema dei brevetti

Due funzioni della tecnologia blockchain la rendono particolarmente importante per il sistema dei brevetti: "hashing" e "proof of existence" (letteralmente "prova dell'esistenza"). Il primo, l'hashing, è un processo mediante il quale un documento viene trasformato in un codice a lunghezza fissa descritto come un'impronta digitale o, con maggiore frequenza, un "hash". Tutti gli hash sono unici e anche lievissime differenze, come un accento o una lettera mancanti in un lungo documento, produrrebbero un hash radicalmente diverso. Solo la ripetizione del processo di hashing su una copia identica del documento originale produrrà lo stesso hash. Cosa d'importanza cruciale, è impossibile rigenerare un documento dal suo hash. La seconda funzione, proof of existence, comporta la registrazione di questi hash nella blockchain. In questo modo viene creato un record dell'esistenza di questo hash in un dato momento. Il record può essere verificato da chiunque, ma nessuno può interpretare i contenuti dell'hash. Tuttavia, i detentori del documento originale possono provare che il documento esisteva al momento in cui è stata eseguita la transazione ripetendo il processo di hashing su una copia identica del loro documento originale (utilizzare lo stesso algoritmo di hashing per produrre lo stesso hash significa disporre dello stesso documento originale). Ciò presenta l'interessante possibilità di registrare pubblicamente il fatto che un documento esistesse senza rivelarne i contenuti. È stato suggerito che gli innovatori potrebbero utilizzare questo processo per proteggere il loro lavoro registrando un hash sulla loro descrizione del brevetto (o magari del testo letterario o un estratto del codice informatico) nella blockchain. In effetti, alcuni servizi "proof of existence" sono già disponibili nel contesto della protezione dei brevetti. In questo caso, si appoggiano alle funzionalità di blockchain esistenti più grandi, specificamente il sistema Bitcoin, anche se potrebbe anche essere progettato e attuato un sistema su misura per registrare gli hash specificamente per finalità di "proof of evidence" (letteralmente "prova testimoniale").

Potenziali impatti e sviluppi

L'applicazione della tecnologia blockchain al sistema dei brevetti potrebbe ridurre le inefficienze nel registrare e stabilire la data/l'ora delle registrazioni in modo efficiente, magari in diversi sistemi dei brevetti nazionali. I servizi "proof of existence" basati sulla blockchain potrebbero essere offerti come prima fase della procedura di deposito di una domanda di brevetto. A partire da questo punto, la procedura potrebbe essere semplificata e protetta, rendendo le varie fasi più trasparenti per il richiedente e riducendo al tempo stesso la possibilità di alterazioni. Tuttavia, anche se apportare

miglioramenti ai modi in cui le innovazioni vengono registrate e corredate di data/ora porterebbe vantaggi tangibili al sistema dei brevetti, i problemi più seri, quali i troll dei brevetti e il costo associato alla traduzione, potrebbero richiedere un altro tipo di risposta.

In alcuni casi si è sostenuto (erroneamente) che un brevetto non è altro che un "concetto timbrato e conservato in un posto dove non è possibile falsificarlo". È stato in effetti suggerito che la blockchain potrebbe sostituire il sistema dei brevetti consentendo al tempo stesso agli innovatori di mantenere segreti i loro dettagli. Tuttavia, la pubblicazione dei brevetti è un aspetto essenziale della loro funzione: la promozione dell'innovazione. La pubblicazione dei brevetti incoraggia i concorrenti a sviluppare alternative e miglioramenti che potrebbero rompere i monopoli dopo la scadenza del brevetto, ispirando al tempo stesso innovazioni in altre aree non coperte dal brevetto. Conservare traccia di chi ha registrato un'idea e quando è solo una piccolissima parte del lavoro svolto dagli intermediari dell'ufficio brevetti. Essi valutano anche l'originalità del brevetto presentato, verificano se è in linea con le normative e le politiche in vigore in quella regione e pubblicano archivi consultabili dei brevetti accettati: tutte queste operazioni sono importanti e non possono essere sostituite dalla tecnologia blockchain.

Politica lungimirante

Gli attuali sistemi dei brevetti potrebbero essere resi più efficienti utilizzando la tecnologia blockchain e gli uffici brevetti potrebbero offrire servizi di "proof of existence" a basso costo. Va tuttavia chiarito che la "proof of existence" mediante una blockchain (o anche con qualsiasi altro mezzo) non può essere interpretata come equivalente alla tutela brevettuale. Per essere accettate come mezzo legittimo di registrazione, le "proof of existence" fornite da terze parti – ad esempio quelle che fanno uso della blockchain Bitcoin esistente – devono essere necessariamente riconosciute come tali dagli organismi preposti all'applicazione della legge.

4. Voto elettronico (e-voting): una rivoluzione del sistema elettorale?

Nonostante la digitalizzazione di numerosi aspetti della vita moderna, le elezioni si svolgono ancora perlopiù offline, su supporti cartacei. Sin dall'inizio del secolo, il voto elettronico è stato considerato uno sviluppo promettente, e, probabilmente, inevitabile che potrebbe accelerare, semplificare e ridurre il costo delle elezioni. Visto come un possibile mezzo per aumentare il coinvolgimento e l'affluenza e anche per ripristinare i legami tra cittadini e istituzioni politiche (affermazioni queste che andrebbero lette con un certo scetticismo), il voto elettronico può esprimersi in molte forme: utilizzando Internet o una rete dedicata e isolata; richiedendo agli elettori di presentarsi a un seggio elettorale o consentendo di esprimere il voto senza supervisione; utilizzando i dispositivi esistenti, quali i telefoni mobili e i laptop, o richiedendo apparecchiature specialistiche. Bisogna ora fare un'ulteriore scelta: continuare ad affidare la gestione delle elezioni alle autorità centrali oppure utilizzare la tecnologia blockchain per distribuire un record di espressione del voto aperto tra i cittadini. Molti esperti concordano sul fatto che il voto elettronico per le elezioni nazionali richiederebbe sviluppi rivoluzionari nei sistemi di sicurezza. Ci sono comunque molti altri tipi di elezioni regionali e organizzative che sarebbe possibile digitalizzare più semplicemente servendosi della blockchain, rendendo più semplice il coinvolgimento di un maggior numero di persone nel prendere decisioni importanti, adottando strategie a lungo termine e selezionando persone per un ampio ventaglio di posizioni.

Come la tecnologia blockchain può essere utilizzata per il voto elettronico

La blockchain è un mezzo per la registrazione e la verifica di record trasparente e distribuito tra gli utenti. Di norma, i voti vengono registrati, gestiti, contati e controllati da un'autorità centrale. Il voto elettronico abilitato alla blockchain (Blockchain-enabled e-voting, BEV) permetterebbe agli elettori di

eseguire tali attività personalmente, consentendo loro di conservare una copia del record di voto. Il record cronologico non può essere modificato perché gli altri elettori vedrebbero che il record è diverso da quello in loro possesso. Non è possibile aggiungere un voto illegittimo poiché gli altri elettori sarebbero in grado di rilevarne la non compatibilità con le regole (magari perché era già stato contato oppure perché non è associato a un record elettore valido). Il BEV sottrarrebbe potere e fiducia agli attori centrali, quali le autorità elettorali, e promuoverebbe lo sviluppo di un consenso della comunità in grado di avvalersi della tecnologia.

Un modo per sviluppare sistemi BEV consiste nel creare un nuovo sistema ad hoc, progettato per riflettere le specifiche caratteristiche dell'elezione e dell'elettorato. Un secondo approccio, che potrebbe essere più economico e più facile, consiste nell'appoggiarsi a una blockchain più consolidata, come ad esempio Bitcoin. Dato che la sicurezza di un libro mastro blockchain si basa sull'ampiezza della sua base utenti, questo approccio potrebbe anche essere più sicuro per elezioni organizzative di minore entità con un ridotto numero di elettori e risorse limitate per sviluppare un sistema su misura.

