Dipartimento di Giurisprudenza

Cattedra di Informatica Giuridica

BLOCKCHAIN E SMART CONTRACT:

Definizioni, funzionamento, profili giuridici ed applicativi

RELATORE
Chiar.mo Prof.re
Gianluigi Ciacci

CANDIDATO
Simone Brina
Matr. 125013

CORRELATORE
Chiar.mo Prof.re
Cosimo Comella

ANNO ACCADEMICO 2021/2022

BLOCKCHAIN E SMART CONTRACT:
Definizioni, funzionamento, profili giuridici ed applicativi

INDICE

Introduzione……...…3

CAP 1: LA TECNOLOGIA BLOCKCHAIN……..…….4

1.1 Riferimenti storici e definizione……....……4

1.2 Blockchain implementa la distributed ledger technology: evoluzione dei registri...7

1.3 La tecnologia alla base……..8

1.3.1 La funzione crittografica di hash……9

1.4 La proof of work: la prova di lavoro……...……11

1.4.1 Il mining……..12

1.5 La biforcazione della rete……....13

1.6 Varie tipologie di blockchain……..…….15

1.6.1 La rete pubblica: "permissionless"……15

1.6.2 Reti private: "permissioned" ……17

1.7 Eventuali attacchi alla rete……..…….18

CAP 2: GLI SMART CONTRACT…….....…….20

2.1 Definizione di smart contract……..……20

2.2 Rapporti con la blockchain…….21

2.3 Ethereum…….……..22

2.3.1 Il funzionamento di ethereum …….22

2.3.2 Proof of stake……...……23

2.4 La completezza di turing……...……..24

2.5 Gli oracoli…….....…….……25

2.5.1 Chainlink……..27

2.6 Smart contract e contratti tradizionali…….……28

CAP 3: PROFILI GIURIDICI…….……30

3.1 Osservazioni introduttive…….....…….30

3.2 Rapporto tra la Blockchain e la legge: quadro giuridico …….……30

3.3 Blockchain e GDPR……..…….33

3.4 Legge applicabile agli smart contract…….....……48
3.5 L'intervento del legislatore italiano…….....……..50
3.6 Il contratto in forma smart contract…….....…….52
3.6.1 Forme di interazione di smart contract…….....….54
3.6.2 Il linguaggio degli smart contract…….....54
3.6.3 Vicende patologiche e diritto di recesso…….....55
3.7 Tecniche investigative sulla blockchain…….....58
3.8 Foro competente…….....…60
3.8.1 Il Regolamento Roma I…….....62
3.9 Disciplina Europea…….....63
3.9.1 La European Blockchain Partnership…….....65
3.9.2 European Union blockchain observatory and forum……66

CAP 4: CASI D'USO E APPLICAZIONI DELLA TECNOLOGIA.....68

4.1 Blockchain applicata ai procedimenti giuridici.....68
4.2 Blockchain per la corporate governance.....69
4.3 Soluzioni per proprietà intellettuale.....70
4.4 Identità digitale: la soluzione "uport"…….....72
4.5 Blockchain nella Pubblica Amministrazione…….....……..75
4.6 Lotta alla frode IVA…….....……77
4.7 Insurance blockchain …….....…….79
4.8 Tracciabilità in filiera…….....80
4.8.1 Blockchain nella supply chain…….....……81
4.8.2 Nel mondo del food…….....……..82
4.8.3 Nel mondo del "fashion"…….....……85
4.8.4 Nel mondo del manufacturing: Industria 4.0……...……..86
4.8.5 Blockchain per l'agricoltura ……...…..89
4.9 L'impiego della blockchain in ambito sanitario ……..…91
4.10 Voto elettronico (e-voting) tramite blockchain…….94

CONCLUSIONI…….……..…….....100

BIBLIOGRAFIA ……...…….....…….102

INTRODUZIONE

Sono trascorsi tredici anni dalla creazione della prima blockchain. L'intento iniziale era quello di contrapporsi al tradizionale modello centralizzato per lo scambio di valore, tramite la moneta elettronica: la criptovaluta. Dopo tredici anni, le opportunità e le innovazioni prospettate potrebbero sembrare già sfumate e posticce. Tuttavia, il fenomeno blockchain è dirompente ed in costante evoluzione. Ma soprattutto non è ancora compreso e distribuito su larga scala, nonostante al giorno d'oggi, il trend delle crypto sembri dilagante. Si pensi che nel mondo i detentori di criptovalute sono circa 100 milioni e in Italia circa il 18% della popolazione ne possiede qualcuna, ma solamente l'8% dichiara di essere informato sull'argomento o di conoscerne la tecnologia. Una fondamentale osservazione da fare consiste nel fatto che non può esistere criptovaluta senza blockchain, cioè la tecnologia alla base.

In questo elaborato, mi focalizzerò su questa tecnologia, con l'obiettivo di esplicarne il meccanismo ed il funzionamento.

Sarà importante definire la funzionalità alla base di ogni blockchain, per poi proseguire con la descrizione delle sue evoluzioni e delle sue applicazioni pratiche.

Inoltre sarà inevitabile un raffronto di diritto, poiché questa tecnologia, con le sue caratteristiche, solleva profili giuridici totalmente nuovi. Ciò comporterà degli sforzi per individuare le opportune modalità al fine di plasmare i tradizionali principi di diritto così da far integrare il fenomeno blockchain in maniera razionale, permettendo che questa possa proliferare ed applicarsi ad ogni livello e ambito che possa trarne giovamento.

CAPITOLO PRIMO

LA TECNOLOGIA BLOCKCHAIN

1.1 RIFERIMENTI STORICI E DEFINIZIONE

"Chancellor on brink of second bailout for bank", ovvero "il cancelliere sta per effettuare un secondo salvataggio per le banche". Questo il titolo del New York Times del 3 Gennaio 2009 in seguito al crollo del colosso Lehman Brothers, quarta banca d'affari per ordine di grandezza.

