

OVER DATA.

Giugno
2023



Artificial Intelligence
& Tech Culture

INDICE



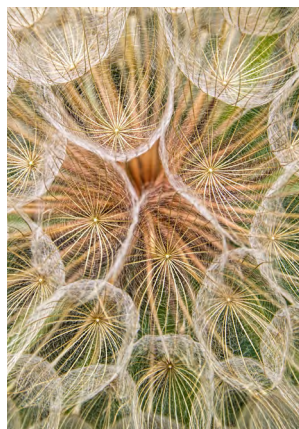
03

**Ai e block-
chain: a fin-
tech romance**



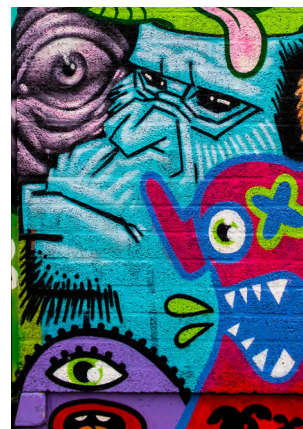
15

**La blockchain
per il settore
energy**



29

**Green new
deal e block-
chain**



42

**L'opera d'ar-
te nell'epoca
della sua (ri)
producibilità
tecnica**

10

**Ai generative,
token e com-
munity buil-
ding**

22

**Tour esplora-
tivo del testo
approvato del
MiCa**

36

**Zero Knowled-
ge Proofs**

48

**“Cogito ergo
sum”: l'identi-
tà sovrana au-
tonoma sposa
la blockchain**



01

AI e blockchain: a fintech romance

Il rilascio di ChatGPT sul mercato ha reso evidente che ormai siamo entrati a pieno titolo nella quarta rivoluzione industriale. Tecnologie dall'ampia portata trasformativa sono ora a disposizione degli operatori che vogliono conquistare nuovi mercati, ampliare la propria market share ed efficientare la propria struttura costi: le potenzialità sono davvero infinite. La sensazione che "il genio sia uscito dalla lampada" è piuttosto chiara. Già nel primo mese di utilizzo più di 1000 tra scienziati e imprenditori hanno proposto una moratoria sugli sviluppi delle AI, per potere comprendere meglio una tecnologia che in

appena tre mesi dal rilascio ha già cambiato numerosi business model e suscitato ammirazione e timore allo stesso tempo. Il Garante della Privacy italiano è intervenuto, tra i primi, a tutela dei dati personali degli utenti. Pare che l'adagio "i dati sono il nuovo petrolio" sia particolarmente azzeccato in questo nuovo spazio digitale nel quale le AI effettivamente li utilizzano come le auto usano il carburante.

L'adozione di tecnologie "disruptive" da parte degli operatori di mercato avviene sempre a seguito di un'approfondita analisi risk/reward. Tra le promesse dell'AI, sulle

quali ci sentiamo fiduciosi a "scommettere", possiamo enumerare sicuramente: il miglioramento della raccolta e processing dei dati; migliori output previsionali; automazione e personalizzazione delle interazioni, con ricadute cross-industry, dall'agricoltura alla sanità alla finanza, all'entertainment.

I rischi maggiori che le imprese dovranno gestire, a fronte degli indiscutibili vantaggi che porta l'IA, sono invece afferenti a tre aree: (I) rispetto dei diritti sostanziali e compliance normativa; (II) trasparenza nella raccolta e utilizzo dei dati; (III) trasparenza nei processi decisionali

delle AI che incidono sui diritti delle persone (principio inserito nell'ordinamento comunitario, per la prima volta, con l'art. 22 del GDPR).

Data questa breve e sintetica descrizione di rischi e benefici che l'utilizzo dell'AI può portare in azienda appare subito la necessità di strutturare i database su cui questi modelli si appoggeranno by design, come compatibili con il framework normativo. E questa sfida è la chiave di volta per cogliere nuove opportunità.

Trasparenza e tracciabilità sono infatti le caratteristiche principali dei network basati su tecnologia blockchain. Essi si rivelano, in questo caso d'uso, i migliori partner possibili per l'utilizzo industriale dell'AI. Il campo di interazione tra queste due tecnologie può essere diviso tra utilizzi di supporto delle AI, e utilizzi per il loro accrescimento funzionale.

Blockchain a supporto delle AI

Le perplessità espresse dal garante della privacy italiano nei primi mesi del 2023 si ri-

trovano, in realtà, nella bozza di Regolamento EU sulle intelligenze artificiali pubblicata nel 2021 (Regolamento che dovrebbe essere adottato entro la fine del 2023 e a cui tutti gli operatori si dovranno adeguare). Come affermato precedentemente, le due principali richieste dei regulator girano attorno alla certificazione delle basi dati utilizzate e alla trasparenza nell'utilizzo di tali dati da parte delle AI.

Gli operatori che utilizzano AI dovranno infatti rispondere

a una serie di requisiti operativi che dovranno trovare una risposta, by design, già nell'architettura dei servizi. Gli operatori dovranno infatti garantire, tra l'altro:

- La governance dei dati: i data set usati per l'addestramento dei modelli AI dovranno soddisfare numerosi criteri di qualità e dovrà essere possibile la disclosure in relazione alla loro etichettatura, pulizia, arricchimento e aggregazione;
- La conservazione delle re-



“

Le due richieste dei regulator girano attorno alle certificazioni delle basi dati

”

gistrazioni: gli operatori di piattaforme AI dovranno registrare in maniera automatica (“log”) gli eventi che accadono su dette piattaforme, e garantire la tracciabilità del funzionamento del sistema;

- Garantire la trasparenza dei processi: gli utenti dovranno essere in grado di interpretare l’output del sistema e utilizzarlo adeguatamente e garantire la trasparenza sugli utilizzi

di output come input per operazioni future (“circuiti di feedback”, feedback loops)

- Gestire i log: conservare i log generati automaticamente per un periodo adeguato per verifiche ex post;
- Monitoraggio continuo: bisognerà implementare un sistema di monitoraggio successivo all’immissione sul mercato della AI

per documentare e analizzare attivamente e sistematicamente i dati forniti dagli utenti o raccolti tramite altre fonti sulle interazioni con le piattaforme AI;

- Accesso ai dati e documentazione: dato che alle autorità di vigilanza sarà concesso pieno e continuo accesso ai set di dati di addestramento, convalida e prova utilizzati dagli operatori AI, gli stessi do-





vranno fornire API, o altri strumenti equiparabili, per consentire adeguati controlli alle autorità di vigilanza.

Se da una parte il Regolamento EU deve ancora essere discusso e approvato, dall'altra la direzione è molto chiara. Come stabilito inizialmente dal GDPR, le pietre angolari dei sistemi informativi che incidono sui diritti delle persone o hanno a che fare con informazioni sensibili degli utenti (talvolta utilizzati impropriamente) sono: consenso sul trattamento dei dati, trasparenza dei processi e ac-

cessibilità.

Per fortuna l'esperienza maturata in ambito privacy e nell'utilizzo della tecnologia blockchain ci viene in aiuto, rispondendo, by design, a questi requisiti di sistema. È infatti facile immaginare una piattaforma di AI che si appoggi a un database distribuito che abiliti le seguenti funzionalità:

- decentralizzazione del data processing per prevenire frodi;
- utilizzo della crittografia per garantire integrità e autenticità dei dati (time

stamping) e allo stesso tempo accessibilità (architettura distribuita e pubblica) e privacy (tecnologie come monero, zsnarks);

- smart contract per tracciare l'utilizzo dei dati nei processi decisionali più significativi (trasparenza);
- smart contract per tracciare l'intervento umano nei processi decisionali (si pensi all'applicazione dell'articolo 22 GDPR alle AI);
- firma digitale e tokenizzazione dei pacchetti dati: per segregare i dati provenienti dai feedback loop e aggiungerli alla base dati, certificando sia il consenso alla loro archiviazione che l'acquisizione nel database.

Una piattaforma mista blockchain / AI permetterebbe quindi, by design, di rispettare i vari paletti normativi che sono stati individuati dal regulator comunitario by design (come per altro consigliato) in modo radicale, che sia scalabile poi con i vari input e requisiti di business.

L'utilizzo congiunto dell'AI e della blockchain può, inoltre, aprire la porta a nuovi scenari e opportunità di business.

Blockchain e AI per la crescita esponenziale

Robot, AI e blockchain. Una delle applicazioni più promettenti a cavallo tra blockchain e AI sono le piattaforme per la gestione di flotte di robot. Pensiamo ad esempio a quelle di droni che operano nella

logistica, che devono interagire tra di loro e possibilmente migliorare il software alla luce delle loro interazioni. In questo caso la soluzione più elegante e scalabile è sicuramente l'utilizzo di un registro distribuito in cui i robot sono agenti che scambiano informazioni e che le processano tramite un'infrastruttura pensata per la condivisione dati e il rispetto della privacy. I dati vengono trasferiti da macchina a macchina, grazie a un sistema di tokenizzazione. Sono poi fruiti grazie a smart

contract, che trasferiscono le evoluzioni dei modelli di AI a tutti i partecipanti del network. Il processo di coordinamento delle azioni dei robot viene invece gestito tramite consenso distribuito a livello di blockchain sullo "stato" della virtual machine sottostante al database distribuito.

Cybersecurity

L'affidabilità del database su cui le AI fanno training diventerà sempre più cruciale negli anni a venire, soprattutto se le AI verranno utilizzate in settori critici come quello farmaceutico, finanziario e amministrativo. Nel campo della cybersecurity stanno già nascendo applicativi basati su blockchain per costruire banche dati distribuite su cui le AI possano fare affidamento, anche per monitorare gli accessi e gli utilizzi dei dati sensibili a fini di compliance. Gli applicativi, sviluppati in un primo momento per risolvere problemi di cybersecurity, possono poi essere utilizzati anche come piattaforme di data sharing che combinino meccaniche di data monetisation con funzionalità per il rispetto della privacy.

AI e community



I protocolli AI, a seguito dei feedback loop che si instaurano con gli utenti, crescono, imparano e cambiano. Le AI possono diventare allora potenti aggregatori di community e nuovi utenti che, dando il consenso all'utilizzo dei propri dati e delle proprie interazioni, partecipano alla "crescita ed educazione" dell'AI stessa. Ciò porta notevoli vantaggi. Ad esempio una community appassionata di musica potrebbe, attraverso una AI "DJ", insegnare alla AI come selezionare nuovi brani che rispecchiano i gusti della community instaurando un feedback loop molto forte tra gusti della community, che vengono quindi restituiti dall'AI tramite la selezione e lo scouting di brani, e appartenenza identitaria ad un brand o una piattaforma che strutturalmente prende in considerazione i gusti della community stessa.

Intelligenze federate

Possiamo anche immaginare delle architetture completamente integrate tra AI e blockchain per aggregare i vantaggi delle interazioni tra queste due tecnologie. Uno dei principali driver della competizione tra AI sarà sicuramente l'accesso ai dati e il

training/feedback loop che si instaurerà con gli utenti. Un modello molto interessante vede la creazione di una "federazione" di AI, che partecipano come validatori ad un network blockchain pubblico. Mentre ciascuna AI gestisce il proprio data set in locale, la stessa condivide metadati e modelli con tutte le altre, che possono a quel punto pagare autonomamente questi "upgrade" e costruire a loro volta modelli più precisi/funzionali da redistribuire nel network federato. Si osserva così un sistema di feedback loop uomo-AI\AI-AI\AI-uomo, che apre nuove opportunità industriali.

Cosa può fare WizKey

WizKey dedica ampio spazio alle attività di R&D e ha già iniziato a sviluppare i primi applicativi per la notarizzazione dei data-set da utilizzare per il training delle AI. Oggi, sta già conducendo un POC della prima AI "comunitaria" per un noto brand di moda. Le piattaforme già sviluppate, DeFiNe e Bellerofonte, possono essere facilmente personalizzate nell'ambito della collaborazione Spindox/WizKey per validare e certificare i dati, tracciare i flussi

informativi e migliorare la cybersecurity dei nostri clienti. Crediamo anche di essere, in tandem con Spindox, il partner giusto per individuare nuove soluzioni, tarate sui bisogni dei nostri clienti, da inserire nei processi di sviluppo delle aziende che intendono utilizzare la AI nei propri processi industriali.