Il massimo potenziale del BEV si esprime nei contesti organizzativi. In effetti, ne è già stato fatto uso per le elezioni interne dei partiti politici in Danimarca e i voti degli azionisti in Estonia. Sviluppando ulteriormente il concetto, il BEV potrebbe essere combinato con gli smart contract per eseguire automaticamente alcune operazioni quando ricorrono specifiche condizioni concordate. In questo caso, ad esempio, i risultati delle elezioni potrebbero attivare l'esecuzione automatica di promesse del programma elettorale, scelte di investimento o altre decisioni organizzative.

Numerosi analisti hanno preso in considerazione la blockchain in un ruolo di supporto per trasformazioni più profonde, ad esempio nelle discussioni relative ad amministrazioni virtuali, "sistemi tecno-democratici" e la (più remota) possibilità di applicare il BEV alle elezioni nazionali. C'è chi ha ambiziosamente suggerito la possibilità di utilizzare la blockchain per attuare la democrazia "liquida", combinando la democrazia diretta (in cui i cittadini votano regolarmente in merito a specifiche decisioni politiche) con un sistema delegato (in cui i cittadini possono votare personalmente su queste tematiche specifiche oppure assegnare in delega i loro voti a qualsiasi altro cittadino, sia esso un politico, un giornalista, uno scienziato o un amico fidato, e ritirare o riassegnare tale delega in qualsiasi momento).

Potenziali impatti e sviluppi

Prendendo in considerazione elezioni di dimensioni ridotte e processi decisionali organizzativi, il BEV potrebbe contribuire a offrire una struttura sociale più partecipativa e dal basso verso l'alto, offrendo un sistema di voto elettronico relativamente economico e sicuro. Nel contesto di suggerimenti più ambiziosi per le elezioni nazionali, la posta in palio è molto più alta e la situazione è più delicata. Voci critiche hanno messo in dubbio il livello di anonimato e accessibilità offerto dal BEV ed espresso il problema della coercizione. Tuttavia, sebbene il BEV potrebbe offrire diversi vantaggi rispetto ai sistemi cartacei e ad altri sistemi di voto elettronico, molte di queste preoccupazioni sussistono anche per i tradizionali sistemi cartacei. La *coercizione* è una minaccia per qualsiasi sistema elettorale che offre la partecipazione remota (ad es. il voto per corrispondenza). Tanto per il BEV quanto per le elezioni cartacee, l'uso di cabine elettorali private è la sola garanzia contro tale rischio. L'*accessibilità* per tutti gli elettori è un'altra preoccupazione fondamentale in tutte le elezioni. A seconda dell'interfaccia, il BEV potrebbe essere considerato troppo complicato per alcuni elettori, soprattutto se il sistema è interamente decentrato con l'opzione di accedere ai dati e controllare che siano state seguite le procedure corrette. L'*anonimato* è spesso considerato un elemento cruciale della partecipazione democratica, anche se alcune elezioni nazionali non sono completamente anonime. Il Regno Unito, ad esempio, ha un sistema di votazione cartaceo mediante "pseudonimo" in cui un codice collega ogni scheda elettorale a una voce personale nel registro elettorale. In questo caso, gli elettori non potranno far altro che fidarsi del fatto che le autorità elettorali proteggeranno il loro anonimato. Scoprire qual è il voto espresso dai singoli elettori non sarebbe facile, ma rimane pur

sempre una possibilità. Anche il BEV si avvale di pseudonimi e, pertanto, a volte potrebbe essere possibile scoprire come ha votato un elettore. Si sta lavorando a una risposta tecnica a questo problema nello sviluppo di sistemi BEV che offrano un totale anonimato. Un altro approccio potrebbe consistere nell'incaricare un'autorità centrale di distribuire pseudonimi da utilizzare in un BEV mantenendoli segreti, come avviene ora nel sistema elettorale cartaceo del Regno Unito. In questo modo si introdurrebbe un grado di centralizzazione nel sistema che potrebbe anche essere considerato accettabile nel contesto di elezioni nazionali.

Un altro punto chiave è come garantire una fiducia diffusa nella sicurezza e nella legittimità del sistema. Come succede per le elezioni cartacee, non è sufficiente che il risultato sia corretto e valido. L'intero elettorato, anche se scontento del risultato, deve accettare che la procedura sia stata legittima e affidabile. Pertanto, oltre a fornire un'autentica sicurezza e accuratezza, il BEV deve anche ispirare fiducia ed essere ritenuto attendibile. La natura abbastanza complicata del protocollo blockchain potrebbe essere una barriera all'accettazione del BEV da parte del vasto pubblico.

Quando si valuta il potenziale impatto del BEV, bisogna tener conto dei valori e delle politiche che riflette. Il BEV non si limita a digitalizzare la procedura elettorale tradizionale; esso propone un'alternativa che poggia su un diverso sistema di valori e di presupposti politici. Solitamente, le autorità gestiscono le elezioni e la procedura è a scatola chiusa, centralizzata e dall'alto verso il basso. Il BEV è l'esatto contrario. La gestione in questo caso è affidata alle persone ed è trasparente, decentrata e dal basso verso l'alto. Mentre la partecipazione alle elezioni tradizionali rafforza l'autorità dello Stato, la partecipazione al BEV sancisce il primato dei cittadini. In quest'ottica, non sorprende che si instaurino dei collegamenti tra il BEV e una transizione a una democrazia più diretta, decentrata e dal basso verso l'alto e con la democrazia "liquida" cui si è accennato in precedenza. In ogni caso, la misura in cui la tecnologia blockchain avrà fortuna nel campo del voto elettronico potrebbe dipendere dalla misura in cui riuscirà a riflettere i valori e la struttura di società, politica e democrazia.

Politica lungimirante

Pur essendo libere, in linea di massima, di organizzare elezioni interne con la blockchain, se decidono in tal senso, le organizzazioni devono rispettare il diritto dell'UE in materia di riservatezza e protezione dei dati. Sebbene la legislazione europea non specifichi protocolli per le elezioni politiche degli Stati membri, si è verificato un certo grado di convergenza e sono stati fatti sforzi per incoraggiare l'uso del voto elettronico, nel rispetto dei principi costituzionali della legislazione elettorale (suffragio universale equo, libero, segreto e diretto).

5. Smart contract: se il codice fosse legge

I libri mastri blockchain presentano varie funzioni innovative e interessanti rispetto ai libri mastri centralizzati. Tuttavia, oltre a registrare la data/ora e i dettagli delle transazioni, possono anche ricoprire un ruolo più attivo e potenzialmente autonomo nella gestione e nell'esecuzione delle transazioni. Incorporando il codice nella blockchain, le transazioni possono essere eseguite automaticamente quando si verificano determinate condizioni, fornendo così una "garanzia di esecuzione". Gli smart contract a esecuzione automatica, basati su questa funzionalità, sono in rapido sviluppo. Quando il codice e la legge si sovrappongono emergono tuttavia degli interrogativi.

Come funzionano?

Se il termine "smart contract" può indicare più concetti diversi, la definizione del 1994 secondo cui uno smart contract è un "protocollo di transazione computerizzato che esegue i termini di un contratto" è tuttora valida in linea di massima nel contesto delle tecnologie blockchain. Nella loro forma più semplice, i termini di un accordo tra due o più parti sono programmati sotto forma di codice (insieme di istruzioni) che viene memorizzato in una blockchain sostanzialmente nello stesso modo in cui le

transazioni sono ordinariamente memorizzate in altre blockchain. Quando sono soddisfatte le specifiche condizioni descritte nel codice, vengono automaticamente avviate specifiche azioni, anch'esse definite nel codice. Quindi, ad esempio, la consegna di prodotti potrebbe attivare un'istruzione di effettuare un pagamento. Tale istruzione potrebbe, a sua volta, attivare altre istruzioni in altri smart contract, magari di cambiare valuta o di effettuare ordini più a valle nella catena di approvvigionamento. Molte delle proposte di applicazione nel prossimo futuro interessano il settore finanziario, ad esempio i prestiti e i prodotti assicurativi che richiedono ingenti risorse manuali suscettibili di automatizzazione. Gli smart contract potrebbero essere utilizzati per automatizzare le eredità, con la distribuzione dei beni, compresi i contenuti multimediali, attivata automaticamente dopo la registrazione del decesso.