È la stessa frase che, sempre il 3 gennaio 2009, venne trascritta nel cosiddetto Genesis Block[1], il primo "blocco" che diede vita alla prima "catena di blocchi". Nasce Bitcoin, nel cui whitepaper si indicava l'invenzione di un sistema monetario decentralizzato che non avesse necessità di una terza parte fiduciaria, e che quindi, tramite la rete peer-to-peer, eliminava il double spending[2], uno dei problemi più significativi nell'ambito dei pagamenti elettronici[3].

Questo quindi, insieme all'intento di arginare l'instabilità causata dalle operazioni bancarie a riserva frazionaria, era l'obiettivo di Satoshi Nakamoto[4], fondatore di Bitcoin, chi sia o chi fosse non ci è dato saperlo.

---

[1] Anniversario del primo blocco della blockchain, https://it.cointelegraph.com/news/bitcoin-turns-ten-on-anniversary-of-genesis-block (consultato il 10/02/2022).

[2] Il double spending viene scongiurato poiché Bitcoin riesce a risolvere il "problema dei generali bizantini", un problema informatico che consiste nel trovare un accordo comunicando tramite messaggi fra le diverse componenti del network. La blockchain di Bitcoin nasce con lo scopo di eliminare la fiducia verso terze parti durante una transazione. L'obiettivo è far sì che tutti siano concordi sull'ordine cronologico delle transazioni e quindi è **fondamentale introdurre un algoritmo di consenso (proof of work)**, che permetta appunto, di mettere d'accordo i diversi attori del network. https://cryptonomist.ch/2019/08/04/problema-generali-bizantini-soluzione-bitcoin/ (consultato il 12/02/2022).

[3] Bitcoin: un sistema di pagamento elettronico peer to peer https://bitcoin.org/it/documento-bitcoin

[4] In generale, la nascita del progetto è piena di storie curiose e di incognite. In primis, l'identità di Satoshi Nakamoto, il cui nome sembra non essere riconducibile a nessun soggetto. Nel 2011, il giornalista Joshua Davis – da anni assiduo seguace della tecnologia – afferma, attraverso un articolo del The New York, che non esisterebbe alcun Satoshi Nakamoto. Il nome, infatti, non farebbe riferimento ad alcun soggetto. Nonostante questo, digitando il nome online è possibile ritrovare una pagina web sul sito di p2pfoundation (un'organizzazione che si occupa dello studio dell'impatto della tecnologia peer-to-peer nella società) dove è possibile verificare età, sesso, cittadinanza.
In particolare, Joshua Davis, si convince dell'inesistenza di Nakamoto dopo un'attenta analisi del progetto. Innanzitutto, si rende conto che tutte le sue pubblicazioni sono scritte in un inglese

«In questo lavoro, proponiamo una soluzione al problema della doppia spesa utilizzando un server di marcatura temporale distribuito peer-to-peer per generare la prova computazionale dell'ordine cronologico delle transazioni». Il problema a cui fa riferimento il white paper Bitcoin è quello per cui è necessario che ciascun pezzo della moneta in corso sia emesso una ed una sola volta. Se questo non avvenisse, non avremmo la certezza del valore del nostro denaro, soggetto ad una quantità variabile e quindi ad inflazione. A livello statale, il problema è superato, ovviamente, dall'esistenza della Zecca di Stato, la quale si accerta dell'emissione di ciascun "pezzo".

Bitcoin risponde a questa necessità, invece, rimuovendo il vincolo di fiducia con l'intermediario (la Zecca, in questo caso) e sostituendolo con l'algoritmo e con la compresenza del registro su tutti i punti della catena.

Il sistema descritto da Satoshi Nakamoto spiega come impacchettare le transazioni dei bitcoin in blocchi[5] che vengono concatenati matematicamente tra di loro. La catena di blocchi permette di segnare i passaggi dei bitcoin, e può essere utilizzata per annotare qualsiasi tipo di transazione, rendendo univoco e non duplicabile il mondo digitale.

---

estremamente corretto. Nel 2009 – durante le sue ricerche - ritrova un tag, nel codice di Bitcoin, che si riferisce ad un articolo del Times di Londra in cui si parla dei primi piani di salvataggio delle banche inglesi, pianificati dal governo britannico. Ulteriori informazioni scoperte sul web dal giornalista, fanno presuppore che Nakamoto sia un cittadino britannico specializzato nella programmazione del linguaggio C++, crittografia, reti, ma anche munito di competenze economiche. Nel 2011 partecipa all'evento Crypto 2011 a Santa Barbara negli Stati Uniti, convinto della presenza di Nakamoto a quell'evento. Li incontra Michael Clear, che pare corrispondere al ricercato elaboratore, ma poco dopo si rende conto di aver fallito nuovamente. Altri messaggi di Nakamoto, in funzione della tipologia di ortografia utilizzata, lasciano supporre che si tratti di un americano, ma anche questi indizi non conducono a particolari scoperte. V. A.TETI, *Bitcoin: la criptomoneta del Cyberspazio che sfida banche e governi, Rivista Mondo Digitale*, n. 46, giugno 2013.

[5] I blocchi sono pacchetti di dati contrassegnati da uno specifico codice, detto hash, che consente a chiunque di verificarne l'autenticità.

Infatti, una volta trovato questo hash, il blocco viene aggiunto alla blockchain e visto che sono tutti dati pubblici, chiunque può scaricare il pacchetto dei dati inclusi nel blocco e verificarne la correttezza dell'hash.