AI generative, token e commu- nity building

Botto emette NFT a partire dalle preferenze della community

Da qualche mese non si fa che parlare di AI e in particolare modo di AI generative, in quanto, come ci insegnano i social media, le immagini attraggono più delle parole. Un altro settore tecnologico che ha saputo utilizzare le immagini per costruire business model è quello della blockchain, che tra il 2021 e il 2022 ha visto il settore degli NFT esplodere.

C'è un sottile filo rosso che unisce queste due tecnologie e che apre già oggi nuovi scenari: quello del community building. Le AI generative sono AI che generano immagini su richiesta degli utenti. Esse sono inizialmente programmate dando loro "in pasto" immagini pre-esistenti, così da "educarle" attraverso feedback loop dati dalle interazioni con la community, per fornire risultati sempre più soddisfacenti. Gli NFT sono token unici, generati sulla blockchain, che danno determinati diritti sulle immagini

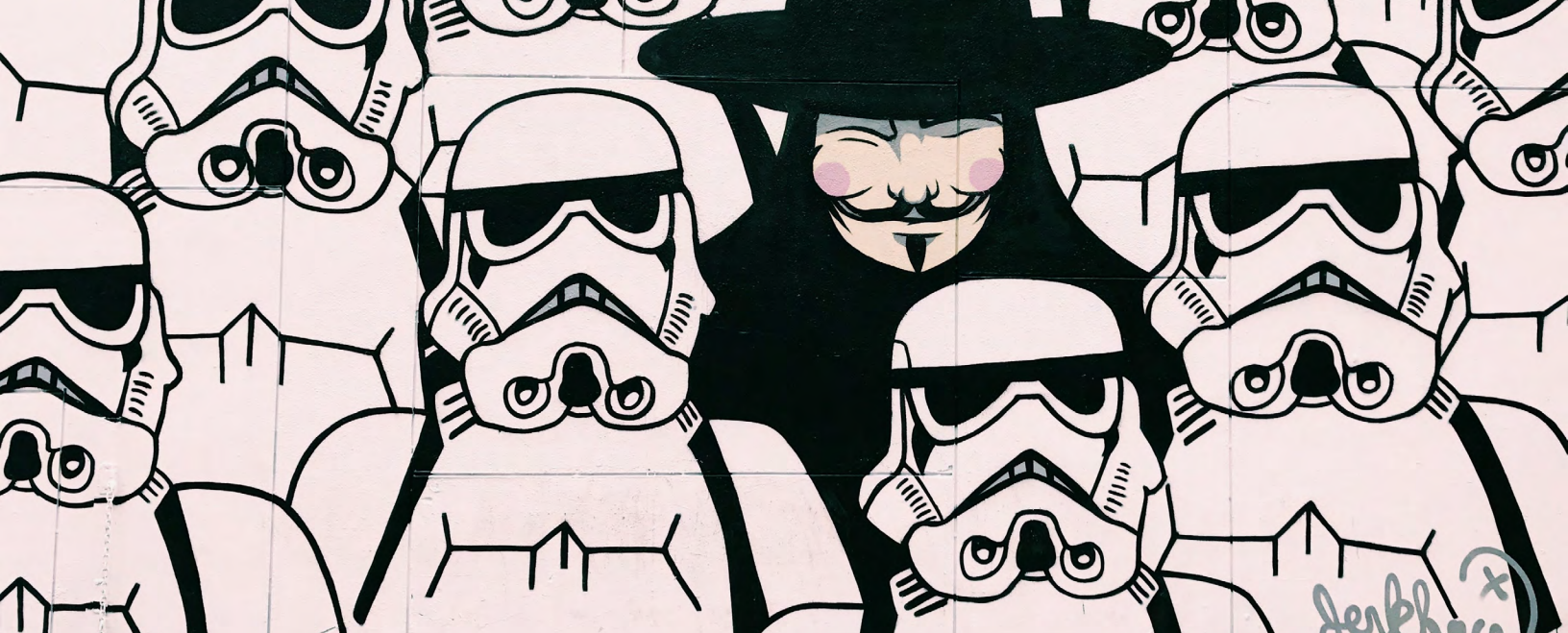
ivi contenute (o cui questi token si riferiscono) e vengono spesso utilizzati a fini di community building: famosi sono i casi di Gucci, Bepple, Cryptopunk e Bored Apes Yacht Club. Sia grazie all'hype di campagne di marketing vincenti che grazie all'asset vero e proprio (l'NFT), queste community sono cresciute esponenzialmente negli ultimi anni.

Abbiamo allora analizzato queste due tecnologie (AI generative e NFT) per comprenderne le potenziali interazioni e astrarre un'architettura flessibile e pronta per l'utilizzo industriale. Per dare a Cesare quel che è di Cesare, abbiamo preso ispirazione da una piattaforma open-source, Botto. Botto emette NFT a partire dalle preferenze della community per elaborare un progetto industriale di successo, in quanto l'utilizzo congiunto di blockchain e AI è un campo di sviluppo particolarmente promettente.

Per raccontarvi questo caso d'uso, ipotizziamo che la ditta Luxury Fashion S.p.A. voglia costruire una piattaforma che utilizzi queste due tecnologie per raggiungere alcuni obiettivi commerciali: community building, appartenenza al brand e maggiori ricavi per cliente. Possiamo immaginare una piattaforma che funziona come segue per raggiungere gli obiettivi di Luxury Fashion:

Tokenizzazione delle partecipazioni

Sulla blockchain creiamo una serie di token che garantiscono l'accesso a una piattaforma esclusiva e proprietaria del brand. I token danno una serie di diritti all'interno di Luxury Fashion, fra cui accesso a contenuti visuali esclusivi, connessione con altri membri della community e interazione con l'AI sviluppata dal marchio. I membri del club possono trasferire a terzi i loro token, come si usa sulla blockchain, qualora non



siano più interessati a queste funzioni. La trasferibilità dei token ci dà informazioni molto importanti sull'andamento del progetto; per esempio, il trasferimento dei token di partecipazione alla piattaforma può essere utilizzato come dato proxy per calcolare il churn rate di Luxury Fashion.

AI Generativa

Luxury Fashion è un brand importante, che si distingue dagli altri e ha una storia di successo alle spalle. Possiede un ampio database di bozzetti, cartamodelli, cad 3d dei vestiti, foto, pubblicità e video. Luxury Fashion vuole che le immagini prodotte dall'AI siano quanto più possibile rispondenti alla sua brand identity. Per questo, "allena" la AI sul suo database proprietario. Questa, dopo un

primo periodo di alfa testing, inizia a creare nuove immagini che sono in linea con Luxury Fashion e a proporle ai membri della community.

Feedback loop

Luxury Fashion AI inizia a proporre alcuni nuovi bozzetti: alcuni sono di ottima qualità, altri un po' strani. I membri della community iniziano a votare le varie immagini e la AI organizza una gerarchia delle preferenze della community stessa per produrre immagini sempre più rispondenti al gusto della community Fashion Luxury. Ma il brand ha capito che possiamo ottenere di più da queste interazioni, e chiede alla AI di indicare, mese dopo mese, quali siano gli aspetti che secondo lei accomunano le preferenze della community. Il brand potrebbe scoprire, a esempio,

che i membri più giovani della community amano il colore rosso più del colore giallo, o che gli utenti tra i 35 e i 50 anni residenti in Spagna mediamente non apprezzano vestiti monocromatici e così via.

Feedback Loop 2

Dopo le prime interazioni, Fashion Luxury ha diverse alternative: può utilizzare la piattaforma per continuare a fare scouting delle preferenze in maniera libera / casuale; oppure, provare a spingere la piattaforma a "testare" le nuove collezioni o indirizzarla verso un certo tipo di gusto, per migliorare la propria campagna di marketing. Potrebbe anche inserire una nuova "collezione" sulla piattaforma, che al posto che immagini produce (per esempio) brevi poemi o haiku giapponesi. Una mossa per capire quali

siano le parole che suonano meglio ai propri consumatori. Le possibilità date dal data mining sono molto ampie.

NFT

Le immagini che piacciono di più alla community, mese dopo mese, sono trasformate in NFT che possono avere diversi scopi: possono essere vendute su un marketplace alla community, possono essere date in premio ai membri più attivi di essa o diventare un vestito Fashion Luxury per la sfilata Autunno 23.

Appartenenza al brand

Nel mondo del lusso, della moda e del design, il brand è un asset estremamente importante: crea un sentimento di appartenenza identitaria nella community e stimola, in ultima analisi, le vendite. Tipicamente il rapporto tra brand e community è top-down: il brand propone i suoi prodotti e la community segue. Nel mondo dei big data questo modello è stato superato e, attraverso le piattaforme, sostituito da uno più efficace. Il sentimento di appartenenza alla comunità aumenta con le interazioni e la loro valorizzazione. Con questa piattaforma i clienti del brand sono direttamente partecipi, alme-



no a livello di AI generativa, al processo creativo. Così, il loro gusto e il loro amore per il brand restituiscono due prodotti: informazioni sulle preferenze di consumo per il brand, e co-creazione per gli utenti. Una strategia win-win.

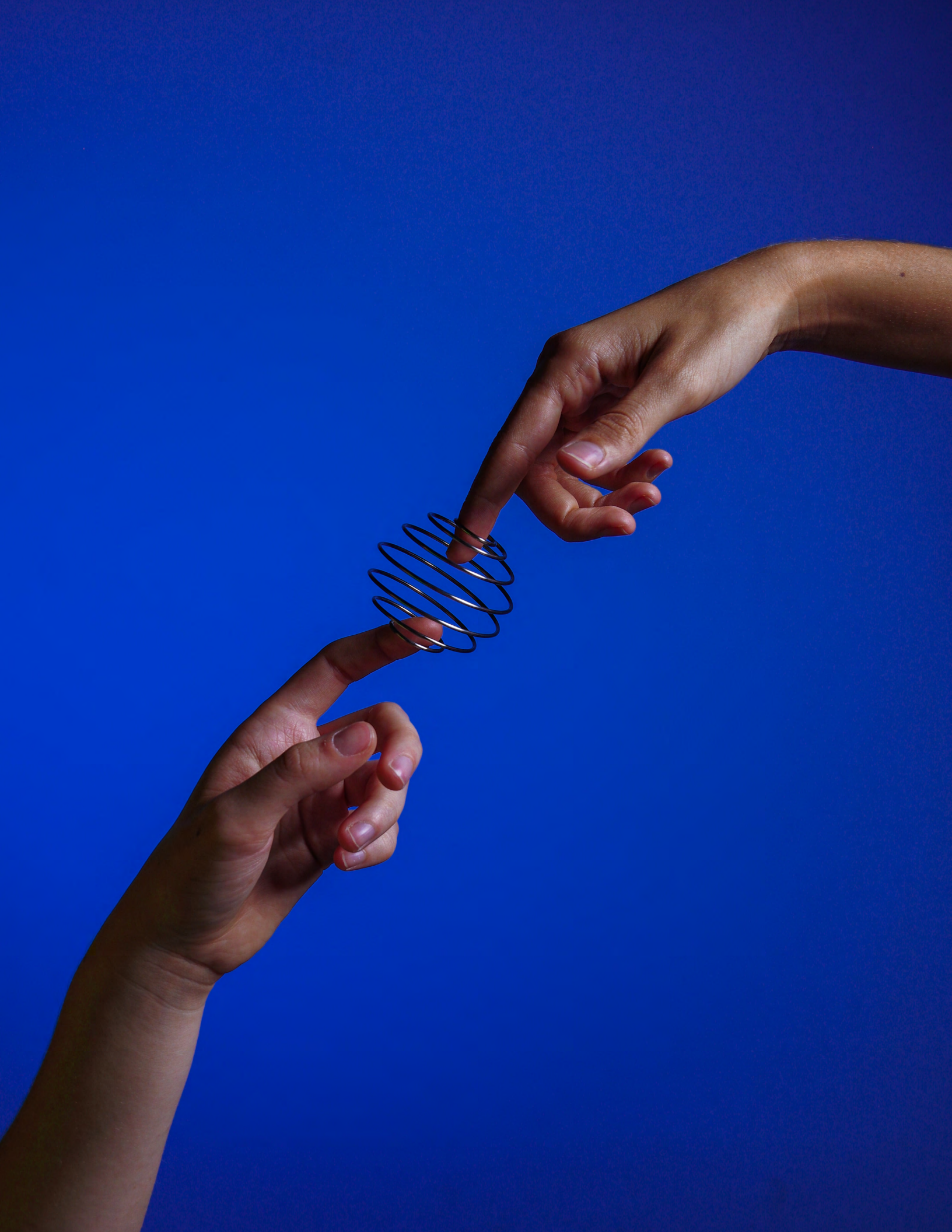
Come possiamo utilizzare questa piattaforma?