La blockchain Ethereum ha un linguaggio di programmazione e una valuta propri, configurati specificamente per supportare gli smart contract. Altri approcci agli smart contract utilizzano implementazioni blockchain diverse, compreso Bitcoin. Attualmente, la configurazione degli smart contract richiede ancora un certo dispendio iniziale in termini di energie e spese, che li rende pertanto più indicati per accordi ripetitivi piuttosto che per contratti una tantum. Data la loro natura predeterminata, gli smart contract non sono particolarmente indicati per situazioni soggette a cambiamenti sostanziali durante il periodo contrattuale. Visto il livello di incertezza giuridica sarebbe in effetti prudente limitarne l'uso a relazioni e accordi relativamente consensuali che difficilmente daranno adito a controversie tra le parti. Infine, poiché rispondono a stimoli digitali e attivano ulteriori processi digitali, sono più efficienti quando le diverse condizioni e conseguenze delle clausole sono anch'esse di natura digitale e sono pertanto indicate per l'automazione digitale.

Potenziali impatti e sviluppi

Poiché il libro mastro blockchain è immutabile, il codice concordato (e quindi il contratto concordato) può essere annullato o modificato solo nel rispetto dei termini già consentiti nel codice stesso. I contratti tradizionali consentono di scegliere tra il pagamento di quanto dovuto in base al contratto e la rescissione del contratto stesso con le conseguenze che ne derivano, tra cui anche azioni legali. Tuttavia, se il pagamento è automatizzato nel quadro di uno smart contract, tale scelta non è più possibile poiché la transazione viene eseguita automaticamente.

Un'interpretazione radicale degli smart contract ridurrebbe il contratto al codice, riconoscendo di fatto il codice come la legge stessa: autonomo, auto-eseguibile e auto-applicabile. Questa potrebbe essere la posizione di una fazione "estrema" del movimento blockchain di base, che si colloca effettivamente fuori dal controllo di strutture consolidate quali gli Stati nazionali e le giurisdizioni. Laddove il codice viene considerato come legge, tutti gli errori o le vulnerabilità accidentali diventano anch'essi parte del contratto. Sfruttare tali bug per assumere il controllo di beni non sarebbe considerato furto, poiché l'errore che ha consentito la sottrazione fa parte del codice e pertanto, per definizione, non esula dalla "legge". Gli smart contract possono anche contenere clausole illegali, ad esempio codici di distribuzione dell'eredità che non prevedono le imposte di successione in vigore nella giurisdizione di competenza.

Un'interpretazione più realistica degli smart contract consisterebbe nel collocarli all'interno del più ampio ordinamento giuridico. Come succede per i contratti cartacei, è possibile imporre ulteriori requisiti ed è possibile invalidare o reinterpretare clausole sulla base dell'intenzione delle parti e del diritto nel suo complesso. La legge di un paese prevale sempre sulla "legge" iscritta nel codice, anche qualora i procedimenti e l'attuazione a livello giuridico si rivelassero difficili. Di conseguenza, anche se la maggior parte delle discussioni sugli smart contract riconosce che aumenteranno l'efficienza in diverse aree, non è previsto che essi vadano a sostituirsi al diritto contrattuale tradizionale o ai tradizionali avvocati operanti nel campo del diritto contrattuale.

A differenza delle blockchain più semplici che registrano le transazioni, quelle che includono un codice eseguibile presentano un ulteriore livello di complessità e azione. Ciò significa che potrebbero richiedere una maggiore potenza di elaborazione per le attività di mining e di mantenimento del sistema, il che potrebbe tradursi in costi più elevati, anche sotto il profilo energetico. Questa complessità può anche esporre le blockchain a ulteriori vulnerabilità in termini di sicurezza che, se associate all'ideologia del "codice come legge", potrebbero comportare seri problemi pratici per gli smart contract. La frequenza di tali problemi potrebbe ridursi con l'evoluzione delle norme e l'emergere della prima generazione di "avvocati smart" (ossia di avvocati in possesso di formazione ed esperienza nella gestione di smart contract).

Politica lungimirante

Vari ambiti del diritto potrebbero essere vulnerabili agli abusi qualora il contratto non sia considerato parte di una giurisdizione legale tradizionale. Tra gli esempi figurano la fiscalità (in relazione a reddito, vendite, eredità, plusvalenze, ecc.), lo sfruttamento (nel quadro di contratti di affitto, di lavoro, ecc.) e i reati societari (accordi per la fissazione dei prezzi, abuso di informazioni privilegiate, ecc.). Potrebbe essere necessario trovare nuovi modi per affermare il primato della legge nazionale nel caso in cui l'automazione degli smart contract ne renda difficile l'applicazione. Nel contesto dell'applicazione delle procedure giudiziarie tradizionali agli smart contract potrebbero emergere nuove responsabilità dei governi, ad esempio l'arbitrato in caso di bug nel codice-contratto. Iniziando progressivamente a convertire i contratti in codice eseguibile, i programmatori prendono di fatto delle decisioni sulla loro attuazione pratica e potrebbero pertanto doversi assumere maggiori responsabilità legali.

Gli smart contract possono essere privi di flessibilità e incapaci di adattarsi a circostanze mutevoli o alle preferenze delle parti. Non è possibile rispondere in anticipo a tutte le possibili domande e ci saranno sempre circostanze impreviste che richiederanno un'interpretazione della corretta modalità di applicazione delle clausole contrattuali. Il codice è semplicemente troppo rigido per consentire di determinare algoritmicamente tutti i contratti. L'evoluzione del settore potrebbe comportare varie sfide in termini di risoluzione delle controversie e di applicazione delle clausole contrattuali.

Potrebbero rendersi necessarie modifiche del diritto contrattuale tradizionale, in particolare per quanto riguarda le norme sulla tenuta della documentazione e le norme probatorie, per tenere conto della natura automatizzata e deterministica degli smart contract, così come dei punti inerenti alla loro validità e applicabilità. In ambito giuridico, occorrerà affrontare questioni spinose relative alla necessità di stabilire un collegamento con il mondo fisico, eseguire le procedure di convalida necessarie e garantire la conformità delle applicazioni blockchain alla normativa vigente. Adottare la prospettiva di Lessig nei confronti del codice tecnico dovrebbe essere considerata la forma di legge più significativa? Sono chiaramente necessari dei criteri per garantire la validità giuridica e l'esecutività degli smart contract nel rispetto della legge.

6. Catene di approvvigionamento: finalmente trasparenza e responsabilità?

Il commercio globale è basato su un settore della catena di approvvigionamento dal valore stimato di 16 mila miliardi di euro. Le merci sono prodotte e distribuite mediante una vasta rete di produttori, dettaglianti, distributori, trasportatori e fornitori in una complessa configurazione di procedure per la gestione di contratti, pagamenti, etichettatura, sigillatura, logistica e misure per contrastare contraffazioni e frodi.

La scala e la complessità dei sistemi coinvolti comporta elevati costi transazionali, frequenti disallineamenti ed errori nella documentazione cartacea, oltre che a perdite dovute a deterioramento e

furti lungo la filiera. Altri problemi includono: condizioni di lavoro abusive o rischiose; danni ambientali dovuti a inefficienze e procedure estrattive e produttive illegali; contraffazione e imitazione; rischi per la salute dovuti a una cattiva gestione della catena di approvvigionamento. Simili questioni emergono spesso in occasione di incidenti di alto profilo, che colpiscono ad esempio le catene di approvvigionamento di generi alimentari, abbigliamento e diamanti. Alcuni sostengono che gli standard e la certificazione hanno migliorato la differenziazione nella scelta e la consapevolezza dei consumatori ma le vere e proprie procedure continuano a essere costose e poco affidabili, soprattutto nelle regioni con elevati livelli di corruzione. Le "catene di custodia" complete, che provano l'origine di ciascun prodotto o materiale, sono ancora frammentate tra diverse organizzazioni ed esposte a frodi ed errori, anche tra le aziende certificate. C'è una richiesta sempre più diffusa di catene di approvvigionamento di merci e servizi che siano più sicure, affidabili e trasparenti. Rimane da chiarire se la tecnologia blockchain possa davvero migliorare le catene di approvvigionamento e il settore logistico attuali per rispondere alle inefficienze operative, alle frodi e magari anche ad alcune delle "grandi sfide" come le pratiche di lavoro non etiche e il degrado ambientale.