Inoltre, questi blocchi sono concatenati perchè nel pacchetto di dati di ogni blocco è incluso l'hash del blocco precedente. Il fatto è che è sufficiente cambiare anche solo un singolo dato per far sì che l'hash cambi; pertanto, una volta creato un blocco con relativo hash, non può più essere modificato (altrimenti il suo hash risulterebbe scorretto). https://cryptonomist.ch/2020/06/15/in-cosa-consistono-blocchi-blockchain/ (consultato il 20/02/2022).

Cercando di dare una definizione, la parola "*blockchain*" significa "blocchi concatenati" ed è possibile immaginarla come una concatenazione di blocchi costituiti dall'insieme delle transazioni verificabili, in grado di collegare diversi nodi, costituiti fisicamente dai server di ciascun partecipante alla rete, che vengono utilizzati dai soggetti per prendere parte alla decisione. Una delle caratteristiche fondamentali della *blockchain* è quella di essere equiparabile a un libro mastro in cui ogni operazione viene registrata nel sistema e non può essere in alcun modo cambiata, modificata o manomessa. Infatti, per aggiungere un nuovo blocco alla catena, è previsto un preciso protocollo di consenso tra questi nodi. Una volta che il consenso è espresso da tutti i server, il nuovo blocco viene aggiunto e ogni nodo aggiornerà la propria copia senza alcuna possibilità di modifica dei dati una volta validati e inseriti[6].

Volendo poi definire cosa sia effettivamente un blocco[7], lo si può identificare come un file, composto principalmente in una parte detta header, nella quale sono conservati una serie di dati crittografati, e in un'altra detta body, in cui sono contenute tutte le transazioni registrate su un dato blocco.

Ogni blocco contiene il codice crittografico del blocco precedente, facendo quindi in modo che si crei una concatenazione fra i precedenti e i successivi. Per l'appunto, blockchain, ovvero, un registro informatico di transazioni composto da una catena di blocchi.

---

[6] Questa impostazione è frutto dell'attività operata da Satoshi Nakamoto (la cui vera identità è ancora oggi un mistero), a seguito della crisi economica e finanziaria mondiale del 2008 (S. NAKAMOTO, *Bitcoin: a Peer-to-Peer Elettronic Cash System*). La pubblicità di questo registro è una reazione al classico sistema dei pagamenti e si ricollega alla fiducia riposta – da parte dell'utente medio - negli intermediari, colpevoli di poter (con dolo o colpa) perdere la loro funzione di garanzia. Muta, quindi, la concezione di fiducia che andrà a farne perno su un registro pubblico distribuito, accessibile e visibile a tutti. Influenti autori sostengono, poi, che la Blockchain rappresenterebbe "il primo sistema, ancora oggi il più diffuso, di pagamento trustless"(F. SARZANA DI S. IPPOLITO, M. NICOTRA, *Diritto della Blockchain, Intelligenza Artificiale e IoT*, Milano, 2018, 9).

[7] Nel contesto di una blockchain, si tratta di un file contenente i dati relativi alle transazioni. Nel caso di Bitcoin, i blocchi contengono informazioni come i dati di alcune transazioni, un riferimento al blocco precedente e un time stamp.

1.2 BLOCKCHAIN E DISTRIBUTED LEDGER TECHNOLOGY: L'EVOLUZIONE DEI REGISTRI

Fin dalla loro origine, i registri sono sempre stati caratterizzati da una gestione centralizzata.

L'evoluzione tecnologica costituita dalla diffusione della connettività, dall'aumento della velocità della rete e dall'introduzione della crittografia, ha reso possibile lo sviluppo di sistemi caratterizzati da architetture nuove, che superano i tradizionali limiti dei sistemi centralizzati, in cui:

- l'affidabilità dipendente dal funzionamento del sistema centrale, che in caso di guasto blocca l'operatività di tutti gli utenti;
- la scalabilità determinata dalle performance del sistema centrale, che deve essere modificato o sostituito qualora le esigenze degli utenti aumentassero.

Con la DLT[8] si tratta di sistemi cosiddetti "distribuiti", che sono caratterizzati dalla replica sincronizzata del registro in diversi punti, detti nodi, che si comportano come sistemi indipendenti collegati tra loro da una rete di comunicazione, in cui ciascun nodo gestisce la propria copia, mantenuta allineata a tutte le altre.

La famiglia delle distributed ledger technology è estremamente ampia e include architetture diverse. La tecnologia blockchain rappresenta invece una particolare scelta implementativa di registro distribuito inclusa all'interno di questa più ampia famiglia. I sistemi blockchain consentono di effettuare dei trasferimenti o, più genericamente, delle transazioni. Le caratteristiche dei trasferimenti dipendono prima di tutto dal loro livello di programmabilità, con cui si intende la capacità del sistema di prevedere alcune condizioni che regolino il trasferimento degli asset all'interno della rete. Tale capacità

[8] Database definiti come "condivisi" che permetto di effettuare trasferimenti di dati anche senza un sistema di validazione accentrato. Può, quindi, effettuare operazione anche se non è detenuto da un unico ente di gestione: generalmente è duplicato nel device di ogni utente del network, grazie al ricorso alla crittografia per registrare e validare le transazioni e ad una sincronizzazione periodica. (A. PINNA, W. RUTTENBERG, *Distributed ledger technologies in securities post-trading*, in *ECB Occasional Paper*, 2016, CLXXII, pp. 15 ss.).

può essere totalmente assente, oppure può essere limitata solo ad alcune applicazioni particolari, come nel caso di Bitcoin, che ad esempio non può gestire processi in più fasi e tutto il programma deve essere eseguito senza la possibilità di mantenere uno stato intermedio. In altri casi invece, come ad esempio nella rete Ethereum, è possibile definire attraverso un apposito linguaggio di programmazione, un qualsiasi programma arbitrario da svolgere all'interno del sistema (si parla di linguaggio "Turing Completo" sui cui si tratterà successivamente). Ethereum, come anche altri sistemi blockchain, è quindi in grado di definire degli Smart Contract (che approfondirò in seguito), cioè veri e propri programmi eseguiti all'interno della blockchain che possono inviare e ricevere moneta elettronica, modificare il proprio stato, comunicare il verificarsi di un certo evento ed interagire con altri contratti. Caratteristiche che sono, insieme alla decentralizzazione e alla crittografia, che garantisce l'estrema affidabilità e sicurezza, decisamente innovative rispetto ai tradizionali registri.