Sicuramente l'interazione tra token, AI e community building è estremamente potente nel mondo della moda, del design e del lusso in generale. Dobbiamo però fare dei distinguo sulle modalità di implementazione: se Fashion Luxury fosse un brand high-end, il direttore creativo ha un posto di primo piano nel flusso decisionale. Questo farebbe sì che le immagini generate potrebbero non essere vestiti o accessori, ma

opere d'arte digitale per non creare conflittualità tra AI e direttore creativo. Se Fashion Luxury fosse un brand di fast fashion, ci si potrebbe spingere e chiedere all'AI di creare, con la community, la prossima collezione.

Gli stessi ragionamenti potrebbero essere applicati a sistemi anche molto diversi:

- Radio e musica: la community potrebbe aiutare l'AI a comporre tracce di musica elettronica;
- Editoria: la community potrebbe utilizzare l'AI per creare nuovi racconti, saggi o raccolte di poesia;
- Moto & automobili: sia il design dei mezzi di trasporto che le varie customizzazioni potrebbero essere filtrate dal gusto della community e poi portate in produzione.



A photograph of several large, white, cylindrical industrial storage tanks. The tanks are arranged in a row, with some having red horizontal bands. Scaffolding and ladders are visible on top of the tanks. A large, white, stylized number '03' is overlaid in the center of the image.

03

La Blockchain per il settore energy

Uno dei primi settori (oltre alla finanza, ovviamente) in cui si è iniziato a ragionare circa l'applicazione del Web3 e della blockchain in particolare è stato il settore energy. Dal 2017 sono nati molti progetti, tutti esperimenti di applicazione della tecnologia in diversi segmenti del settore. Come spesso capita in questi casi, molti di questi progetti sono risultati solamente costose operazioni di marketing senza alcuna sostanza che,

in fin dei conti, non hanno creato nulla di tangibile. Altri invece, costruiti su basi più solide, hanno fallito nell'industrializzazione del loro prodotto, nonostante i progetti pilota di successo. Questo perché la complessità del settore energy rende difficile per le compagnie essere realmente competitive: le risorse richieste in termini di capitali da investire e lavori legali per essere aderenti alla regolamentazione sono davvero

importanti. Inoltre, la creazione di una nuova infrastruttura basata su blockchain, IoT e AI è all'inizio dello sviluppo, e questo rende ancora più complesso il lavoro richiesto. Questa nuova infrastruttura va sempre più a definirsi, ma anche in questo caso abbiamo un'importante barriera all'ingresso, a causa dell'alta richiesta di capitali e della scarsità di lavoratori con le competenze necessarie. Non ultimo, abbiamo un deficit di

“ SI PREANNUNCIANO DELLE SFI- DE A LIVELLO LEGALE DI NON POCO CONTO ”

regolamentazione, in particolare modo per quanto riguarda blockchain e AI, che sono ancora in fase di sviluppo o implementazione. Si preannunciano delle sfide a livello legale di non poco conto: pensiamo a un sistema complesso, come un network governato e ottimizzato dall'AI, che prende dati da fonti reali (come gli smart meter), li registra su blockchain e va a generare dei token. Questi token rappresentano diritti che spettano a una persona fisica o giuridica e li distribuisce in maniera automatizzata conformemente a quanto prestabilito contrattualmente. Per un sistema del genere, serviranno regole certe, che al momento mancano.

Per quanto riguarda il settore energy, grazie a queste nuove tecnologie siamo nel mez-

zo di una transizione verso un sistema di generazione e distribuzione totalmente digitalizzato, efficiente ed economicamente ottimizzato. Attualmente, la narrazione che va per la maggiore circa l'applicazione della tecnologia blockchain nel settore energy riguarda la gestione delle identità digitali dei dispositivi IoT, che permetterebbe lo scambio di dati in un ambiente trustless e sicuro, rispettando la privacy sia del device che dell'utente. Questa narrazione è sicuramente vera, ma non è l'unica come molti sostengono: queste persone non tengono conto del continuo sviluppo della tecnologia sottostante e soprattutto dell'integrazione tra blockchain, IoT e AI.

A nostro avviso esistono almeno tre use case importanti da evidenziare:

- **Trading di energia:** creazione di microreti, Comunità Energetiche e semplificazione gestionale di sistemi complessi;
- **Miglioramento gestionale della rete principale;**
- **Certificati di Energia Rinnovabile.**

Il settore dell'energia rinnovabile sta acquisendo sempre maggior risalto nel panorama internazionale, poiché in tutto il mondo i governi incentivano quella che viene chiamata "Green Economy", per arginare il problema del climate change. L'espansione del mercato delle energie rinnovabili è affiancata dalla creazione delle cosiddette microreti, cioè generatori di energia locali che sono anche consumatori della stessa

La blockchain è la tecnologia che, congiuntamente a IoT ed AI, si presta meglio come base per la transizione ad una nuova infrastruttura per il mercato dell'energia.

(i cosiddetti prosumer, crasi tra i termini inglesi consumer e producer) e vendono gli eccessi generati in un'area specifica (come può essere il proprio quartiere, un complesso industriale, il molo in un porto marittimo) oppure direttamente alla rete principale. Le microreti favoriscono e semplificano il processo di creazione delle Comunità Energetiche, che vengono definite come associazioni di persone, imprese, attività commerciali o pubbliche amministrazioni che decidono di associarsi per la produzione, lo scambio e il consumo di energia elettrica da fonti rinnovabili su scala locale. Da questa definizione si capisce come il mercato energetico stia tendendo sempre di più alla decentralizzazione, sia nei processi che nelle funzionalità. Il coordinamento tra le parti sta progressivamente diventando di fondamentale

importanza perché tutto funzioni al meglio.

Ovviamente la migliore infrastruttura tecnologica attualmente disponibile per il coordinamento tra le parti è, neanche a dirlo, il Web3. Questo grazie alla sua architettura basata sul coordinamento degli attori in modalità cosiddetta trustless; il suo registro immutabile, sicuro e non corruttibile; ma anche alle possibilità offerte dall'utilizzo degli smart contract. Così, la blockchain è la tecnologia che, congiuntamente a IoT ed AI, si presta meglio come base per la transizione ad una nuova infrastruttura per il mercato dell'energia.

La trasformazione del trading di energia è una delle conseguenze dirette di questa nuova infrastruttura. Se guardiamo nello specifico la situazione attuale del settore

energetico, troviamo una serie di frizioni ed inefficienze dovute principalmente ad una mancanza di dati in tempo reale sull'energia generata nelle centrali, sulla sua distribuzione ed eventuale stoccaggio. Il risultato di queste frizioni ed inefficienze è uno spreco di parte di essa. Questo perché i consumatori non possono fare affidamento su un mercato che funziona in tempo reale (al contrario di ciò che avviene, ad esempio, per la borsa valori, in cui domanda e offerta sono incrociate in tempo reale). Risulta chiaro quindi come la digitalizzazione dell'intero processo di generazione, distribuzione e vendita dell'energia possa portare benefici a questo mercato.

Analizziamo ora le microreti, e la loro efficacia nella creazione delle Comunità Energetiche. Questo è un ottimo esempio di come la digitalizzazione dei processi, congiuntamente all'utilizzo delle più recenti tecnologie, possa apportare effettivi benefici all'intero mercato. Partiamo

da un caso pilota di qualche anno fa: l'implementazione della microrete nell'Innovation Dock del porto di Rotterdam, il più grande porto commerciale al mondo, e la creazione dell'applicazione relativa Blockchain & AI-based, per il trading di energia.

Questo progetto pilota, denominato "Distro" e condotto da S&P Global Pattel insieme a BlockLab nel 2020, ha visto la creazione di una comunità energetica nell'innovation dock del porto di Rotterdam attraverso l'implementazione di una microrete. Sono stati installati pannelli fotovoltaici sui tetti dei capannoni per generare energia, e sono state installate diverse batterie per lo stoccaggio degli eccessi. Parallelamente è stata sviluppata un'applicazione basata su blockchain, per gestirne la compravendita all'interno della comunità energetica, facendo leva sull'AI e su algoritmi di high-frequency trading, spesso utilizzati nel mercato azionario. Quando un molo necessita di più energia, il sistema automaticamente indirizza la quanti-



tà necessaria, comprandola sul mercato al miglior prezzo possibile e tenendo in considerazione la quantità, la fonte di generazione e la fascia oraria di disponibilità. Tutta questa complessità è possibile grazie ad un feed di dati in tempo reale che viene trasmesso dagli smart meter installati nella microrete, e certificato attraverso la blockchain. A partire da questi dati viene strutturato un order book e un algorit-

mo di trading ottimizzato dall'AI incrocia domanda e offerta nel miglior modo possibile. La blockchain è utilizzata come layer transazionale e per il settlement delle operazioni, scrivendo tutte le transazioni finalizzate all'interno del suo registro distribuito e facendo leva sulla tokenizzazione degli asset per semplificare la gestione degli scambi. Da un punto di vista economico, Distro è stato un succes-

so: gli utenti hanno pagato in media l'11% in meno rispetto ai prezzi di mercato e i produttori hanno visto crescere i loro ritorni del 14%.

Come già detto, il complesso sistema creato per Distro è stato reso possibile dall'implementazione di una nuova infrastruttura, che utilizza le tecnologie più recenti: questa ha permesso una migliore gestione dei dati, un mercato senza frizioni e più efficiente, oltre a una maggiore flessibilità nella generazione e distribuzione dell'energia. Si è giunti così a impattare su tutte le componenti fondamentali del mercato energetico. Il Web3 ha portato diversi benefici:

- Costi di transazione ridotti, e creazione di uno storico certificato di tutto ciò che è accaduto nella rete;
- Accesso al marketplace migliorato, processo di KYC migliorato e semplificato; un miglior coordinamento tra gli attori;
- Peer-to-peer trading in un ambiente sicuro, con maggiore trasparenza per gli stakeholder.

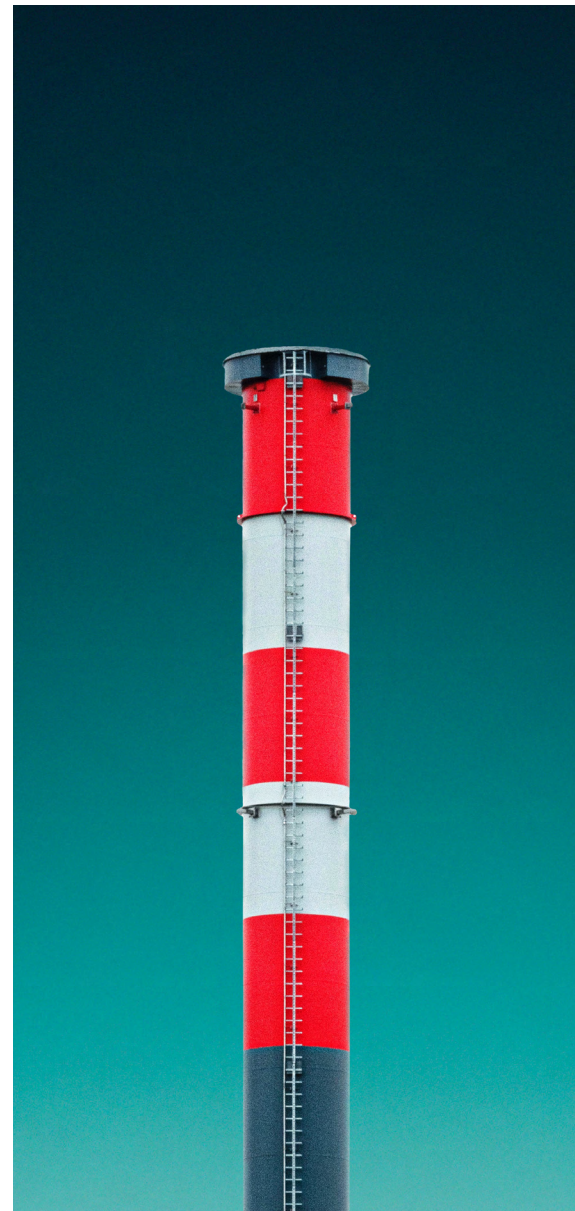
Questo senza compromettere la privacy dei partecipanti;

- Migliore compliance regolamentare grazie al feed di dati in tempo reale e a una gestione migliorata di enormi quantità di dati.