Come potrebbero essere gestite le catene di approvvigionamento nella blockchain

Le applicazioni basate sulla blockchain hanno il potenziale per migliorare le catene di approvvigionamento fornendo l'infrastruttura per registrare, certificare e tracciare a basso costo le merci trasferite tra parti spesso distanti, connesse tramite una catena di approvvigionamento ma che non necessariamente si fidano l'una dell'altra. Tutte le merci sono identificate in modo univoco tramite dei "token" e possono quindi essere trasferite per mezzo della blockchain, dove ogni transazione viene verificata e corredata di data e ora secondo una procedura crittografata ma trasparente. Ciò fornisce l'accesso alle parti interessate, siano esse fornitori, venditori, trasportatori o acquirenti. I termini di ogni transazione restano irrevocabili e immutabili, aperti a fini d'ispezione a chiunque o ai controllori autorizzati. Gli smart contract possono anche essere impiegati per eseguire automaticamente pagamenti e altre procedure.

Potenziati impatti e sviluppi

Diverse aziende così come alcuni innovatori e operatori storici stanno già testando la blockchain per la tenuta della documentazione nelle loro catene di approvvigionamento. Everledger consente alle aziende e agli acquirenti di tracciare la provenienza dei diamanti dalle miniere alle gioiellerie e di contrastare le frodi assicurative e documentarie. Per ogni diamante, Everledger misura 40 attributi quali il taglio e la purezza, i gradi degli angoli del padiglione e il luogo d'origine. Genera un numero di serie per ciascun diamante, inciso microscopicamente, e aggiunge quindi l'ID digitale alla sua blockchain (che attualmente conta 280 000 diamanti). In tal modo diventa possibile creare e mantenere cronologie complete della proprietà, che possono essere utili a contrastare le frodi e aiutare la polizia e gli investigatori assicurativi a rintracciare le gemme rubate. Consente anche ai consumatori di prendere decisioni d'acquisto più consapevoli, ad esempio limitando la ricerca ai diamanti con una storia "pulita", esente da frodi, furti, lavoro forzato e operazioni di venditori sospetti legati al mondo della violenza, della droga o del traffico d'armi.

L'impresa sociale con sede a Londra Provenance ha sviluppato una piattaforma di dati in tempo reale che raccoglie e verifica l'origine di un bene assegnandogli un token o "passaporto digitale" che può essere rintracciato lungo tutta la catena di approvvigionamento finché non arriva a destinazione. Ciò potrebbe essere utile per contrastare le frodi nella vendita di merci con denominazione di origine protetta, che viene spesso concessa alle specialità regionali come i vini e i formaggi. SmartLog integra gli smart contract nei container per rintracciarne la posizione e l'ambiente circostante ai fini della pianificazione delle risorse. La blockchain è utilizzata anche per ridurre al minimo i rischi nei pagamenti, con aziende quali Skuchain e Fluent che offrono un supporto basato sulla blockchain per il finanziamento e i pagamenti delle catene di approvvigionamento. Un altro progetto sta sviluppando

un sistema per ottimizzare l'elaborazione manuale della documentazione utilizzando una blockchain privata per condividere informazioni tra gli esportatori, gli importatori e le loro banche. Wal-Mart, la più grande catena di negozi al dettaglio del mondo, sta sperimentando la blockchain nel settore della sicurezza alimentare. Si prevede che record accurati e aggiornati basati sulla blockchain potranno aiutare a identificare il prodotto, la spedizione e il venditore, ad esempio in caso di epidemia, ottenendo così dati relativi alle modalità e all'area di produzione di un prodotto nonché ai soggetti preposti ai controlli. Un record accurato può anche rendere più efficiente la catena di approvvigionamento accelerando la distribuzione dei prodotti alimentari ai negozi e riducendone il deterioramento e gli sprechi.

I sistemi basati sulla blockchain hanno il potenziale di migliorare l'efficienza dei processi di approvvigionamento, logistica e pagamenti, ridurre l'elaborazione manuale della documentazione di importazione/esportazione, garantire la conformità e la consegna di merci e prevenire le perdite, abbassando in questo modo i costi, migliorando la sicurezza e la protezione e riducendo al minimo le frodi. Possono anche fornire i mezzi per verificare l'autenticità, l'origine e gli standard etici di merci e servizi. Le cronologie della proprietà trasparenti e tracciabili rivelerebbero eventuali precedenti in termini di frode, furto, uso di lavoro forzato, collegamenti al mondo della violenza, della droga o del traffico d'armi o qualsiasi altra pratica discutibile, migliorando la capacità di applicare la legge e consentendo un consumo più responsabile. Ci sono tuttavia dei motivi che inducono alla cautela. La fiducia reciproca tra i partecipanti dipende dalla fiducia nella tecnologia blockchain, che però non è completamente scevra da vulnerabilità, compresi tanto gli errori accidentali quanto gli attacchi dannosi. L'automazione non garantirà l'eliminazione di bug, conflitti d'interesse o corruzione nelle complesse catene di approvvigionamento globali.

Tramite la blockchain è possibile avvalersi dello pseudonimato. In altre parole, tutte le transazioni sono trasparenti ma non sono collegate esplicitamente a persone od organizzazioni nel mondo reale, proteggendo l'identità delle parti lungo la catena di approvvigionamento senza compromettere l'integrità del record. Il controllo degli attributi delle merci e dei loro movimenti può essere disgiunto dall'identità completa degli utenti, nascondendo i dati personali dettagliati riservati che esulano dalle esigenze di registrazione. Tuttavia, questo anonimato non è assoluto e, con il dovuto impegno, è possibile collegare le transazioni a specifiche parti. Sebbene tale approccio sia ampiamente considerato un miglioramento rispetto all'attuale sistema, potrebbero nascere questioni di riservatezza. Una volta che i beni hanno raggiunto i consumatori, il rintracciamento dettagliato dovrebbe cessare o, almeno, conformarsi agli standard di riservatezza e protezione dei dati.

Politica lungimirante

Lo sviluppo della blockchain nella gestione della catena di approvvigionamento presenta importanti sfide sul piano normativo. Atti quali la direttiva europea sulla comunicazione di informazioni di carattere non finanziario possono avere delle ripercussioni sulle applicazioni della blockchain per le catene di approvvigionamento. Alle aziende viene richiesto di divulgare informazioni affidabili sui temi ambientali, su aspetti riguardanti la sfera sociale e occupazionale, sul rispetto dei diritti umani e sulle problematiche relative al contrasto della corruzione, promuovendo così una maggiore trasparenza nelle loro operazioni. Tuttavia, l'assenza di un intermediario nella maggior parte delle fasi della catena di approvvigionamento, se non in tutte, potrebbe un giorno suscitare incertezza nelle parti coinvolte, soprattutto per quanto riguarda le forme automatizzate di esecuzione e supervisione delle transazioni. Nella maggior parte dei casi, è necessario porre in essere, ed eventualmente anche rielaborare, concetti e meccanismi di responsabilità per far fronte a problemi imprevisti.

7. Stati e blockchain: ripensare i servizi pubblici

Nel contesto dell'apertura di dati, servizi e decisioni nel settore pubblico grazie alle tecnologie digitali, è in fase di sviluppo una nuova generazione di servizi di governo elettronico aperti, responsabili, trasparenti e collaborativi. Il consulente scientifico capo del governo britannico ha di recente pubblicato una relazione in cui descrive in che modo le tecnologie basate sulla blockchain possono fornire nuovi strumenti per ridurre le frodi, evitare errori, tagliare i costi operativi, aumentare la produttività, supportare la conformità e imporre la responsabilità in molti servizi pubblici. Le potenziali applicazioni includono la riscossione delle imposte, la gestione delle identità, l'erogazione delle prestazioni sociali, le valute digitali locali (o nazionali), i catasti dei terreni e delle proprietà e qualsiasi tipo di documentazione governativa. La stessa tecnologia offre anche agli attori non statali la possibilità di fornire servizi simili a quelli statali, da quelli notarili a quelli di cittadinanza e identità globali. Il ruolo che rivestirà la blockchain nel settore pubblico è ancora da definire.