1.3 LA TECNOLOGIA ALLA BASE

Le tecnologie alla base della blockchain sono essenzialmente due. Una è la rete di collegamenti informatici, o più semplicemente Internet, l'altra è la crittografia.

La crittografia è la "tecnica di rappresentazione di un messaggio in una forma tale che l'informazione in esso contenuta possa essere recepita solo dal destinatario; ciò si può ottenere con due diversi metodi: celando l'esistenza stessa del messaggio o sottoponendo il testo del messaggio a trasformazioni che lo rendano incomprensibile"[9].

[9] BATTAGLINI. R., GIORDANO M., *Blockchain e smart contract: funzionamento, profili giuridici e internazionali, applicazioni pratiche,* 2019.

Tale definizione ci aiuta a comprendere due elementi principali alla base della crittografia:

- L'algoritmo, regola con cui si cela il messaggio
- La chiave, strumento per decifrare il codice

Ci sono esempi di cifrature antiche, di tipo simmetrico cioè in cui si utilizzava una stessa chiave per criptare e decriptare, un esempio era il cifrario di Cesare. Ma mediante le tecnologie moderne, e soprattutto con Internet, è stato possibile evolvere in un metodo di cifratura asimmetrico, attraverso l'inserimento di due chiavi distinte: una chiave pubblica per criptare e una privata per decriptare.

La chiave pubblica è nota a chiunque abbia interesse ad inviare un messaggio, quella privata logicamente è nota solamente al destinatario che la utilizzerà per decifrare il messaggio inviatogli.

Tuttavia anche questo metodo mostra un punto debole. Infatti potrebbe accadere che un terzo soggetto estraneo riesca ad intercettare un messaggio e riuscire a modificarlo o manometterlo, utilizzando la chiave pubblica del destinatario senza che questo se ne accorga.

Per risolvere a tale incombenza, la Blockchain ricorre all'utilizzo di una doppia cifratura unitamente ad una funzione hash.

1.3.1 LA FUNZIONE CRITTOGRAFICA DI HASH

La funzione di hash è di fondamentale importanza nella crittografia. Serve a verificare l'integrità di un messaggio e la si può immaginare come una macchina che prende in ingresso un messaggio qualsiasi e produce in uscita un dato di lunghezza fissa come ad esempio una stringa di 32byte detto hash. Quindi se da un lato possiamo avere in input un numero infinito di possibili messaggi, l'uscita della funzione di hash invece sarà

limitata all'insieme di tutte le combinazioni di bit possibili per una stringa di 32byte (256 bit), ovvero 2^256, un numero sicuramente enorme da poter manomettere. Questo significa che la funzione di hash non stabilisce una corrispondenza biunivoca fra dati in ingresso e dati in uscita. L'algoritmo non è invertibile ed è altamente improbabile ricostruire l'informazione originale a partire dalla stringa. Per questo motivo, si definisce funzione unidirezionale.

L'importanza di questa funzione risiede nel fatto che una qualsiasi minima modifica del messaggio, comporterebbe un'alterazione radicale di tutta la stringa: il cosiddetto effetto valanga e quindi ci si accorgerebbe subito dell'alterazione di un messaggio.

Attualmente l'algoritmo di hash più diffuso è lo SHA-256[10] che ottiene un Hash di 32byte (256 bit) a partire da un qualsiasi messaggio di input.

Volendo fare un esempio, mi reco su un sito in grado di calcolare una funzione di hash SHA-256 e digito la parola: *Bitcoin*

Che viene codificata in

b4056df6691f8dc72e56302ddad345d65fead3ead9299609a826e2344eb63aa4

Una stringa alfanumerica di 64 caratteri corrispondenti a 256 bit. Il codice sarà unico e irreversibile di volta in volta. Infatti, volendo causare volontariamente un effetto valanga, basterà apportare una modifica al testo precedente, aggiungendo una semplice virgola: *Bitcoin,*

e87926c808b28a379d3bd7d1187521ff843da75f18a35c9fb582d418cc21513d

[10] SHA256, o *secure hash algorithm* 256-bit, è un algoritmo di hash utilizzato per la sicurezza crittografica.

La stringa che si ottiene è completamente diversa[11]. Questo fondamentale requisito fa si che la funzione di hash possa essere utilizzata per autenticare in maniera univoca e sicura qualsiasi documento.

Unendo la funzione di hash con un sistema di cifratura a chiave pubblica è possibile costruire le basi di un sistema di firma digitale. Lo schema più semplice di firma digitale di un documento parte dalla funzione di hash. Con questa funzione, il mittente genera un identificativo unico e di lunghezza fissa, ad esempio 32byte, del documento originale. Con la sua chiave privata, cifra tale hash, ottenendo come risultato la firma. Ricevendo il documento originale insieme alla sua firma, il destinatario potrà usare la chiave pubblica del mittente per decifrare la firma e confrontare l'hash del documento ricevuto con l'hash decifrato dalla firma. Se i due coincidono la verifica della firma è riuscita[12].