A completamento di questa nuova infrastruttura, l'applicazione del Web3 può risolvere un ulteriore problematica tipica della green economy: i Certificati di Energia Rinnovabile (REC). Un REC equivale a 1MWh di energia generata attraverso fonti a zero emissioni (pannelli solari, centrali idroelettriche, turbine eoliche ecc...) e può essere acquistato dalle aziende per compensare le emissioni di carbonio, aggiungendoli ai loro bilanci ESG. Il mercato delle REC è internazionale: chiunque nel mondo può generare un certificato che verrà poi venduto dall'altra parte del globo. Il problema che si crea è chiaro a tutti: l'elettricità generata per il REC potrebbe non essere stata generata da fonti rinnovabili, ma comunque il REC rimane nel bilancio di sostenibilità dell'azienda che lo ha acquistato, senza avere un reale

impatto nel mondo esterno. Il Web3 può risolvere questa problematica abbastanza facilmente: migliorando in maniera sostanziale il tracciamento della creazione e distribuzione dell'energia, la tokenizzazione può aiutare a conoscere con certezza la fonte di generazione dell'energia sottostante il REC.

Attraverso il feed di dati in tempo reale, alla creazione di asset digitali che utilizzano questi dati come base e aggiungendo un livello ul-



teriore di AI per migliorare i processi in corso d'opera attraverso un algoritmo di machine learning che migliora costantemente, è possibile creare applicazioni Web3 che semplificano e standardizzano le modalità di gestione dell'energia. Questo è un punto cruciale, poiché non esistono standard di processo nella certificazione delle energie rinnovabili.

Prendiamo come esempio un parco fotovoltaico o agrovoltaiico: in Italia richiede una quantità enorme di documentazione per l'approvazione. Inoltre, la gestione e la manutenzione richiedono una grande mole di documentazione. Tutti questi documenti, estremamente eterogenei fra loro, sono richiesti per legge. Un approc-

cio standardizzato sarebbe reso possibile dall'utilizzo di una piattaforma che copra l'intero processo end-to-end: dalla creazione e messa a terra del progetto per la generazione dell'energia, passando per la distribuzione e stoccaggio della stessa, arrivando fino alla vendita del progetto a parti terze non intervenute inizialmente. Questo faciliterebbe sia le richieste di conformità previste da parte degli investitori/produttori, sia i controlli necessari da parte delle autorità garanti, poiché tutti gli step necessari sarebbero portati avanti direttamente in piattaforma, con il controllo preventivo di tutte le parti in causa.

Un processo standardizzato di questo tipo potrebbe essere il primo passo per un'a-

dozione massiva delle microreti, del trading di energia peer-to-peer e delle comunità energetiche. Un processo reso possibile dai benefici portati da un processo interamente digitalizzato. Da una parte le autorità di controllo potranno interfacciarsi con una singola fonte di informazioni affidabile, non corruttibile, trasparente e facilmente accessibile; dall'altra gli investitori, i consumatori e le compagnie di distribuzione di energia potranno beneficiarne economicamente, tagliando i costi di setup e gestione e migliorando il trading di energia attraverso mercati altamente efficienti ed automatizzati.







04

Tour esplorativo del testo approvato del MiCa

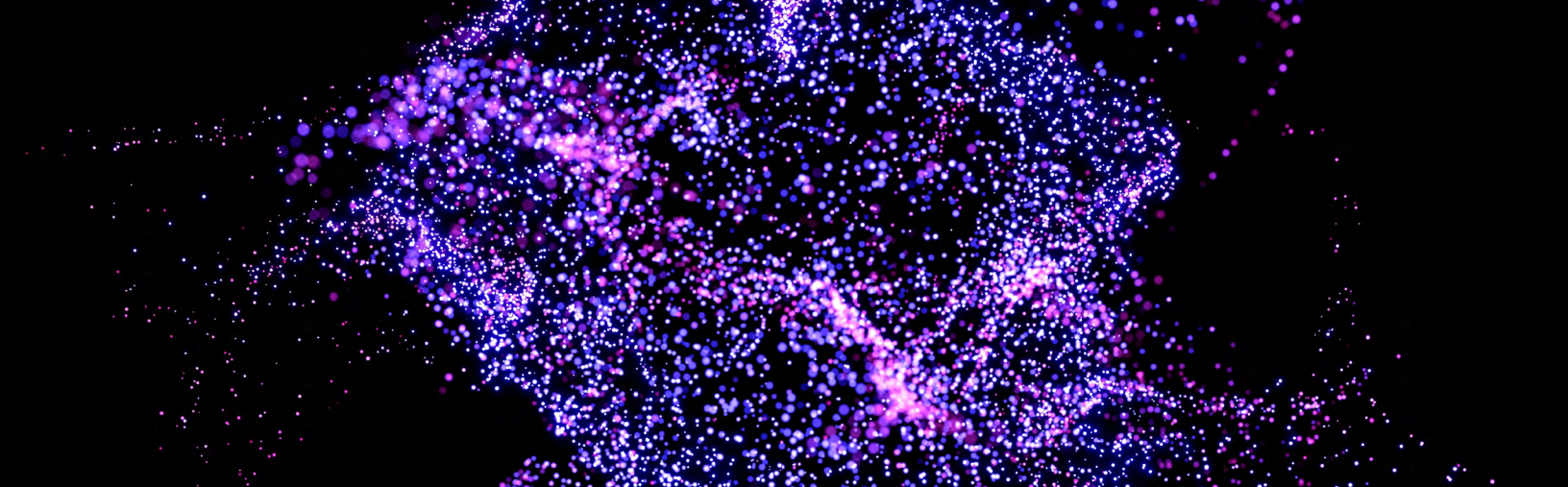


A cura di Raffaella Aghemo

Giugno si prospetta un mese molto intenso da un punto di vista di produzione normativa, essendo previste le approvazioni definitive di importanti regolamenti europei in materia di crypto asset e di intelligenza artificiale.

Proprio il 20 aprile scorso, con 517 voti a favore, 38 contrari, e 18 astensioni, il Parlamento Europeo ha adottato quello che viene comunemente chiamato il MiCA, acronimo di Markets in

Crypto Assets Regulation, ovvero il regolamento sui mercati delle criptovalute, che verrà pubblicato in Gazzetta Ufficiale entro la fine di giugno 2023 ed entrerà in vigore a luglio 2023. Il fine di questa normativa è «garantire che la legislazione dell'Unione in materia di servizi finanziari sia adatta all'era digitale, e contribuisca a un'economia pronta per il futuro che lavora per le persone, anche consentendo l'uso di tecnologie



innovative.»

Si legge infatti: «I crypto-asset sono una delle principali applicazioni DLT. I crypto-asset sono rappresentazioni digitali di valore o diritti che hanno il potenziale per portare vantaggi significativi sia ai partecipanti al mercato che ai detentori al dettaglio di crypto-asset... Semplificando i processi di raccolta di capitali e rafforzando la concorrenza, le offerte di crypto-asset possono consentire un modo di finanziamento innovativo e inclusivo, anche per le piccole e medie imprese (PMI). Se utilizzati come mezzo di pagamento, i token di pagamento possono presentare opportunità in termini di pagamenti più economici, rapidi ed efficienti.»

Al punto 8 si specifica anche quanto segue: «Qualsiasi legislazione adottata nel settore delle crypto-attività dovrebbe essere specifica, a prova di futuro ed essere in grado di tenere il passo con l'innovazione e gli sviluppi tecnologici ed essere fondata su un incentive-based approach. "Crypto-asset" e "tecnologia di registro distribuito" dovrebbero pertanto essere definiti nel modo più ampio possibile per catturare tutti i tipi di crypto-attività che attualmente non rientrano nell'ambito di applicazione della legislazione dell'Unione sui servizi finanziari. Tale legislazione dovrebbe, inoltre, contribuire all'obiettivo della lotta al riciclaggio di denaro e al finanziamento del terrorismo. Per questo motivo, le entità che offrono servizi nell'ambito di applicazione del

presente regolamento, saranno tenute a seguire le norme in materia di antiriciclaggio applicabili nell'UE, che integrano gli standard internazionali.»

Categorie di crypto-asset

Il MiCA, che va a modificare la direttiva (UE) 2019/1937, intanto categorizza i cryptoasset, non precedentemente regolamentati dalle legislazioni finanziarie, suddividendoli in tre sottocategorie:

- **Electronic Money / E-Money Tokens (EMT)**, le cui caratteristiche consistono nel poter fungere da strumenti di pagamento, e la cui stabilità si ottiene ancorandoli alla valuta di un Paese;
- **Asset-Referenced Tokens (ART)**, che pur non essendo monete elettroniche possono mantenere un valore stabile, ricorrendo a combinazione di fattori, quali altri valori o diritti o valute ufficiali di un Paese;
- **All other crypto-assets**, fra i quali rientrerebbero i cosiddetti utility tokens, che consentono ad un soggetto emittente di accedere ad un bene o servizio, tokens di tipo fungible.

L'Art. 1 comincia con lo stabilire dei criteri alla base proprio della presente normativa, rivolgendosi espressamente ai cosiddetti **CASP**, ovvero **Crypto Asset Service Provider** (*persona giuridica o altra impresa la cui attività, che consiste nella fornitura di uno o più servizi di crypto-asset ai clienti su base professionale, deve essere autorizzata*). Fra di essi rientrano:

- Requisiti di trasparenza e divulgazione per l'emissione, l'offerta al pubblico e l'ammissione alla negoziazione di crypto-attività su una piattaforma di trading crypto;
- L'autorizzazione e la supervisione dei fornitori di servizi di crypto-asset, emittenti di asset-reference token ed emittenti di token di moneta elettronica;
- Il funzionamento, l'organizzazione e la governance degli emittenti di token con riferimento ad asset, emittenti di token di moneta elettronica e fornitori di servizi di crypto-asset;
- protezione dei detentori di crypto-asset nell'emissione, nell'offerta al pubblico e nell'ammissione alle negoziazioni;
- protezione dei clienti dei fornitori di servizi di crypto-attività;
- Misure per prevenire l'abuso di informazioni privilegiate, la divulgazione illecita di informazioni privilegiate e la manipolazione del mercato relativa alle crypto-attività, al fine di garantire l'integrità dei mercati delle crypto-attività.

A chi si rivolge

L'Art. 2, relativo espressamente allo **scopo** della presente regolazione, dichiara quanto

segue:

«Il presente regolamento si applica alle persone fisiche e giuridiche e alle altre imprese impegnate nell'emissione, nell'offerta al pubblico e nell'ammissione alla negoziazione di crypto-attività o che forniscono servizi relativi alle crypto-attività nell'Unione.

Il presente regolamento non si applica ai seguenti soggetti:

- persone che forniscono servizi di crypto-valute esclusivamente per le loro società madri, per le loro controllate o per altre controllate delle loro società madri;
- un curatore o un amministratore che agisce nel corso di una procedura concorsuale, salvo ai fini dell'articolo 42 (n.d.r. Piano di Riscatto: Gli emittenti di asset-referenced token redigono e mantengono un piano operativo a sostegno di un rimborso ordinato di ciascun asset-referenced token da attuare su decisione dell'autorità competente qualora l'emittente non sia in grado o sia probabile che non sia in grado di adempiere ai propri obblighi, anche in caso di insolvenza o risoluzione);
- la Banca centrale europea, le banche centrali nazionali degli Stati membri quando agiscono in qualità di autorità monetarie o altre autorità pubbliche degli Stati membri;
- la Banca europea per gli investimenti, comprese le sue controllate;
- il Fondo europeo di stabilità finanziaria e il Meccanismo europeo di stabilità;
- organizzazioni internazionali pubbliche.»