Come la tecnologia blockchain può supportare i servizi pubblici

I dati utilizzati dalle istituzioni pubbliche sono spesso frammentati internamente e non trasparenti agli altri attori, in particolare i cittadini, le aziende e gli organismi di sorveglianza. La tecnologia blockchain potrebbe consentire di creare e verificare dei record con un maggiore livello di velocità, sicurezza e trasparenza. Le applicazioni più immediate della tecnologia blockchain nelle amministrazioni pubbliche sono nel campo della tenuta della documentazione. Si prevede che la combinazione di marcatura temporale e firme digitali su un libro mastro accessibile offrirà vantaggi a tutti gli utenti, consentendo loro di condurre transazioni e creare dei record (ad es. per i registri catastali, i certificati di nascita e le licenze commerciali) riducendo la dipendenza da avvocati, notai, funzionari pubblici e altre terze parti.

Il governo estone ha sperimentato applicazioni delle blockchain consentendo ai cittadini di utilizzare la carta d'identità per richiedere prescrizioni mediche, votare, svolgere operazioni bancarie, presentare domande di sussidi, registrare attività commerciali, versare le imposte e accedere a circa altri 3 000 servizi digitali. Questo approccio consente anche ai dipendenti pubblici di crittografare documenti, esaminare e approvare permessi, contratti e domande e inoltrare delle richieste di informazioni ad altri servizi. Questo è un esempio di una blockchain con autorizzazioni, in cui l'accesso è parzialmente limitato per proteggere i dati e cautelare la riservatezza degli utenti. Allo stesso modo, il ruolo dello Stato quale autorità che mantiene il controllo sul sistema è in conflitto con la struttura dal basso verso l'alto di molte iniziative promosse dalla comunità di sviluppo della blockchain. Tuttavia il sistema, che sta per essere applicato anche ai servizi notarili pubblici e alle cartelle cliniche, rimane una delle iniziative governative più avanzate a fare uso della blockchain.

Diversi paesi, tra cui il Ghana, il Kenya e la Nigeria hanno iniziato a usare le blockchain per gestire i registri catastali. L'obiettivo è di creare un registro delle proprietà chiaro e affidabile in risposta ai problemi di registrazione, corruzione e scarso livello di accesso pubblico alla documentazione. Anche la Svezia sta effettuando dei test per inserire le transazioni immobiliari in una blockchain, in questo caso per consentire a tutte le parti (banche, governo, intermediari, acquirenti e venditori) di tenere traccia dei progressi della transazione in tutte le sue fasi e per garantire l'autenticità e la trasparenza della procedura, consentendo al contempo notevoli risparmi di tempo e denaro.

Anche il ministero del Lavoro e delle pensioni del Regno Unito ha sperimentato l'uso della tecnologia blockchain per i pagamenti assistenziali. In questo caso, i cittadini utilizzano il telefono per ricevere e spendere le prestazioni sociali erogate e, con il loro consenso, le transazioni sono registrate in un libro mastro distribuito. Lo scopo dell'iniziativa è di aiutare i cittadini a gestire le loro finanze e creare un sistema assistenziale più sicuro ed efficiente, evitando frodi e rafforzando la fiducia tra i richiedenti e il governo. Il governo britannico sta anche valutando in che modo la tecnologia blockchain potrebbe consentire ai cittadini di monitorare l'allocazione e la spesa dei fondi da parte del governo, dei

donatori e delle organizzazioni umanitarie a beneficio dei destinatari effettivi, sotto forma di sovvenzioni, prestiti e borse di studio.

Potenziati impatti e sviluppi

L'introduzione della tecnologia blockchain nelle pubbliche amministrazioni potrebbe portare a procedure interne ottimizzate, costi delle transazioni ridotti, interazioni più affidabili e scambi di dati con altre organizzazioni e strutture governative, oltre che a una maggiore protezione da errori e falsificazioni. Alcune procedure potrebbero anche essere automatizzate grazie agli smart contract. Esistono tuttavia dei rischi di cui bisogna tener conto. Innanzitutto, il passaggio a un nuovo sistema per la documentazione digitale comporterà dei costi di configurazione e potenziali difficoltà tecniche e procedurali di esecuzione di sistemi di backup e paralleli durante le fasi transizionali. Inoltre, è importante che le aspettative di custodia e controllo delle registrazioni pubbliche in essere al momento della loro creazione continuino a essere rispettate per lungo tempo a venire. Infine, poiché la tecnologia memorizza gli hash (descritti nella sezione relativa ai brevetti) o altre rappresentazioni digitali incomplete dei documenti, i privati e le organizzazioni dovranno investire ulteriori risorse per conservare i documenti nel lungo termine.

I libri mastri blockchain possono registrare la data/ora e i dettagli di una transazione ma non sono in grado di verificare l'accuratezza di quanto in essa descritto. È sufficiente che una transazione sia conforme ai requisiti tecnici del protocollo per diventare una parte immutabile del record, indipendentemente dalla veridicità dei suoi contenuti. Così come tutte le richieste e le presentazioni di informazioni agli uffici pubblici vengono esaminate prima di essere attuate, resta la necessità di garantire adeguati controlli per accettare e condividere informazioni sui loro equivalenti blockchain. Anche se un giorno potrebbe essere possibile automatizzare, supportare e rendere sicure alcune di queste procedure, non si pensa che esse saranno le nuove depositarie del ruolo di controllo attribuito ai dipendenti pubblici.

Il fatto che i dati nella blockchain siano immutabili, ossia che una volta immessi non possano essere modificati o rimossi, garantisce trasparenza e responsabilità. Tuttavia, ciò potrebbe anche tradursi in un rischio per la riservatezza e la protezione dei dati, in particolar modo quando si tratta di dati personali o riservati (che non dovrebbero mai essere memorizzati in una blockchain). Le blockchain non garantiscono l'anonimato e, quanto più sono personali i dati, tanto più è facile identificare la persona a cui si riferiscono. Questa immutabilità potrebbe compromettere il "diritto all'oblio", in base al quale gli utenti possono, in determinate circostanze, richiedere che i loro dati personali vengano cancellati.

È importante garantire che tutti i cittadini possano accedere ai servizi pubblici loro destinati. La blockchain rischia di esacerbare l'attuale divario digitale. I cittadini che, per qualsivoglia motivo, non sono in grado di utilizzare i servizi Internet potrebbero non essere in grado di trarre pieno e diretto vantaggio degli sviluppi della blockchain che offrirebbero un maggior controllo sui loro dati e sulle loro transazioni. In molti casi, i servizi basati sulla blockchain sarebbero celati sotto interfacce di servizio familiari e facili da usare. La precisa implementazione del protocollo, in termini sia di struttura sia di interfaccia utente, riveste grande importanza per i valori politici e sociali promossi dal sistema. Vale infine la pena osservare che alcune iniziative relative alla blockchain promuovono l'elusione delle istituzioni e delle autorità centralizzate tradizionali, compresi i governi e i servizi pubblici. Dei servizi "simili a quelli statali" basati sulla blockchain, offerti da attori non statali, stanno già emergendo. Potrebbero essere allettanti per le comunità sempre più digitalizzate e globalizzate ma potrebbero anche porre le autorità statali di fronte a problematiche complesse.