1.4 LA PROOF OF WORK: LA PROVA DI LAVORO

Una ulteriore tecnologia su cui si basa la blockchain è l'algoritmo di consenso che prende il nome di Proof of Work. Questo, attraverso la già descritta funzione di hash, permette di implementare la sicurezza nella rete. Quindi, utilizzando una funzione matematica per crittografare, si riduce la possibilità di manipolazione dell'informazione che viene trasmessa. Nel caso Bitcoin, queste funzioni sono utilizzate al fine di

[11] Prova eseguita mediante il sito: https://www.convertstring.com/it/Hash/SHA256

[12] Un meccanismo di verifica che si può ottenere grazie alla funzione di hash è il cosiddetto Merkle Tree. I merkle tree sono una struttura dati creata con l'obiettivo di facilitare la verifica di grandi quantità di dati organizzati mettendoli in relazione attraverso varie tecniche crittografiche e di gestione delle informazioni. Un albero di merkle è una struttura dati suddivisa in più livelli il cui scopo è mettere in relazione ciascuno nodo con un'unica radice associata ad essi. Per ottenere ciò, ogni nodo deve essere identificato con un identificatore univoco. Questi nodi iniziali, chiamati nodi figlio (foglia), vengono quindi associati a un nodo superiore chiamato nodo padre (ramo). Il nodo padre avrà un identificatore univoco risultante dall'hash dei suoi nodi figli. Questa struttura si ripete fino al nodo radice o radice di merkle la cui impronta è associata a tutti i nodi dell'albero. https://academy.bit2me.com/it/que-es-un-arbol-merkle/#Tecnologia_blockchain (consultato il 22/06/2022).

controllare la correttezza delle transazioni eseguite. Inoltre, nel corso di ogni transazione, viene firmato l'hash della funzione precedente e chi riceve la transazione può controllare i passaggi di proprietà della moneta trasferita, in questo caso. Una volta che la transazione è approvata, non è possibile modificarla poiché gli hash non verrebbero più a corrispondere. La proof of work, inoltre, va ad incentivare i miner nell'elaborazione degli scambi di moneta, ricevendo una ricompensa ad ogni problema matematico risolto[13]. Intendendo con problema, la funzione di hash o la scomposizione in numeri primi. Il problema, è definito hashcash, e l'algoritmo cambia la propria difficoltà in maniera dinamica proporzionalmente alla potenza computazionale della rete.

1.4.1 IL MINING

Quando la prima blockchain venne ideata, il quesito che ne scaturì successivamente, fu in quale modo si potesse creare una moneta all'interno di un sistema basato sulla decentralizzazione, la cui creazione e diffusione venisse demandata agli utenti fruitori della rete[14]. La soluzione fu quella di progettare il sistema affinché elargisse coin come premio ai componenti della rete che fornivano potenza elaborativa, necessaria a rafforzare e strutturare la rete stessa, secondo un sistema casuale elaborato in maniera tale da elargire coin proporzionalmente alla potenza computazionale fornita. Questa attività è appunto definita mining. Il termine indica il processo attraverso il quale i "minatori" riescono a confermare le transazioni, validando nuovi blocchi da aggiungere alla catena e quindi incrementando la sicurezza del sistema. Il miner che

[13] Di qui il termine Proof of Work, in italiano prova di lavoro

[14] In riferimento ad alcune criptovalute, come bitcoin, il mining è il processo attraverso cui le transazioni tra utenti vengono verificate e aggiunte alla blockchain, nonché il processo che consente, in base a un algoritmo specifico, di immettere in circolazione nuove monete.

per primo risolve il problema[15] e, quindi, aggiunge un nuovo blocco alla catena, ottiene una ricompensa consistente dalle commissioni derivanti dalla transizione all'interno del blocco stesso. Questo è quanto avviene nelle blockchain pubbliche, in quelle private, invece, il mining è svolto dall'autorità che crea e governa la rete. Essenzialmente i miner svolgono due funzioni rilevanti: certificare gli scambi tramite la proof of work e immettere in circolazione nuovi coin. Per quanto riguarda la rete Bitcoin, ogni due settimane devono essere prodotti circa 2016 nuovi blocchi (1 ogni 10 minuti circa). La difficoltà computazionale dell'attività di mining si regola in automatico nel tempo per mantenere una velocità costante di creazione di blocchi. Un ulteriore incentivo per il miner è rappresentato dalla cosiddetta *fee,* che consiste in una sorta di tariffa che il mittente paga per velocizzare una transazione. Infatti, se si fermasse l'attività di mining, si bloccherebbe l'intero sistema[16].

1.5 LA BIFORCAZIONE DELLA RETE

Il protocollo prevede che ogni nodo osservi e misuri il tempo medio tra un blocco e l'altro che per Bitcoin deve essere, come detto, di dieci minuti. Ogni 2016 blocchi tutti i nodi calcolano il tempo medio e se troppo breve ricalcolano il nuovo target che sarà

[15] I miner calcolano degli hash crittografici sull'head del blocco. Per ogni nuovo hash, il software di mining utilizza un numero casuale detto Nonce. Per far sì che l'estrazione di un blocco diventi un "lavoro" non semplice, il miner deve trovare un hash che sia inferiore ad un determinato numero. La difficoltà è un numero che regola il tempo che impiegano i miner per estrarre il blocco successivo, che verrà poi aggiunto alla blockchain. In media questo tempo è di dieci minuti. Come detto la difficoltà si "aggiusta" ogni due settimane, in realtà ciò avviene ogni 2016 blocchi. Trascorso questo intervallo, ciascun nodo esegue una operazione che consiste nel moltiplicare il tempo atteso per i 2016 blocchi (2016 x 10 minuti) e divide il risultato con un numero che si ottiene dal prodotto del tempo effettivo per i 2016 blocchi. https://cryptonomist.ch/2019/08/25/come-funziona-difficolta-bitcoin/ (consultato il 03/03/2022).