Il presente regolamento non si applica ai **crypto-asset unici e non fungibili (NFT)**.



L'Art. 3 dà un elenco di **definizioni**, tra le quali vorrei segnalare quella relativa ai cosiddetti ART, sopra menzionati, intesi quali: *«un tipo di cripto-asset che non è un token di moneta elettronica e che pretende di mantenere un valore stabile facendo riferimento a qualsiasi altro valore o diritto o una combinazione di questi, incluse una o più valute ufficiali»*.

L'Art. 4 fornisce i requisiti per le offerte al pubblico, richiedendo obblighi quali:

- redazione, notifica e pubblicazione di un white paper (Art. 8);
- redazione e pubblicazione di comunicazioni di marketing;
- diritto di recesso (Art.12);
- requisiti di salvaguardia, ove applicabili.

IL Titolo III è dedicato proprio ai cosiddetti ART - Asset-referenced tokens e al Capitolo 1 si stabiliscono i requisiti di autorizzazione di

offerte di ART al pubblico e di loro ammissione a piattaforme di trading: «Le autorità competenti che ricevono una domanda di autorizzazione di cui all'articolo 16, entro 25 giorni lavorativi dal ricevimento di tale domanda, valutano se tale domanda, compreso il libro bianco sulle cripto-attività ... comprenda tutte le informazioni richieste. Essi comunicano immediatamente all'emittente richiedente se nella domanda, compreso il white paper sulle cripto-asset, mancano le informazioni richieste. Se la domanda, compreso il white paper sulle cripto-asset, non è completa, stabiliscono un termine entro il quale l'emittente richiedente deve fornire le eventuali informazioni mancanti.» L'Art.23 ribadisce il concetto con un generico ma decisivo "Obbligo di agire in modo onesto, equo e professionale nel migliore interesse dei detentori di ART". Come se questo non fosse sufficiente, l'Art. 31, stabilisce la predisposizione di Fondi propri, pari ad almeno 350.000 euro o al 2% delle attività di riserva, cui si aggiunge, nell'art. successivo,

il 32, l'obbligo di costituzione e di mantenimento di una "asset reserve", la quale servirà a sostenere un diritto di rimborso obbligatorio che gli emittenti di ART dovranno concedere ai detentori dei tokens.

Il Titolo IV, invece, si occupa degli EMT - Electronic money tokens, i cui requisiti non differiscono di molto da quelli richiesti per gli ART:

- possono essere emessi solo da istituti di moneta elettronica (IMEL) regolamentati da istituti di credito. C'è un obbligo informativo verso le autorità competenti, consistente solo del white paper sui token di moneta elettronica emessi.
- gli emittitori di EMT devono inoltre rispettare rigorosi obblighi di rimborso, disporre di adeguati "fondi propri" (2% dell'offerta) e soddisfare requisiti di gestione delle riserve analoghi a quelli degli emittenti di ART.
- L'EMT può essere offerto solo da istituti di credito e istituti di moneta elettronica autorizzati ai sensi delle leggi dell'Unione Europea. Qualora, ex Art. 50, siano di significativo valore, saranno anche sotto la vigilanza dell'EBA, l'Autorità bancaria europea.

Requisiti di significatività, richiamanti l'Art. 39, relativo agli ART, sono:

- il numero di titolari di token con riferimento all'attività sia superiore a 10 milioni;
- il valore dei token con riferimento all'attività emessi, se del caso, la loro capitalizzazione di mercato o l'entità della riserva di attività dell'emittente del token con riferimento all'attività, sia superiore a 5 miliardi

di euro;

- il numero e il valore delle transazioni in tali token con riferimento all'attività sia superiore a 2.500.000 transazioni e a 500 milioni di euro, rispettivamente al giorno.

CASP – Crypto Asset Service Provider

Il Titolo V si occupa dei cosiddetti CASP, i cui requisiti si rifanno alla normativa MiFID - Markets in Financial Instruments. Questa norma permette tempi e modalità più rapide oltre che semplificate, ma senza fare nessuno sconto sui necessari caratteri di governance (Art.61), di attenzione, di controllo (Obligation to act honestly, fairly and professionally in the best interest of clients and information to clients, ex Art. 59) e di tutela del patrimonio, ottenibile attraverso anche una costante obbligatoria strategia di cybersicurezza. Quest'ultima è a garanzia del buon funzionamento della piattaforma di trading. Qualora i requisiti non vengano rispettati è possibile applicare la revoca dell'autorizzazione, come si evince dall'Art.56. Anche qui i requisiti di significatività, ex Art. 75a varrebbero per almeno 15 milioni di utenti attivi, in media, in un anno solare nell'Unione Europea. La media è calcolata come quella del numero giornaliero di utenti attivi durante l'anno solare precedente, soglia che farebbe scattare la notifica alla propria Autorità competente entro due mesi. Conseguentemente, la segnalazione arriverebbe all'ESMA, nell'ottica di una costante collaborazione tra le varie Autorità regolatorie (compresa l'EBA), ex Art. 83.

Conclusione

126 Articoli, sei Appendici, 380 pagine sembrerebbero riassumere quanto è stato previsto, pensato, elaborato e stigmatizzato a tutela dei singoli investitori e di un mercato in espansione. Ciò rischia però di suonare già un po' datato, e non in linea con i progressi tecnologici in essere: tant'è che si è preferito escludere dalla presente normazione (volutamente o meno) gli NFT, soggetti alle linee guida dell'Autorità europea degli strumenti finanziari e dei mercati (ESMA), così come i DeFi, in quanto soggetti alle linee guida dell'Autorità bancaria europea (EBA).

Nota invece che sembra gettare un ponte verso il futuro, è il richiamo alla sostenibilità, dal momento in cui i fornitori di servizi di crypto-attività dovranno rendere noto l'impatto ambientale dei crypto-asset che offrono.

In ultimo, il MiCA potrebbe anche applicarsi al fenomeno emergente delle DAO, sebbene l'UE abbia chiarito che le attività e i servizi completamente decentralizzati siano al di fuori dell'ambito di applicazione del regolamento.

Riproduzione Riservata
Avv. Raffaella Aghemo





Green new deal e blockchain



Climate Change, Green New Deal ed ESG sono tra le parole più ricercate su Google negli ultimi anni, a dimostrazione dell'attenzione crescente ad uno dei temi centrali del nostro tempo: come fare convivere sviluppo economico e tutela dell'ambiente. A partire dagli anni '70-80, scienziati ed esperti del settore hanno sensibilizzato la società civile su questo argomento e la politica, con tutte le sue limitazioni, ha raccolto questa importante sfida con una serie di atti e trattati ad ogni livello.

Gli accordi degli anni '90, come il protocollo di Kyoto, sottoscritto nel 1997 da 192 paesi, si focalizzavano su un sistema di controlli delle emissioni di CO₂; quelli più recenti si concentrano non solo sulla necessità di regolamentare le emissioni di carbonio, ma anche di preservare e migliorare altri aspetti dei nostri ecosistemi (come, ad esempio, la gestione della falda acquifera e biodiversità). Vediamo infatti come l'Unione Europea abbia esteso le finalità del Green New Deal al miglioramento e preservazione degli ecosistemi, piuttosto che focalizzarsi solo sul controllo della CO₂. Proposito espresso chiaramente nell'Action Plan Europeo del 2018 e nelle azioni successive.

Altro pilastro cardine della politica ambientale "moderna" è quello del necessario coordinamento delle politiche pubbliche, statali e/o regionali con le azioni dei privati a livello industriale, come si evince chiaramente da tutti i nuovi obblighi e impegni che le aziende dovranno assumere entro il 2025 nel contesto della normativa ESG. Come sempre, nel contesto delle innovazioni dei modelli industriali ci saranno imprese che "subiranno" questo tipo di processo come un costo. Altre invece sapranno trasformarsi e adattarsi a queste nuove esigenze sociali, cogliendo il movimento green come una opportunità di mercato.

Il mercato ESG

La strada migliore per capire le esigenze di questo nuovo mercato è di prendere le mosse dal sistema inaugurato con il protocollo di Kyoto del '97, per capire i bisogni dell'industria e metterla in condizione di sfruttare questa nuova opportunità anche alla luce delle tecnologie oggi disponibili, ben più potenti di quelle che si utilizzavano quasi 30 anni fa.

Il sistema introdotto dal Pro-

TOCOLLO di Kyoto è stato quello del "cap and trade": ogni nazione riceve una certa quantità di emissioni di CO₂ annue in linea con gli obiettivi di riduzione calendarizzati; alle industrie inquinanti di ogni stato vengono assegnati massimali di emissioni di CO₂, che possono essere compensati con l'acquisto sul mercato di certificati CO₂. Sebbene il sistema europeo Carbon Emission Trading (CET), il più importante schema internazionale per il controllo dei gas serra, si sia rivelato un buono strumento per controllare e gestire le emissioni, sono emerse molte carenze legate alla scarsa trasparenza sulle informazioni relative ai progetti emittenti certificati CO₂ e a numerosi casi di corruzione.

La struttura di mercato per le quote di carbonio più importante è la European Union Emission Trading Scheme, fondata nel 2005. Questo sistema stabilisce dei limiti assoluti di gas serra, nei quali i diritti di emissione vengono emessi sotto forma di permessi commerciabili, gli European Union Allowances (EUAs). Queste quote sono espresse in tonnellate di CO₂, oppure nell'equivalente



“Assigned Amount Unit” di anidride carbonica stabilito nel Protocollo di Kyoto. Accanto alla piattaforma ETS, relativa al mercato “obbligatorio” della CO₂, vediamo anche altre piattaforme, meno regolamentate, per il mercato “volontario” delle quote CO₂. Esse si rivolgono alle aziende che non sono tenute a compensare le proprie emissioni, ma che sono soggette alla disciplina ESG e dei bilanci di sostenibilità (che rappresentano un mercato potenziale di circa 50 mld di Euro entro il 2025, per la sola EU). A fianco al mercato volontario delle quote CO₂ vediamo nascere, negli ultimi anni, anche mercati secondari di certificati di altri ecosystem services, come gestione della falda ac-

quifera e biodiversità.

Se il mercato ETS è altamente regolamentato e di difficile accesso, quello volontario di quote CO₂ ed ecosystem services non lo è: fatto dimostrato da scandali come quello che ha colpito Verra, nota società di certificazione e vendita di certificati CO₂ per la compensazione volontaria, molto attiva nel settore.

Ma quali sono i principali problemi che si trovano ad affrontare gli operatori di mercato?

- **Mancano controlli e trasparenza nelle emissioni dei certificati CO₂.**

Nello scandalo Verra il problema principale è stata la mancanza di contro-

lli sulle operazioni green fatte coi fondi raccolti dalla società, che ha ampiamente sovrastimato l'impatto in termini di assorbimento CO₂, creando danno ai suoi clienti che, nei bilanci di sostenibilità, hanno dichiarato il falso.

- **Il prezzo di mercato è calcolato over the counter.**

Il mercato dei crediti CO₂ volontario è quasi tutto “over the counter”: ciò impedisce alle società che vogliono o devono fare compensazione volontaria di poter stimare correttamente le loro strategie di investimento green

- **Si parla solo di CO₂**

Come già sottolineato, una delle limitazioni più

importanti dell'attuale mercato è il concentrarsi sulla sola CO2, mentre l'attività economico/industriale ha un impatto ambientale molto più complesso (si pensi ad esempio a quello sulla falda acquifera)

Molti dei problemi sopra menzionati possono essere oggi risolti grazie all'utilizzo della tecnologia, ed in particolare la blockchain/DLT.