Politica lungimirante

Le amministrazioni pubbliche manterranno probabilmente un sostanziale controllo centrale sulle loro applicazioni della blockchain e potrebbero anche chiedere delle "backdoor" ai sistemi blockchain crittografati privati per finalità di contrasto, anche se in tal modo rischierebbero di introdurre nuove vulnerabilità in termini di sicurezza. La crittografia end-to-end potrebbe essere un altro elemento da prendere in considerazione in occasione della futura revisione della direttiva e-privacy dell'UE. I governi potrebbero valutare in che modo la blockchain potrebbe aiutarli a migliorare i servizi pubblici, in particolare in termini di trasparenza e responsabilità, e se sia opportuno che i governi riconoscano i servizi indipendenti "simili a quelli statali" nell'ambito delle rispettive giurisdizioni.

8. Blockchain per tutto? Organizzazioni autonome decentralizzate

I primi pionieri di Internet immaginavano un nuovo ordine sociale di organizzazioni più indipendenti, decentralizzate e agili, facilitato dalle tecnologie dell'informazione e delle comunicazioni. Secondo alcuni, il modello peer-to-peer e quello basato sui beni collettivi gestirebbero meglio l'uso delle risorse, e qualcuno sta già sviluppando delle cooperative di piattaforma di proprietà collettiva dei loro utenti o lavoratori, che le governano democraticamente. La blockchain può supportare tali organizzazioni consentendo uno scambio di dati o proprietà, l'esecuzione di bilanci e l'esecuzione automatica di contratti o di processi decisionali in un'organizzazione in maniera diretta e istantanea, il tutto in modo trasparente e crittografato. Potrebbe questo annunciare l'affacciarsi di nuove organizzazioni abilitate alla blockchain, e cosa significherebbe per la società europea?

Libri mastri decentralizzati per organizzazioni decentralizzate

Le organizzazioni autonome decentralizzate (decentralized autonomous organization, DAO) possono essere intese come dei pacchetti di smart contract, culminanti in un insieme di regole di governance attuate ed eseguite automaticamente mediante le blockchain. Una DAO può adottare un ruolo di mediazione tra le diverse parti in un'organizzazione decentralizzata ma in ultima istanza controllata da persone oppure può costituire un'organizzazione più pienamente autonoma interamente controllata mediante algoritmi. Il livello di autonomia e autosufficienza che verrà raggiunto dalle DAO resta ancora da capire. La DAO più matura, denominata "The DAO", non è pienamente autonoma, anche se non è impossibile immaginare un futuro in cui altre DAO saranno quasi completamente indipendenti dall'intervento umano, controlleranno le proprie risorse e interagiranno con altre entità, umane e non umane, comprese altre DAO. Una DAO potrebbe ad esempio possedere una vettura senza conducente che opera come un taxi 24 ore al giorno. Tale attività genererebbe un ricavo che userebbe per pagare carburante, riparazioni e assicurazione e per accantonare i soldi necessari per sostituire il veicolo alla fine della sua durata di vita utile.

Nelle DAO la cooperazione tra persone nelle e tra le organizzazioni può basarsi non tanto su un'autorità centrale o pure forze di mercato bensì sul consenso crittografico e la trasparenza quali caratteristiche tecniche di base. Gli smart contract sulla blockchain hanno il potenziale non solo di lasciare una registrazione a prova di manomissione di ogni aspetto di un'organizzazione ma anche di eseguire automaticamente, e persino autonomamente, operazioni quotidiane quali il supporto dell'accesso a attività ed edifici, l'assegnazione di incarichi, la gestione di azioni e diritti di voto oppure agevolando la distribuzione dei profitti o la trasmissione di micropagamenti.

È stato suggerito che la tecnologia blockchain potrebbe consentire a una nuova generazione di organizzazioni di modificare le dinamiche economiche e di potere degli organi centralizzati tradizionali. Un esempio può essere una piattaforma di social media appartenente ai suoi utenti che si attribuiscono reciprocamente una valutazione e vengono ricompensati automaticamente per il loro contributo; un altro esempio ancora potrebbe consistere in una app di condivisione delle corse, in cui

gli autisti sono anche comproprietari e gestiscono le operazioni quotidiane oppure altre comunità come Steem-it, in cui gli utenti sono anche azionisti e valore e processi decisionali sono ripartiti in modo trasparente.

Potenziali impatti e sviluppi

La blockchain può essere utilizzata per sviluppare strutture decentralizzate all'interno delle organizzazioni. Allo stesso tempo, però, utilizzare la blockchain per tutte le transazioni potrebbe limitare i flussi di informazioni che finora sono stati prevalentemente liberi. Una supervisione e un controllo dell'accesso a ogni trasferimento di attività o contenuti potrebbe portare a rivendicazioni di proprietà intellettuale più rigorose (ad esempio nella gestione dei diritti digitali) e potrebbe soffocare l'innovazione e la comparsa di nuovi operatori. Rimuovendo la gestione centralizzata, le DAO potrebbero eliminare gli errori e la corruzione introdotti dalla componente umana. La fiducia si sposterà dalla classica reputazione alle reti tecno-sociali (come nei contratti e nelle valute abilitati alla blockchain). Qualcuno afferma che questo potrebbe portare a nuove forme di azione collettiva democratica, trasformando gli approcci di governance dall'alto verso il basso oggetto di critiche perché non flessibili, opachi, lenti e scarsamente democratici.

“The DAO” ha raccolto più di 100 milioni di euro nella più grande campagna di crowdfunding mai vista. Si tratta di una combinazione tra un sito di crowdfunding e un fondo di capitale di rischio basata su smart contract di Ethereum. I fondatori esprimono il loro voto per ogni decisione presa, dalla nomina e dal licenziamento dei suoi curatori al finanziamento di progetti. Nel giugno del 2016 un attacco ha sfruttato talune debolezze nel codice della DAO prosciugando circa un terzo delle sue risorse e scatenando una controversia nella comunità in merito al da farsi. Le opzioni erano congelare i fondi nel conto (un "soft fork"), forzare il sistema e ripristinare il saldo originale (un "hard fork") oppure non fare nulla. Da una parte, poiché gli autori dell'attacco hanno sfruttato una debolezza nel codice, si potrebbe argomentare che non hanno violato il contratto e che modificare la blockchain di “The DAO” minerebbe la fiducia del pubblico nel suo principio di immutabilità. Dall'altra, l'attacco ha chiaramente violato lo spirito del contratto, potrebbe avere infranto il diritto contrattuale e potrebbe scoraggiare i partecipanti effettivi e potenziali alla comunità. In ogni caso, l'incidente ha reso palesi le vulnerabilità esistenti in termini di sicurezza e ha messo alla prova le fondamenta ideologiche della comunità di sviluppo della blockchain.

La resistenza all'utilizzo delle strutture legali esistenti (ad esempio trattare i core developer e i miner come fiduciari) è stata fautrice di meccanismi alternativi o più sofisticati, quali i sistemi di buona reputazione/ meritocratici per incentivare la partecipazione o per l'adozione di norme e valori etici condivisi. Tuttavia, il funzionamento autonomo di tali organizzazioni suscita anche perplessità per la delega e la regolamentazione, che sono affidate ad algoritmi. C'è chi afferma che tale governance distribuita mediante codice implica comunque il dovere o la responsabilità morale della comunità di intervenire sulle decisioni fondamentali, mentre c'è chi sta lavorando all'integrazione di valori umani e della volontà generale dei cittadini nei contratti sociali algoritmici.

Politica lungimirante

Le DAO, come molte iniziative basate sulla blockchain, esistono in una zona grigia a livello normativo che potrebbe non offrire garanzie di responsabilità, protezione e rendicontabilità, soprattutto quando non sono esplicitamente fondate sui sistemi giuridici esistenti. Preoccupazioni di natura legale sono suscitate anche dalle offerte azionarie nelle aziende a base crittografica, che potrebbero far rientrare tali aziende nell'ambito dell'esistente mercato mobiliare con requisiti di registrazione e conformità a una serie di norme e obblighi. Operando fuori da un quadro normativo, le organizzazioni basate sulla blockchain che non sono incorporate o riconosciute legalmente potrebbero essere a rischio di frodi sugli investimenti e di attacchi hacker e i loro membri potrebbero essere esposti a passività in quanto partner. Si è anche levata qualche voce per chiedere una maggiore supervisione e trasparenza nel

processo decisionale algoritmico e una modellazione interattiva. La complessità degli algoritmi avanzati rende arduo anche per gli sviluppatori comprendere appieno le norme che li disciplinano e controllare la loro conformità giuridica, ad esempio con le leggi in materia di trasparenza e anti-discriminazione. Le organizzazioni ad esecuzione e applicazione automatiche potrebbero anche sfidare le classiche nozioni di personalità giuridica, azione individuale e responsabilità.