[16] Per le primissime operazioni, anche un singolo partecipante alla rete con un piccolo computer poteva effettuare la transazione. Oggi esistono dei veri e propri pool che – dall'unione di vari elaboratori – danno vita ad una potenza informatica maggiore per effettuare quante più validazioni possibili. E. FLORINDI. *Criptovalute: manuale di sopravvivenza.* [ebook] Imprimatur. Reperibile su: https://www.perlego.com/book/1080129/criptovalute-manuale-di-sopravvivenza-pdf

più difficile del precedente. Se invece sarà superiore ai dieci minuti previsti allora il target dovrà essere ricalcolato al ribasso per rendere la prova di lavoro più facile. Invece, per quanto riguarda il tempo di transito che l'annuncio di un nuovo blocco impiega per raggiungere tutti i nodi della rete, bisogna considerare la possibilità che due blocchi validi possano essere generati da nodi diversi e in momenti molto vicini e trasmessi agli altri nodi che li ricevono in una sequenza casuale. Ogni nodo avrebbe il dilemma di scegliere quale dei due nuovi blocchi è quello veramente valido. Quello che succede è di fatto un fork[17], o biforcazione. Una situazione gestita dal protocollo che prevede una riorganizzazione della catena dei blocchi per eliminare uno dei due rami, poiché la blockchain deve avere una storia univoca. La riorganizzazione prevede che solo il ramo che contiene la maggior prova di lavoro sia conservato, perché più sicuro, mentre l'altro verrà scartato e tutte le sue transazioni saranno di nuovo "non confermate". Esistono tuttavia altri tipi di biforcazione che possono essere indotte volontariamente con lo scopo di modificare il protocollo. Tali modifiche possono essere ostili o consensuali e attengono alla governance dell'intera rete. In generale si definiscono soft fork le modifiche del protocollo le cui nuove regole sono più restrittive delle precedenti o comunque in cui il nuovo formato dei blocchi è compatibile con le vecchie regole. Un hard fork[18], al contrario, è una biforcazione creata appositamente da un gruppo di nodi che intendono conservare la storia della Blockchain cambiando in modo più sostanziale le regole di funzionamento. In generale

[17] Nel settore delle criptovalute, il termine si riferisce ad un aggiornamento del software, volto all'introduzione di cambiamenti, nuove funzionalità o nuove regole. In relazione alle criptovalute decentralizzate, i fork rappresentano spesso un motivo di forte dibattito all'interno della comunità. I fork che implementano cambiamenti retrocompatibili, ovvero che consentono ai nodi non aggiornati di continuare a partecipare alla rete purché rispettino le nuove regole, sono detti soft fork.
I fork che non consentono ai nodi non ancora aggiornati di partecipare alla rete sono detti hard fork. Gli hard fork possono talvolta dar vita a blockchain indipendenti e nuove criptovalute, utilizzate da porzioni
della comunità che non intendono aderire ai cambiamenti proposti e accettati dal resto della comunità. GL COMANDINI "da zero alla luna" 2020

[18] https://it.cointelegraph.com/bitcoin-cash-for-beginners/what-is-hard-fork (consultato il 10/03/2022).

i blocchi generati dai nodi che appoggiano un hard fork non vengono accettati dai nodi non aggiornati e questo può causare una partizione della rete con relativa divisione della comunità in due fazioni creando di fatto due monete che continuano con una vita propria. Un esempio notevole di questo fenomeno degli hard fork ostili è il fork del Bitcoin Cash. Tuttavia, non tutti gli hard fork sono ostili. Ad esempio, la rete Ethereum sistematicamente si aggiorna grazie a degli hard fork proposti dagli sviluppatori e ai quali normalmente tutti i nodi si adeguano senza troppi problemi.

1.6 LE VARIE TIPOLOGIE BLOCKCHAIN

Dopo aver delineato la tecnologia alla base, si possono ora introdurre le varie tipologie di blockchain. Esse differiscono a seconda del numero di partecipanti che possono o meno prendere decisioni all'interno della rete e del modo di consenso con cui vengono inserite le informazioni all'interno della rete.

1.6.1 LA RETE PUBBLICA: "PERMISSIONLESS"

La prima e principale rete pubblica e quella Bitcoin, in cui non vi è alcun soggetto in grado di esercitare il controllo delle transazioni, proibirle, regolamentarle.

Inoltre, poiché il protocollo Bitcoin è open source, chiunque è in grado di scaricarlo e utilizzarlo. Il protocollo gratuito blockchain è stato adoperato per progetti alternativi che si applicano sulla stessa catena Bitcoin, oppure sono state create una moltitudine di nuove blockchain completamente separate da essa e caratterizzate da differenze più o meno marcate, pur mantenendo la tecnologia di base. Tra gli aspetti tecnici più rilevanti delle reti pubbliche è interessante la gestione della sicurezza in modo auto-regolamentato. Poiché infatti il sistema è completamente decentralizzato, ognuno possiede una copia del database e, per creare ogni modifica, è necessario attraversare

preliminarmente un certo numero di autorizzazioni, il che rende impossibile per un hacker contraffare una transazione, salvo che non entri in possesso di una chiave privata e quindi si sostituisca al "legittimo proprietario", termine qui espresso tra virgolette, poiché che il concetto di legittima proprietà "vacilla" insieme al concetto di identificazione e autenticazione. Infatti, nella rete pubblica, non ci si accede attraverso un account creato a seguito della verifica del codice fiscale, o della e-mail. Nome, cognome ed indirizzo non hanno nessuna utilità, poiché i nodi non riportano dati anagrafici, sono infatti sorretti dallo pseudonimato.