L'impatto della blockchain sul greentech

La tecnologia blockchain è tra le tecnologie più promettenti in ambito greentech, in quanto, strutturalmente, alcune delle lacune viste nei mercati legacy come l'ETS possono essere facilmente colmate. In generale, possiamo definire i network blockchain un registro per transazioni di natura distribuita, dove la veridicità dei dati viene decisa dal consenso di un numero indeterminato di nodi. Questo evita possibili conflitti di interessi dei gestori delle piattaforme e porta i seguenti vantaggi:

- **Sicurezza:** le informazioni aggiunte alla rete hanno tutte data certa;
- **Trasparenza:** tutte le transazioni e le informazioni sono visibili agli utenti;
- **Automazione:** grazie agli smart contract si possono automatizzare i workflow relativi a certificazioni dei dati ed emissione dei certificati
- **Tracciabilità:** è possibile tracciare la "filiera del dato" per validare gli effetti ecosistemici di un'attività;
- **Riservatezza:** le informazioni possono venire crittografate per preservare la privacy

Tutte queste caratteristiche rendono la blockchain la tecnologia adatta a censire operazioni "green", il loro impatto ambientale e l'emissione dei vari certificati afferenti ad ecosystem services. Da un punto di vista funzionale possiamo individuare alcuni flussi che sicuramente verranno migliorati dall'utilizzo di questa tecnologia:

Certificazione

uno dei problemi principali

del mercato degli asset green è la certificazione del workflow a valle del quale i certificati stessi vengono emessi. La soluzione a questa sfida è la pubblicazione dei dati grezzi relativi alle operazioni: ad esempio, quelli della riforestazione, derivanti o da sensori (device IOT o satelliti) o da analisi sul campo (in questo caso si tratta di dichiarazioni che devono venire tracciate). Un'altra criticità è la scissione delle formule di calcolo dai dati grezzi, atta a dare trasparenza alla filiera del dato.

Emissione dei Certificati

una volta pubblicati in chiaro i dati grezzi le formule, quest'ultime si possono tradurre per l'emissione dei certificati in smart contract. Così facendo, si aumenta la fiducia di utenti e stakeholders: la base di calcolo, già certificata sulla blockchain, viene utilizzata con una formula, resa pubblica. Pubblicizzare quest'ultima porta ulteriori vantaggi in termini di trasparenza, affidabilità e scalabilità del prodotto

Mercato secondario

i crediti CO2 nel mercato della compensazione volontaria vengono quasi tutti negoziati

over the counter, ossia privatamente. Si impedisce così la formazione del prezzo e diminuisce la liquidità dell'asset. La trasformazione dei certificati digitali di CO2 o altri ecosystem services in token migliora drasticamente questo aspetto: questo perché la blockchain è un sistema ampiamente testato per essere un mercato primario e secondario di asset digitali.

Finanziarizzazione:

l'utilizzo del token quale supporto digitale per veicolare i certificati CO2 rende molto

più facile la loro finanziarizzazione: questo perché le strutture tipiche disponibili ad operatori di mercato (come il pegno titoli), possono essere facilmente tradotte in smart contract per automatizzare i processi di creazione di garanzie, erogazione di finanziamenti e sviluppo di derivati.

Sulla scorta di quanto detto sopra è possibile allora immaginare una o più piattaforme, completamente digitali, nelle quali diversi soggetti possano operare in sicurezza e autonomia. Ad esempio:

- Gli investitori, potendo fare affidamento sul workflow certificato sulla blockchain, potrebbero investire su un portafoglio di operazioni che generano certificati CO2, piuttosto che acquistare tali certificati;
- Gli operatori del settore green (es. aziende che certificano l'impatto ambientale) parteciperebbero alla piattaforma tramite wallet. Le loro interazioni verrebbero certificate e mappate, per poi sostene-



WizKey vuole fornire agli operatori di mercato e stakeholder uno strumento tecnologicamente adatto e altamente flessibile per affrontare le sfide ambientali del XXI secolo.

re il processo di emissione dei certificati;

- Banche e intermediari potrebbero finanziare questi progetti prendendo in pegno i certificati CO2 e gestendo, in maniera automatica, il processo di finanziamento ed eventuale escussione dei certificati

Conclusioni e casi d'uso

WizKey, attiva nel fintech, ha dedicato buona parte del 2022 in progetti di ricerca sperimentali sull'utilizzo nel mondo del greentech, della sua piattaforma per l'emissione di asset digitali, DeFiNe. DeFiNe è già predisposta per l'emissione di asset digitali relativi a CO2 e altri ecosystem services in quanto:

- La "logistica del dato" è costantemente monitorata, grazie a un sistema

misto di data room sul cloud, per archiviare documenti, dichiarazioni, e analisi sul campo, i cui dati vengono notarizzati (muniti di data certa) sulla blockchain.

- L'emissione degli asset digitali è collegata permanentemente alla data room e utilizza un sistema di smart contract che può essere collegato alla data room stessa, per assicurare la corrispondenza tra ciò che accade nel mondo reale (gli ecosystem services effettivamente implementati) e gli asset digitali emessi sulla blockchain;
- Si possono emettere smart contract finanziari, per veicolare le operazioni di finanziamento, in stile crowdfunding o club deal. Tutto ciò è per costruire strutture finanziarie simili a quelle del mondo legacy, come il pegno su strumenti finanziari

- Ci sarebbe un mercato secondario nativamente presente, per migliorare la liquidità degli asset digitali emessi.

WizKey vuole fornire agli operatori di mercato e stakeholder uno strumento tecnologicamente adatto e altamente flessibile per affrontare le sfide ambientali del XXI secolo. La componente tecnologica è già disponibile e saranno sicuramente gli operatori più lungimiranti ad avvantaggiarsene per primi.



Zero Knowledge Proofs



06

Dimostrazione a conoscenza zero

Le Zero Knowledge proofs sono un metodo per dimostrare la validità di un set di dati senza rivelarli sul network utilizzato: la tecnologia definitiva in materia di privacy. Le prime proposte in ambito scientifico sono emerse in un paper del 1985 di Goldwasser, Micali e Rackoff intitolato "The knowledge complexity of interactive proof systems". Lì, la zero Knowledge proof è definita come: "Metodo grazie al quale un soggetto dimostratore (prover) può dimostrare ad un soggetto verificatore (verifier) che una affermazione è vera, senza rivelare nessun'altra informazione, oltre al fatto che l'affermazione sia vera".

Un famoso esempio che illustra come le zero knowledge proofs funzionano è quello della caverna di Ali Baba.

Tutti conosciamo la storia di Ali Baba: lui insegue i 40 ladroni nella famosa caverna, e dopo averli visti "sparire" uno dopo l'altro nelle profondità della montagna riesce a carpire la parola magica e entrare nella porta segreta,

per poi uscire da uno specifico corridoio della montagna, accessibile solo a chi usa la porta segreta. Ali Baba scrive di questa storia in un manoscritto, omettendo le parole magiche ma lasciando degli indizi in modo da poterle indovinare. Il manoscritto viene quindi recuperato da dei ricercatori alla fine del XX secolo che lo decifrano e con uno scavo archeologico riescono a ritrovare la caverna. Uno dei ricercatori vuole quindi dimostrare di conoscere il segreto senza rivelarlo, e invita un giornale americano a fare le riprese. Per 40 volte il ricercatore entra ed esce da quello speciale corridoio, dimostrando così, logicamente, di conoscere la parola magica senza però rivelarla.

L'esempio citato sopra è parte della classe di dimostrazioni chiamata Interactive Zero-Knowledge Proofs. Questa tipologia di dimostrazioni ha però un uso limitato poiché richiede che le due parti siano disponibili ed interagiscano ripetutamente. Anche se il verifier fosse convinto dell'onestà del prover, la dimostrazione non sarebbe disponibile per una verifica indipendente, in quanto per produrre una nuova dimostrazione ser-

virebbe un nuovo insieme di messaggi tra il prover ed il verifier. Una dimostrazione zero-knowledge interattiva è quindi composta principalmente da tre elementi: testimone, sfida e risposta:

- **Testimone:** Il prover vuole dimostrare la conoscenza di un'informazione nascosta. L'informazione segreta è il "testimone" della dimostrazione e quindi la presunta conoscenza di questa da parte del prover porta a stabilire un insieme di domande alle quali può dare una risposta solo chi è a conoscenza dell'informazione. Perciò il prover inizia il processo di dimostrazione selezionando una domanda scelta in modo casuale, calcolandone la risposta, ed inviandola al verifier.
- **Sfida:** Il verifier seleziona casualmente una domanda dall'insieme e richiede al prover di rispondere a questa.
- **Risposta:** Il prover accetta la domanda, ne calcola la risposta e la invia al verifier. La risposta del prover consente al verifier di controllare se questi ha davvero accesso al testi-



mone. Per assicurarsi che il prover non si muova alla cieca e che non stia ottenendo la risposta per caso, il verifier seleziona più domande da porre. Ripetendo quindi questa interazione molte volte, la probabilità che il prover stia fingendo la sua conoscenza del testimone diminuisce significativamente, fino a quando il verifier non è soddisfatto.

Più in generale un protocollo ZK deve rispettare determinati criteri per poter essere definito tale, ovvero:

- **Completeness** (completezza): se l'input è valido il protocollo restituisce sempre 'vero'; quindi, se l'affermazione in input è vera, e il prover ed il ve-

riifier agiscono in modo onesto, la dimostrazione può essere accettata.

- **Soundness** (solidità): Se l'input non è valido, è teoricamente impossibile ingannare il protocollo zero-knowledge in modo che restituisca 'vero'. Perciò un prover menzognero non potrebbe ingannare un verifier onesto, facendogli credere che un'affermazione non valida sia in realtà valida (ad eccezione di un margine di probabilità molto basso).
- **Zero-knowledge** (conoscenza-zero): Il verifier non scopre nulla circa l'affermazione oltre la sua validità o non validità. In questo modo il verifier non può derivare l'input originale, ovvero il con-

tenuto dell'affermazione, dalla dimostrazione.

Queste caratteristiche base di un sistema ZK sono rispettate anche da dei protocolli non interattivi, che trovano una maggiore possibilità di applicazione pratica. Le due principali categorie sono ZK-SNARKs e ZK-STARKs.

Il nome della prima categoria sta per Zero-Knowledge Succinct Non-Interactive Argument of Knowledge ed un protocollo che rientra in questa categoria ha le seguenti caratteristiche:

- **Zero-knowledge** (Conoscenza-zero): Un verificatore può validare l'integrità di un'affermazione senza avere alcuna altra informazione riguardante



Il prover vuole dimostrare la conoscenza di un'informazione nascosta

l'affermazione stessa.

- **Succint** (Breve, succinto): La dimostrazione a conoscenza-zero è più piccola del testimone e può essere verificata velocemente.
- **Non-Interactive** (Non interattiva): La dimostrazione è non interattiva perché il dimostratore e il verificatore interagiscono solo una volta, al contrario delle dimostrazioni interattive che richiedono più turni di comunicazione.
- **Argument**: La dimostrazione soddisfa il requisito di solidità, perciò barare è estremamente difficile.
- **Knowledge** (Conoscenza): La dimostrazione non può essere costruita senza essere a conoscenza dell'informazione segreta (testi-

mone). È difficile, se non impossibile, per un dimostratore che non possiede il testimone produrre una valida dimostrazione a conoscenza-zero.

Un esempio di protocollo a conoscenza-zero non interattivo viene illustrato in un paper del 1988 intitolato "Non-interactive Zero-Knowledge and its applications" a firma di Blum, Feldman e Micali. Nel paper un dimostratore ed un verificatore possiedono una chiave condivisa. Questa, nelle implementazioni odierne, si riferisce ai parametri pubblici che i due attori accettano di utilizzare nella generazione e nella verifica delle dimostrazioni. La generazione della chiave è un'operazione delicata, a causa della sua importanza per la sicurezza del protocollo: infatti,

se questa finisse nelle mani di un dimostratore disonesto comporterebbe la possibilità di generare dimostrazioni contraffatte.

Per mitigare questo problema si è fatto ricorso alla computazione multi-parte: nello specifico, si è ideato un processo chiamato Trusted Setup Ceremony, dove ogni utente contribuisce a generare la Common Reference String (il segreto). Questo processo richiede però di fidarsi di ogni utente che vi partecipa.