Le DAO potrebbero essere programmate per commerciare in merci illecite o prodotti vietati. Anche laddove non è garantito l'anonimato, la struttura efficiente, automatica e distribuita della sottostante blockchain potrebbe rendere difficile per gli enti normativi applicare la legge e disporre la chiusura delle attività. Le vittime di reati perpetrati da una DAO potrebbero avere difficoltà a esigere il risarcimento dei danni o a ottenere un'ingiunzione contro la DAO in malafede nel caso in cui la capacità di intraprendere tali misure non sia specificamente codificata nella sua struttura.

Conclusioni

Anche se l'applicazione della blockchain meglio conosciuta, più utilizzata e con il maggiore impatto è Bitcoin, gli effetti potenziali di questa tecnologia sono molto più grandi e vanno ben oltre le valute virtuali. In effetti, poiché altre applicazioni possono servirsi della blockchain Bitcoin, le maggiori ripercussioni di Bitcoin possono essere riscontrate fuori dall'ambito delle valute. Le transazioni di qualsiasi tipo sono di norma più veloci ed economiche per l'utente quando sono completate mediante una blockchain e si avvalgono anche della sicurezza del protocollo. Considerato che la maggior parte delle transazioni in Europa sono spesso sufficientemente rapide, economiche e sicure, gli utenti e i proponenti di applicazioni blockchain spesso vedono dei vantaggi aggiuntivi nella trasparenza e immutabilità che caratterizzano la blockchain. Si riscontra in effetti una tendenza crescente a fidarsi di meno delle istituzioni finanziarie e di governance e ad avere maggiori aspettative sociali in termini di rendicontabilità e responsabilità. La popolarità della tecnologia blockchain potrebbe anche riflettere una tendenza sociale emergente a privilegiare la trasparenza rispetto all'anonimato.

Ovviamente, per ogni transazione che usa un libro mastro distribuito invece di un sistema centralizzato classico, gli intermediari e i mediatori sono sostituiti e privati della loro tradizionale fonte di potere e reddito. Per le valute si tratta delle banche, per i brevetti dell'ufficio brevetti, per le elezioni delle commissioni elettorali, per gli smart contract degli esecutori e per i servizi pubblici delle autorità statali. Un livello di crescita significativo nell'uso della tecnologia blockchain potrebbe tradursi in un cambiamento sostanziale della natura e, probabilmente, della quantità di lavoro dei "colletti bianchi". Per fare un esempio, parte del lavoro degli intermediari e degli avvocati operanti nel campo del diritto contrattuale potrebbe essere sostituito da transazioni peer-to-peer e smart contract. Molti commentatori non sembrano particolarmente preoccupati da questa prospettiva. Qualcuno asserisce che le blockchain subentrerebbero solo ad alcune delle attività meno interessanti, come ad esempio fornire la prova della certificazione, lasciando più tempo per le attività essenziali e ad elevato valore di prestazione di servizi personalizzati. Sebbene la cosa potrebbe riflettersi in una certa riduzione della quantità di lavoro totale, altri commentatori citano delle similitudini con le ondate di automazione nel lavoro delle "tute blu" di cui siamo già stati testimoni, come ad esempio le linee di produzione robotizzate, in cui lo spostamento delle attività ripetitive significò sì una perdita di posti di lavoro ma anche la creazione di nuovi lavori di elevata qualità nella progettazione e manutenzione dei sistemi necessari. In ogni caso, benché non sussistano molte prove, la maggior parte dei commentatori prevede un cambiamento nel profilo delle attività eseguite dagli esseri umani senza alcuna riduzione globale del numero totale di posti di lavoro e, forse, con un aumento della loro qualità. Un altro potenziale impatto indiretto dello sviluppo blockchain potrebbe essere un maggiore consumo energetico. Nel 2014 il consumo di elettricità imputabile alla blockchain Bitcoin era paragonabile a quello dell'Irlanda ed è continuato a crescere. Anche se potrebbero essere messi a punto degli algoritmi e dell'hardware più efficienti, l'intensità energetica delle blockchain (e, in effetti, quella di tutti i processi digitali) rischia di diventare nel tempo un problema crescente.

L'effetto più profondo dello sviluppo della blockchain può riscontrarsi negli impatti più sottili su strutture e valori sociali diffusi. Tali impatti sono associati ai valori integrati nella tecnologia. Tutte le tecnologie hanno dei valori e delle politiche, che di norma rappresentano gli interessi dei loro creatori. In quest'ottica, i motivi per cui i classici sistemi di libro mastro mettono i loro creatori in una posizione di intermediari centrali sono chiari: poiché tutte le transazioni passano per le loro mani, i creatori mantengono la loro posizione di potere e la capacità di trarre profitti dai loro utenti. Utilizzando le tecnologie, le persone riaffermano i valori e le politiche che esse rappresentano e quindi, ogni volta che questi libri mastri vengono utilizzati per registrare una transazione, vengono riaffermate la centralità e l'indispensabilità dell'attore al centro delle stesse. Naturalmente anche un libro mastro distribuito senza un intermediario centrale è espressione di valori e politiche, in quanto ripone fiducia nella tecnologia di crittografia e di networking e ridistribuisce il potere dalle autorità centrali a strutture non gerarchiche e peer-to-peer. In questo contesto, l'uso di questo tipo di blockchain *significa*

partecipare a una transizione più ampia in cui diminuiscono la fiducia nelle istituzioni classiche, quali le banche e i governi, nonché il loro potere. I casi presi in considerazione in questa relazione rivelano diversi esempi di come le applicazioni blockchain incarnino questi valori. Ovviamente, riuscire a percepire questi cambiamenti a un livello sociale generale richiederebbe uno sviluppo tanto consistente della blockchain da arrivare a permeare la vita di tutti i giorni e le sue consuetudini.

Giova osservare che l'interesse per le applicazioni basate sulla blockchain sembra spesso andare di pari passo con l'insoddisfazione per i sistemi, le procedure e i mediatori tradizionali. Lo sviluppo della blockchain spesso presenta delle analogie con l'economia collaborativa, nel senso che promettono di connettere tra di loro le persone, finalmente liberate da intermediari e dal peso di Stati, banche e altre

Politica lungimirante

A prima vista, la natura decentralizzata, crittografata e ad esecuzione automatica delle applicazioni tecnologiche blockchain sembra presumere e contare su un approccio di autoregolamentazione che in linea di principio opererebbe in parallelo ai classici strumenti giuridici. Tuttavia, un'osservazione più attenta delle applicazioni blockchain più sofisticate rende palese una serie di questioni normative e giuridiche, sia nuove sia classiche, di cui bisogna tener conto in modo contestuale, poiché alcune delle applicazioni summenzionate mettono in discussione taluni aspetti fondamentali del diritto e diffondono l'oggetto dell'attenzione regolamentare in quanto tale in diversi modi.

Innanzitutto, la natura decentralizzata e transfrontaliera della blockchain solleva problemi giurisdizionali poiché sembra diffondere la rendicontabilità istituzionale e la responsabilità legale in un modo che non ha precedenti, rendendo l'esigenza di un approccio regolamentare armonizzato a livello transnazionale più pertinente di uno locale o regionale. Se la tecnologia blockchain si sviluppasse in modo significativo, le strutture giurisdizionali centralizzate potrebbero non riuscire più a controllare il libro mastro, con un passaggio del controllo ai suoi utenti o ad altre parti nel sistema, o a orientare le attività di persone eterogenee o organizzazioni decentralizzate autonome, poiché nessuno (compreso il creatore originale) può controllare il libro mastro, una volta introdotto. Ci sarebbero meno punti di controllo per guidare e assistere il flusso di dati. Ci sono anche diverse questioni da prendere in considerazione, come l'applicabilità giuridica degli smart contract e i problemi di responsabilità e rendicontabilità, poiché ai libri mastri attualmente manca la personalità giuridica necessaria perché vengano loro assegnati responsabilità e obblighi. Il problema è esacerbato dal fatto che operano a livello transfrontaliero e che gli smart contract potrebbero non essere ancora in grado di eseguire operazioni complesse.