Quindi il concetto di "permissionless" indica una rete che è pubblica, aperta a tutti e decentralizzata. Un tale modello impedisce ogni forma di censura e nessuno può impedire che una transazione possa aggiungersi al registro, dopo aver ottenuto il consenso da tutti i nodi della rete. Le reti permissionless quindi, possono essere utilizzate come database per ogni tipologia di documenti, soprattutto per quelli che hanno necessità di essere immutabili nel tempo. Gli esempi classici di reti pubbliche sono senza dubbio Bitcoin ed Ethereum. Alcune sono cloni queste, come Bitcoin Cash o Litecoin, con le stesse regole di consenso, mentre altre divergono, come IOTA[19], che ha l'ambizione di essere "il ledger di qualunque cosa", proponendosi come protocollo IOT (Internet of things)[20] basato su blockchain.

[19] Per approfondimenti: https://www.iota.org/ (consultato il 03/06/2022)

[20] L'espressione Internet of Things è stata formulata per la prima volta nel 1999, in stretta relazione con i dispositivi RFId (Radio Frequency Identification), dall'ingegnere inglese Kevin Ahston, cofondatore dell'Auto-ID Center di Massachussetts. Per Internet of Things (IoT) o Internet delle Cose si intende quel percorso nello sviluppo tecnologico in base al quale, attraverso la rete Internet, potenzialmente ogni oggetto dell'esperienza quotidiana acquista una sua identità nel mondo digitale. Come detto, l'IoT si basa sull'idea di oggetti "intelligenti" tra loro interconnessi in modo da scambiare le informazioni possedute, raccolte e/o elaborate.
https://blog.osservatori.net/it_it/cos-e-internet-of-things#iot-significato

1.6.2 LA RETE PRIVATA: "PERMISSIONED"

Le reti di tipo permissioned sono di tipo centralizzato, a prima vista, il risultato è quanto di più distante esista dalla filosofia insita nella blockchain. Infatti, possono essere gestite da una o più organizzazioni e sono basate da un insieme di regole condivise da tutti colore che fanno parte della rete e che sono autorizzati ad utilizzarla. La struttura di un simile modello è risultata interessante per il mondo aziendale, che ne ha intravisto una enorme potenzialità per automatizzare e gestire processi interni ed esterni. Nel settembre 2015 nasce infatti il consorzio R3, fondato da una decina dei maggiori istituti bancari nel mondo, con lo scopo di concentrare le forze per la creazione di un ledger distribuito a scopo finanziario. Ancora, il progetto Hyperledger, lanciato dalla Linux Foundation, e supportato da grandi colossi del settore informatico quali IBM, SAP ed Intel, con l'obiettivo di generare una avanzata collaborazione "cross-industry" attraverso lo sviluppo di blockchain e registri distribuiti, con particolare attenzione agli aspetti della performance e dell'affidabilità, in modo da poter supportare con maggiore efficacia i business globali.

Il tema portante resta la centralizzazione del controllo da parte di un ente "terzo", che offre agli utilizzatori la possibilità di controllare chi e come utilizza le risorse della rete, mettendo nelle mani dell'ente gestore la gestione delle regole d'accesso, di utilizzo e in pratica il meccanismo del consenso. È evidente come più gli obiettivi delle reti siano orientati al business e al commercio, più la decentralizzazione venga meno, a favore di un grado più o meno elevato di "controllo". Ad esempio, la rete VeChain si propone espressamente di essere «the World's Leading Blockchain Application Platform Driven by Enterprise Adoption», concentrando quindi i suoi sforzi per creare una rete "robusta e sicura" per veicolare strumenti hardware e software di avanguardia per sviluppatori e aziende, operanti in un buon numero di industry differenti, quali Agriculture, Energy commodities, Automotive, Logistic, Retail.

Quindi, per rete privata si definisce quella blockchain che "appartiene" ad un ente o organizzazione. Questa organizzazione può successivamente scegliere una autorità che garantisca e limiti gli accessi indicando a chi è consentito l'utilizzo in lettura e scrittura della rete, stabilendo inoltre le regole di gestione ed occupandosi della governance.

Meglio permissionless o permissioned? La domanda nasce quasi spontanea. In certi casi casi la scelta è di tipo "politico", cioè in riguardo a quali valori la rete si vuole fare portatrice, in sostanza quale rappresentazione della stessa si vuole dare. Certamente nel voler disegnare una soluzione di business basata sulla blockchain, bisognerà soppesare il "*must have*" dal "*nice to have*" e quindi sarà sicuramente necessaria un'analisi realistica di cosa serva e di cosa si ha necessità per la realizzazione del fine che si vuole perseguire.

1.7 EVENTUALI ATTACCHI ALLA RETE

Gran parte della sicurezza del sistema è garantita dalla crittografia, che lega tutti i blocchi tra loro. Dal momento che i dati vengono inseriti nei blocchi successivi, il sistema è sempre in grado di confrontare il nuovo blocco con l'intera catena e quindi è in grado di accorgersi di eventuali contraddizioni al fine di riconoscere un ipotetico blocco hackerato. Ci sono, tuttavia, alcuni tipi di attacchi, seppur improbabili, che potrebbero avere luogo. L'attacco DDoS (Distrubet Denial of Service) è ad esempio, un tentativo di paralizzare un nodo della rete, sovraccaricandolo con un elevato volume di traffico. Vengono inviate molteplici e svariate transazioni di piccola entità, spesso non valide, al solo scopo di impedire l'elaborazione delle transazioni reali. Tuttavia, le principali reti sono strutturate in maniera tale da non temere un simile attacco.