Lo sviluppo degli ZK-STARKs invece, che sta per Zero-Knowledge Scalable Transparent Argument of Knowledge, ha permesso di ovviare al problema della fiducia nel trusted setup, consentendo di abilitare protocolli che funzionano con un non-trusted setup. Questa tipolo-



gia di protocolli è simile agli ZK-SNARKs, tranne che per due caratteristiche:

- **Scalability** (Scalabilità): Gli ZK-STARKs sono più veloci degli ZK-SNARKs nella generazione e verifica delle dimostrazioni quando la dimensione del testimone è più grande. Con le dimostrazioni ZK-STARKs il tempo di dimostrazione e di verifica aumentano solo leggermente all'aumentare delle dimensioni del testimone.
- **Transparency** (Trasparenza): Gli ZK-STARKs fanno uso di generatori pubblici e verificabili di casualità per generare i parametri pubblici per la dimostrazione e la verifica, anziché usare un trusted setup. Per questo motivo sono più trasparenti rispetto agli ZK-SNARKs.

Ma perché questo approfondimento sulle Zero Know-

ledge Proofs? Perché sono la risposta a molti casi d'uso e permettono l'utilizzo delle blockchain pubbliche per qualsiasi tipo di applicativo, per ottenere il meglio da questa tecnologia in termini di certezza, automazione e, da oggi, privacy.

Con l'introduzione di questa tecnologia possiamo infatti abilitare use case molto complessi con la massima sicurezza:

- sistemi decentralizzati di gestione dell'identità;
- piattaforme di tokenizzazione a disposizione dei consumatori;
- KYC/AML on chain;
- certificazione delle informazioni sensibili delle AI direttamente sulla blockchain;
- applicazioni finanziarie con dati sensibili on chain (es. anagrafica del debitore, condizioni del mutuo,

informazioni sull'ipoteca etc.);

- sistemi misti di calcolo on-off chain (c.d. computazione verificabile).

In conclusione, alcune delle tecnologie blockchain che usano la tecnologia Zero-knowledge sono: Mina Protocol, Starknet, zkSync e Polygon Zero. L'avvento dei protocolli zero-knowledge sta portando una nuova ondata di innovazione nel mondo blockchain e non solo. La potenzialità di questa tipologia di protocolli è alta, poiché questi sono in grado di abilitare tecnologie conservando un alto grado di privacy, decentralizzazione dei sistemi di gestione dell'identità e dei pagamenti anonimi on-chain.





07

L'opera d'arte
nell'epoca della sua
(ri)producibilità
tecnica



Il 2021 è sicuramente l'anno in cui il fenomeno NFT ha preso posto nelle cronache, arrivando fino alle prime pagine di giornale. La vendita astronomica dell'opera di Beeple presso la casa d'aste Christie è stato il punto di svolta. Nel giro di poco tempo sono comparsi artisti, collezioni, marketplace, trend e consulenti più o meno esperti del settore, che si sono lanciati in quella che si è rivelata, come sempre accade alle asset class di nuova introduzione sul mercato, una bolla speculativa.

Detto questo, dobbiamo ammettere che l'universo NFT ha portato alla sensibilizzazione sulle possibilità effettive che l'applicazione di questa tecnologia nei diversi settori. Per nominarne alcuni: distribuzione di royalties a seguito del finanziamento di progetti musicali, digital twin a valere su capi di alta moda, skins per gli avatar utilizzati

in videogiochi, oppure all'interno del metaverso.

Protocolli per arte generativa

Tra le molte applicazioni, una in particolare si è dimostrata innovativa e all'avanguardia: i motori per lo sviluppo generativo di arte basati su input di codice. In sostanza, a differenza di un NFT "classico", nell'arte generativa il medium sottostante all'NFT viene creato da un software che utilizza input di codice e di immagine, realizzando l'opera secondo criteri stabiliti.

Gli NFT di arte generativa sono opere create attraverso l'utilizzo di sistemi autonomi come il codice creativo, l'intelligenza artificiale e gli algoritmi. Essi creano le opere in maniera randomica e, solitamente, vengono attivati dallo smart contract, interagendo con gli algoritmi e con altri sistemi autonomi. L'artista può

sempre controllare alcuni elementi come un certo tipo di tratto, alcune varietà di colore e forme, ma può anche impostare determinati criteri di selezione di elementi e del processo di generazione.

Il processo di creazione si inquadra, quindi, come una collaborazione tra uomo e macchina, dove l'artista non può prevedere esattamente il risultato, così come la macchina non può creare "dal nulla". Questo nuovo aspetto collaborativo apre nuove frontiere sia a livello di produzione che dal punto di vista filosofico. Siamo di fronte ad una rinascita artistica e tecnologica.

Arte digitale: le prime creazioni

La prima serie di arte digitale viene considerata l'esibizione Computergraphik di Georg Nees negli anni '60, quando vennero per la prima volta programmati dei computer



**Secondo questo schema l'artista si
trova in un ruolo più di regista che di
diretto autore dell'opera.**

per lavorare su grafiche e sculture.

Dalle prime sperimentazioni, siamo arrivati alla generazione di serie che “si producono” da sole e si scambiano dati con le strutture generative autonome. Secondo questo schema l'artista si trova in un ruolo più di regista che di diretto autore dell'opera. In questo caso, infatti, è facile incorrere in opinioni e riflessioni che mettono in dubbio il ruolo dell'artista, non essendo lui concretamente a realizzare l'opera, bensì un sistema artificiale. Tuttavia, ci basti ricordare che posizioni simili erano emerse anche quando fu inventata la fotografia.

NFT e arte generativa

Vi sono alcune collezioni di NFT auto-generati che meritano esposizione per la genialità e l'intreccio di tecniche diverse. Il prezzo di vendita rimane relativo, in quanto le opere NFT sono spesso create all'interno di un sistema speculativo e sostanzialmente non regolato.

Autoglyphs è una serie di NFT generativi creati da Larva Lab, meglio noto per la creazione della famosissima serie CryptoPunks. In questa serie di arte generativa, le opere sono create da linee di codice

in Solidity, che “girano” sulla blockchain di Ethereum. Una volta implementato il codice sulla blockchain, questo diventa autonomo e non può più essere controllato. Gli Autoglyphs sono algoritmi generativi altamente automatizzati capaci di generare milioni di versioni uniche racchiuse all'interno di un token ERC-721. Solitamente gli NFT sono l'entità digitale che certifica la proprietà sul file media, che è conservato in differenti ambienti di “storage”. Nel caso degli Autoglyphs, l'opera d'arte è all'interno del contratto stesso. Questo diventa verificabile quando si esamina la transazione di creazione di uno degli NFT. Nei

dati della transazione è incluso il pattern generato, che quindi può essere “disegnato” in grafica vettoriale, seguendo le istruzioni di scrittura contenute nei commenti del contratto stesso.

Un altro esempio interessante è la serie Fidenza di Tyler Hobbs. In questo caso l'artista è partito dagli strumenti grafici chiamati flow fields.

I flow fields sono basati su una griglia grafica che va a coprire l'intera immagine. Tramite l'impostazione dei setting sulla risoluzione desiderata, si ottengono delle linee curve armoniose e dalla forma imprevedibile. Successivamente,

vengono utilizzate delle “palette colori probabilistiche” per l'assegnazione di segmenti colorati tra le linee. Allo stesso modo, vengono impostati i criteri per le pennellate e per i tratti. Tutti questi dati vengono attivati dallo smart contract e veicolati nell'algoritmo che crea l'opera al momento del minting richiesto dal compratore.

Sistemi generativi: l'evoluzione continua.

WizKeyha preso a modello queste nuove tecnologie e le sta evolvendo, impiegando

questi strumenti in nuove applicazioni e in diversi settori di business. Come azienda, stiamo sperimentando forme autonome di generazione artistica, utilizzando modelli creati dai codici e, assieme a nostri clienti, creiamo prototipi e studiamo possibili applicazioni. Esse vanno oltre la creazione artistica in sé e, basandosi sullo stesso sistema tecnologico, possono avere degli output maggiormente commerciali e di indagine. Tra questi spiccano lavori basati su matrici per la creazione grafica di capi di abbigliamento: l'inserimento di input da parte degli utenti permette di fornire un prodotto che sod-



I sistemi autonomi di sviluppo possono aiutare a trovare soluzioni complesse partendo da input precisi all'interno di criteri prestabiliti, per arrivare alla computazione dei dati (generazione di output).

disfa i gusti di tutti gli utenti, o quasi: mostrando le loro preferenze rispetto ad un colore, dettaglio o forma, si trova una media fra le loro preferenze. Come viene applicato alla moda, si può usare anche in altri settori, con l'obiettivo di poter interpellare i differenti bacini di utenza e capire le nuove tendenze. Successivamente è possibile utilizzare strumenti come algoritmi o macchine di processo di intelligenza artificiale, per ottenere dei risultati da proporre al mercato e al pubblico.

Per concludere, possiamo affermare che i modelli di creazione artistica autogenerativa rappresentano essenzialmente un punto di partenza: dall'arte potranno espandersi ad altri campi. L'artista imposta dei criteri al processo di creazione dell'opera d'arte; allo stesso modo, gruppi di persone facenti parte di una comunità di consumatori, o anche di spettatori, possono inserire all'interno di questi strumenti i dati necessari ad ottenere risultati

ottimali (non più randomici) secondo le scelte degli utenti. Gli use case possono essere i più svariati: dalla ricerca a fini commerciali fino allo sviluppo di nuove tecniche di chirurgia. Il concetto rimane sempre lo stesso: i sistemi autonomi di sviluppo possono aiutare a trovare soluzioni complesse partendo da input precisi all'interno di criteri prestabiliti, per arrivare alla computazione dei dati (generazione di output).







08

“Cogito ergo sum”: l'identità sovrana autonoma sposa la blockchain

“C'era una volta, tanto tempo fa, un mondo pervaso di tecnologia e innovazione dove i nostri antenati, le persone, vivevano in un immenso regno chiamato Internet.

In questo regno, le persone erano riconosciute attraverso le loro identità digitali, variopinte maschere indossate ogni volta che varcavano le porte di una città virtuale. Queste identità, però, erano spesso sfruttate per guadagno da grandi corporazioni, i

cosiddetti giganti tecnologici, che raccoglievano le loro caratteristiche più specifiche e personali rivendendole per molti denari. Alcuni, i più lestofanti, le usavano addirittura per rubare le identità e influenzare le opinioni politiche. Tale situazione provocò grande indignazione tra la popolazione di Internet.

Uno di loro, un tipo strano, che aveva a cuore il tema dell'identità umana, un giorno addirittura scrisse:

Una delle poche cose, anzi forse la sola ch'io sapessi di certo era questa: che mi chiamavo Mattia Pascal.[...] Non pareva molto, per dir la verità, neanche a me. Ma ignoravo allora che cosa volesse dire il non sapere neppur questo, il non poter più rispondere, cioè, come prima, all'occorrenza: lo mi chiamo Mattia Pascal.

Il fu Mattia Pascal – Luigi Pirandello

Gli abitanti del regno si sen-

“ PENSARE VUOL DIRE ESSERE UNA PERSONA. ”

tivano quindi profondamente violati nella loro privacy, come se elementi del proprio essere fossero stati rubati e divulgati senza il loro consenso. Così, iniziarono a cercare una soluzione, un modo per riappropriarsi del controllo delle proprie identità...”

Vivendo nel tempo delle Intelligenze Artificiali generative, questo è ciò che un'intelligenza artificiale post-umana potrebbe scrivere in un prossimo ipotetico futuro, ripensando ai giorni nostri.

Spindox con la sua divisione specializzata in Intelligenza Artificiale (aHead-Research) ripercorre gli elementi distintivi del precedente racconto (concetto di identità e il controllo di essa da parte degli individui), cercando di fornire una Soluzione. Spindox sta disegnando e im-

plementando soluzioni avanzate per la gestione delle identità digitali sfruttando le potenzialità offerte dalla tecnologia blockchain, al fine di consegnare nuovamente nelle mani delle singole persone il controllo sui loro dati. Spindox ha infatti interesse nel navigare le complessità dell'identità digitale e nel promuovere l'autonomia individuale nella gestione e condivisione delle informazioni personali.