I sistemi basati sulla blockchain e decentralizzati potrebbero essere esposti alla cooptazione di poteri esterni e, in assenza di una sufficiente protezione istituzionale, le piattaforme potrebbero evolversi in oligarchie. Un'organizzazione autonoma decentralizzata malintenzionata potrebbe essere fonte di preoccupazioni regolamentari, data la possibilità di un uso improprio di questa tecnologia trasformativa. Inoltre, le qualità crittografate della tecnologia blockchain potrebbero rendere impossibili le legittime forme di sorveglianza utilizzate per intraprendere azioni legali e applicare la legge. Anche la protezione dei consumatori è una preoccupazione chiave per le autorità di regolamentazione, poiché le clausole contrattuali e i mezzi di ricorso potrebbero non essere chiari per i consumatori e, data la loro natura automatizzata, non facilmente adattabili a un possibile cambiamento delle circostanze. Inoltre a livello regolamentare si nutrono timori inerenti alla sicurezza, poiché potrebbe essere possibile, partendo dalle transazioni, risalire all'identità di una parte o dedurla. Infine, le blockchain potrebbero sollevare dubbi sulla scelta della legge applicabile e del foro competente per deliberare sulle controversie in questione.

grandi istituzioni, spesso con una retorica di transizione, rottura o anche rivoluzione. Tuttavia, come si è visto, le iniziative di maggiore successo di questo movimento hanno alla fine assunto la forma di intermediari all'ennesima potenza, strutturalmente molto distanti dalla visione di decentralizzazione che molti cittadini auspicavano. La stessa situazione si può osservare con la blockchain, dove il maggiore impatto si manifesta nelle applicazioni che sembrano lontane dalla più idealistica visione di uno sviluppo della blockchain caratterizzato da decentralizzazione e trasparenza. Un'autorità elettorale potrebbe, ad esempio, attuare un sistema elettorale basato sulla blockchain ad accesso ristretto, mantenendo il controllo sulla distribuzione di pseudonimi per garantire l'anonimato e affermando il suo ruolo come autorità di ultima istanza e mediatore centrale attraverso il quale devono passare tutti i voti. E' tuttavia innegabile che un siffatto approccio presenta potenziali vantaggi tecnici e politici, ma va anche detto che in questo tipo di blockchain ad accesso ristretto il livello di decentralizzazione e trasparenza è ridotto, con conseguenze per la struttura tecnica e la funzionalità del libro mastro, oltre che per i valori e le politiche di cui è l'espressione. È possibile immaginare vari parallelismi per registri catastali, banche e uffici brevetti, ciascuno dei quali potrebbe adattare aspetti tecnici del protocollo blockchain moderando al tempo stesso gli elementi idealistici dei valori in esso integrati. È plausibile che tali sistemi offrirebbero comunque miglioramenti sostanziali in termini di maggiore trasparenza e rendicontabilità e minore corruzione. In effetti, cooptando la blockchain, le istituzioni di governance potrebbero utilizzarla per creare delle "tecnologie di regolamentazione" impiegate per raggiungere gli stessi obiettivi di regolamentazione, ad esempio trasparenza o rendicontazione, delle leggi esistenti.

Poiché gli intermediari sono esclusi dalla blockchain, non è possibile contare su di loro perché ne regolino il funzionamento. È necessario pertanto sviluppare strumenti regolamentari alternativi per far rispettare la legge e conservare la capacità di pianificare e agire in modo efficace. È possibile identificare quattro ampie categorie di azione che le istituzioni di governance potrebbero mobilitare in risposta all'emergere della tecnologia blockchain:

- Una prima opzione consiste nel rispondere ai "problemi per i quali la blockchain rappresenta una soluzione" senza utilizzarla affatto. Ad esempio, se la domanda di blockchain è basata su un desiderio di maggiore trasparenza nelle procedure, ai cittadini potrebbe essere concesso un maggiore accesso alle procedure e ai dati governativi senza usare i sistemi blockchain.
- Una seconda opzione consiste nell'incoraggiare in modo attivo lo sviluppo e l'innovazione di blockchain da parte del settore privato attribuendo legittimità ai loro prodotti. Ad esempio, in alcune condizioni, alle transazioni sulle blockchain si potrebbe dare un riconoscimento giuridico esplicito come registrazioni di transazioni eseguite.
- Una terza opzione consiste nell'invertire quella precedente, ossia scoraggiarne lo sviluppo rifiutando l'accettazione della legittimità delle transazioni basate sulla blockchain, ad esempio invalidando e annullando le clausole negli smart contract.
- Una quarta opzione consiste nell'adottare una blockchain permissioned nei sistemi e nelle infrastrutture esistenti, mantenendo efficacemente il ruolo e il potere dei responsabili in quanto intermediari fornendo alcune delle funzionalità di base delle blockchain ma senza offrire una decentralizzazione e una trasparenza complete. Questo modello si può già osservare nell'uso della tecnologia blockchain nel settore pubblico, ad esempio nel Regno Unito e in Estonia, oltre che nel settore privato.

Variazioni e combinazioni di tutte e quattro le strategie summenzionate saranno probabilmente applicate alla tecnologia blockchain in vari settori e giurisdizioni nel prossimo decennio. Un intervento a livello europeo non suscita al momento particolare interesse. In effetti, una recente relazione del Parlamento europeo sulle valute virtuali ha riconosciuto i crescenti rischi che richiederanno un rafforzamento della capacità normativa e competenze tecniche adeguate, chiedendo nel contempo un approccio normativo proporzionato da parte dell'UE per non ostacolare l'innovazione in una fase così precoce.

In conclusione, il fatto che il protocollo blockchain fornisca alle piattaforme sia azioni buone che azioni cattive non significa che sia una tecnologia neutrale. Nella sua essenza la tecnologia blockchain promuove una redistribuzione del potere dagli attori centrali ad ampie comunità tra pari. Mentre le visioni più idealistiche e rivoluzionarie dello sviluppo blockchain rimarranno probabilmente nient'altro che visioni, anche un'implementazione moderata della blockchain potrebbe comunque promuovere un certo grado di redistribuzione e trasparenza. Come osserva Glyptis, la blockchain non ci rende migliori ma renderà alcune delle misure precauzionali necessarie nella vita quotidiana più rapide, economiche, sicure e trasparenti.

La tecnologia blockchain suscita sempre più l'interesse di cittadini, imprese e legislatori in tutta l'Unione europea. La presente relazione intende fornire i primi rudimenti a chi è incuriosito dalla tecnologia blockchain al fine di stimolare l'interesse e provocare un dibattito sul suo potenziale impatto. Dopo un'introduzione generale, si procede a un esame più approfondito di otto aree in cui la blockchain avrebbe un sostanziale impatto potenziale. Per ciascuna di esse, viene fornita una spiegazione del modo in cui la tecnologia potrebbe essere sviluppata in tale ambito specifico, i possibili impatti di tale sviluppo e i potenziali problemi politici da prevedere.

La presente è una pubblicazione della
Direzione Valutazione d'impatto e valore aggiunto europeo
Direzione generale dei Servizi di ricerca parlamentare, Parlamento europeo



PE 581.948
ISBN 978-92-846-1042-6
doi: 10.2861/13366
QA-02-17-043-IT-N

Il presente documento costituisce materiale informativo destinato ai membri e al personale del Parlamento europeo ed è stato preparato per assisterli nelle loro attività parlamentari. Il suo contenuto è di esclusiva responsabilità degli autori e i pareri ivi espressi non devono essere considerati rappresentativi di una posizione ufficiale del Parlamento.