Concetto di identità

L'identità è un concetto unicamente umano. È quell' "io" ineffabile dell'autocoscienza, qualcosa che viene compreso in tutto il mondo da ogni persona che vive in ogni cultura.

Come disse Cartesio, "Cogito ergo sum - penso, quindi sono".

Pensare vuol dire essere una persona, vuol dire avere un nome, quindi essere "qualcuno" nella comunità. Se si è una persona, si ha perciò un'identità. Se si ha un'identità ci si distingue dagli altri o dalle altre persone, perché identificare vuol dire distinguere e non già accomunare.

L'identità umana è un argomento complesso, dibattuto per secoli dai filosofi, che può essere formalizzato attraverso un modello mentale che suddivide l'identità umana in due parti, entrambe necessarie per essere un membro produttivo della società:

- **Identità intrinseca:** è la nostra identità di genere, politica o culturale, ciò che vediamo quando ci guardiamo allo specchio e chi siamo nelle nostre relazioni più strette. È la



forma più vera di identità.

- **Identità estrinseca:** è come gli altri, spesso le istituzioni, ci identificano.

Nella società odierna si aggiunge un nuovo concetto di identità: l'identità digitale.

Identità digitale

“L'identità digitale si riferisce alla rappresentazione virtuale di un individuo. È un insieme di informazioni uniche che identificano una persona o un soggetto all'interno dell'ambiente digitale.”

Molte delle più grandi piattaforme di internet (es., social-media) esistono per aiutare le persone a esprimere

la loro identità intrinseca. Tuttavia, non esiste ancora un buon modo per gestire le nostre identità estrinseche digitalmente, ad esempio le attuali forme di autenticazione/verifica delle identità impongono di fornire l'identità a ogni sito web che visitiamo e il processo varia da un sito all'altro. Si tratta di migliaia e migliaia di siti diversi con cui condividiamo aspetti diversi dei nostri dati personali. Spesso il processo si conclude addirittura con il dover fornire una documentazione cartacea “reale” per verificare la nostra identità online.

Inoltre, la società moderna ha confuso il concetto di identità digitale accostandolo ad elementi di scopo dell'identità, come ad esempio l'accesso a servizi internet o l'appar-

tenere ad una comunità social. Questo è problematico perché suggerisce che una persona possa perdere la sua stessa identità revocando le sue credenziali o anche solo abbandonando un fornitore di servizi.

Riformulando Cartesio: “Penso, ma non sono.”

Self-Sovereign Identity (SSI):

L'Identità Sovrana Autonoma o Self-Sovereign Identity (SSI) si riferisce all'idea che l'identità sia un diritto universale e che gli individui abbiano la proprietà esclusiva della loro identità, così facendo l'individuo acquisisce il pieno controllo sulle modalità di condivisione, tracciabilità e utilizzo

dei propri dati personali. Anziché limitarsi a chiedere che gli individui siano al centro del processo di identità, l'identità auto-sovrana richiede che gli individui siano i padroni della propria identità.

Il concetto di identità auto-sovrana è un modo per rendere l'ecosistema digitale più inclusivo e paritario. Il concetto di SSI esprime che per la prima volta saremo i custodi dei nostri dati personali.

Questo è il cuore dell'identità auto-sovrana, un termine diffusosi già negli anni '10, quando lo sviluppatore Devon Loffredo scrisse di "Sovereign Source Authority" nel Febbraio 2012. L'Unione Europea nel 2020 ha iniziato a sviluppare un quadro di riferimento per l'SSI, noto come European Self-Sovereign Identity Framework (ESSIF). L'ESSIF mira a specificare un protocollo di Identità Sovrana Autonoma (SSI), definendo come gli utenti possano creare e controllare la propria identità attraverso i confini degli stati senza doversi affidare ad autorità centralizzate.

I primi tentativi di raggiungere questo obiettivo hanno

abbandonato il paradigma di gestione centralizzato dell'identità, giungendo ad un paradigma composto da entità federate interoperabili con controllo centralizzato che rispettano al contempo un certo livello di consenso dell'utente sulle modalità di condivisione dell'identità (e con chi). Ciò è stato un passo importante verso il vero controllo dell'identità da parte dell'utente, ma solo un passo. Per fare il passo successivo occorre l'autonomia dell'utente.

Blockchain come soluzione per implementare la SSI?

La richiesta di controllo e autonomia da parte dell'individuo nella gestione della propria identità e dei dati connessi diventa pertanto un elemento cruciale. La tecnologia decentralizzata di Blockchain presenta un cambiamento infrastrutturale che sta trasformando e trasformerà notevolmente il mondo digitale ("il regno di internet").

In particolare, è possibile sfruttare le potenzialità della tecnologia blockchain per rispondere alle esigenze della

Self Sovereign Identity (SSI). La blockchain fornisce un framework tecnologico ideale per realizzare tali esigenze, consentendo: un controllo personale diretto dei dati personali, una sicurezza robusta, una gestione della privacy e una verificabilità delle identità digitali.

Vediamo come la blockchain risponde alle esigenze delle SSI:

- **Decentralizzazione:** la blockchain è una rete distribuita, senza un'autorità centrale. Questo significa che l'identità di un individuo non è controllata da un'unica entità (come un'azienda o un governo), ma è piuttosto gestita dall'individuo stesso. Questa decentralizzazione è allineata con il principio fondamentale delle SSI che sostiene che ogni individuo dovrebbe avere il pieno controllo sulla propria identità digitale.
- **Immutabilità:** una volta che i dati sono registrati su una blockchain, non possono essere modificati o eliminati. Questo rende la blockchain una soluzione ideale per registrare e verificare le credenziali

digitali in un sistema SSI, garantendo che le informazioni di identità non possano essere alterate una volta validate e registrate.

- **Privacy:** la blockchain può essere progettata per proteggere la privacy dell'utente. Ad esempio, le tecnologie come le "zero knowledge proofs" permettono agli individui di condividere la prova che un'informazione è vera, senza dover condividere l'informazione stessa.

- **Trasparenza e Verificabilità:** tutte le transazioni sulla blockchain sono

trasparenti e possono essere verificate da chiunque. Questo significa che le credenziali di identità digitali possono essere verificate in modo indipendente, senza dover fare affidamento su un'autorità centrale.

- **Interoperabilità:** la blockchain può consentire l'interoperabilità tra diverse piattaforme di identità, consentendo agli utenti di utilizzare la stessa identità SSI attraverso vari servizi e applicazioni.

Spindox non poteva farsi trovare impreparata

Spindox, nel contesto del

progetto PILOTA (Piattaforma tecnologica intelligente per la gestione dei processi industriali logistico-produttivi di filiera) finanziato dal Ministero dello Sviluppo Economico e in collaborazione con il Dipartimento di Informatica dell'Università di Salerno, ha sviluppato un modulo di autenticazione che implementa il concetto di Self Sovereign Identity (SSI) basandolo completamente su infrastruttura blockchain.

In particolare, il modulo è stato progettato per permettere la creazione di applicazioni e servizi che gestiscono l'identità digitale in modo decentralizzato. Il modulo fornisce un mezzo sicuro e affidabile per l'implementazione del pa-



radigma SSI, sfruttando registri distribuiti su blockchain per i quali non sussiste il controllo di un'unica entità centrale.

Infine, il modulo permette di interagire e gestire vari tipi di dati di identità, permettendone l'emissione e la verifica. Questo abilita sistemi di autenticazione applicativa (es., Log-In ad una Web UI) tramite SSI su blockchain.

Conclusione

Quanto proposto finora pone Spindox all'avanguardia nello sviluppo di tecnologie di gestione dell'identità digitale

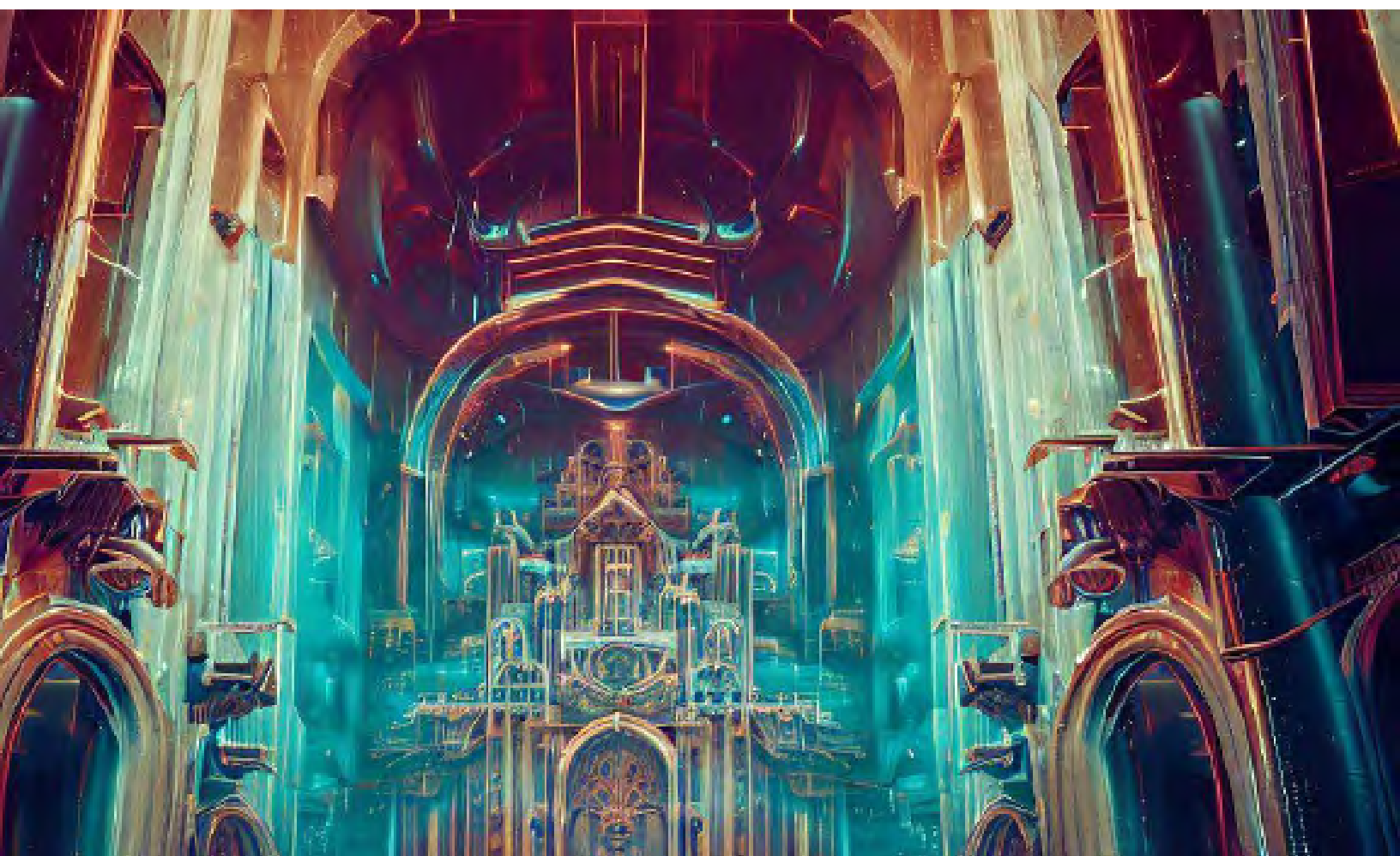
basate su SSI sfruttando la blockchain. Spindox mostra una visione innovativa e pionieristica nel campo dell'identità digitale, supportando gli individui sia nel processo di controllo della propria identità digitale, che nel modo di condividere selettivamente le proprie informazioni con terze parti.

Il promuovere l'autonomia individuale nella gestione dell'identità digitale, unito all'uso di tecnologie avanzate come la blockchain, determina Spindox come un leader nell'evoluzione dell'identità digitale e guida nel modellare i futuri modi con cui interagi-

remo con il mondo digitale.

R. SPAEMANN,

Persone. Sulla differenza tra "qualcosa" e "qualcuno", L. Al-
lodi, Laterza, Roma-Bari 2005





OVER DATA.

Un magazine di proprietà
di Spindox sui temi
dell'artificial intelligence
e della tech culture

Contact us

info@spindox.it

www.spindox.it



spindox