Diverso invece è il cosiddetto attacco 51%. Questo consiste nel tentativo di soppiantare il normale processo di consenso del protocollo, cercando di ottenere il

controllo del 50% + 1 dei nodi della rete, per far approvare blocchi creati ad hoc per dar vita, ad esempio, ad un fenomeno di doppia spesa. In questo caso si mirerebbe ad effettuare una transazione, e successivamente cancellarla dalla cronologia della catena per poter effettuare nuove transazioni con le stesse coin per una seconda volta. Si può affermare che un simile attacco è solamente teorico, mai ancora verificato. Infatti, per attuarlo sarebbe necessaria una potenza computazionale ed un impiego economico, che ad oggi nessuno sarebbe in grado di sostenere e in aggiunta non sarebbe per nulla redditizio. Infine, si rende necessario puntualizzare che tali considerazioni si riferiscono esclusivamente alle blockchain decentralizzate. Infatti, quelle più centralizzate possono presentare più rischi di hackeraggio, poiché una blockchain meno decentralizzata è maggiormente esposta a rischi di attacco.

CAPITOLO SECONDO

GLI SMART CONTRACT

2.1 DEFINIZIONE DI SMART CONTRACT

Non esiste una definizione univoca di *smart contract*[21], un termine che oggi viene associato alla tecnologia blockchain[22], ma che risulta in realtà oggetto di studio già dagli anni '90.

Le definizioni che sono state date sono molteplici e mettono in luce l'aspetto "*smart*", costituito proprio dalla sua capacità di autoeseguirsi senza il bisogno di intermediari.

Il primo a parlare di smart contract è stato Nick Szabo[23] nel 1994. Egli appartiene ai cc.dd. Cypherpunks, un movimento, nato alla fine degli anni Ottanta del XX secolo, che pone il tema della privacy come obiettivo da perseguire per il bene comune[24].

Szabo definisce gli *smart contract* come "*protocolli di transazione informatizzati, che eseguono i termini di un contratto"*. Più precisamente, suggerì che traducendo clausole contrattuali in codici e incorporandole in hardware o software in grado di auto applicarle era possibile ridurre al minimo la necessità di intermediari tra le parti e il verificarsi di eccezioni dannose o accidentali.

---

[21] https://www.blockchain4innovation.it/mercati/legal/smart-contract/blockchain-smart-contracts-cosa-funzionano-quali-gli-ambiti-applicativi/

[22] Gli smart contract sono codici per computer inseriti in registri distribuiti o blockchain, che memorizzano su tali registri il risultato della loro esecuzione.

[23] Secondo Szabo: «A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises». «I call these new contracts "smart", because they are far more functional than their inanimate paper-based ancestors. No use of artificial intelligence is implied». «The basic idea behind smart contracts is that many kinds of contractual clauses (such as collateral, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive (if desired, sometimes prohibitively so) for the breacher» N. SZABO,Smart Contracts: Building Blocks for Digital Markets, 1996, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (consultato il 01/06/2022).

[24] I Cypherpunk sostengono l'utilizzo della crittografia e di altre tecnologie, al fine di tutelare la privacy e ottenere, così, un cambiamento nel paradigma sociale e politico. Agli inizi degli anni Novanta del secolo scorso,il movimento comunicava grazie ad unaserie di mailing list crittografate. La prima prova dell'esistenza di questa corrente di pensiero si trova nel lavoro di DAVID CHAUM:"Security without Identification: Transaction Systems to Make Big Brother Obsolete", pubblicato nel 1985 (v. https://nextgenerationcurrency.com/cypherpunk-david-chaum-satoshinakamoto/)

Il carattere del contratto intelligente è rappresentato dal fatto che le parti raggiungano un accordo sulle clausole contrattuali e sui tempi sfruttando poi la logica del "*if-this-then-that*", ossia se si verifica un presupposto (*this*) allora consegue un risultato (*that*); per il resto il contratto intelligente ha la capacità di far rispettare le proprie clausole ed entrare in esecuzione senza il supporto di una parte esterna (si pensi ,ad esempio, ad una clausola inserita nello *smart contract* stipulato tra Tizio e Caio che prevede il versamento di una somma di denaro in caso di inadempimento contrattuale: al verificarsi della condizione di inadempimento la somma pattuita a titolo di penale verrà versata automaticamente dal conto di Tizio al conto di Caio). In altri termini, il codice degli smart contract è progettato in modo tale da essere eseguito al verificarsi di una determinata condizione. A tal proposito, occorre sottolineare, così come evidenziato dallo stesso Nick Szabo, che gli smart contract non sono del tutto "smart". Il codice di uno smart contract, infatti, viene eseguito solo quando viene attivato da una transazione inviata da un account esterno (facente capo ad una persona fisica o ad un'azienda) o da un messaggio inoltrato da un altro smart contract.

A causa della mancanza di un ambiente di sviluppo adatto, tuttavia, gli smart contract, così come concepiti da Szabo, non sono mai stati utilizzati su larga scala.

2.2 RAPPORTI CON LA BLOCKCHAIN

La vera svolta per gli smart contract è arrivata con la proliferazione della tecnologia blockchain. La blockchain technology ha portato a nuove discussioni sull'utilizzo degli smart contract per far rispettare gli accordi tra individui senza ricorso a terzi.

Ad oggi, si contano sempre più società e sempre più diversi protocolli finalizzati alla creazione degli smart contract, il cui lavoro, aggregato, costituisce la base essenziale

delle regole di scrittura degli stessi. Sta nascendo, così, un ecosistema per la sperimentazione e l'implementazione degli smart contract.

Non tutte le blockchain, tuttavia, consentono la programmazione degli smart contract. La prima ad offrire tale possibilità è stata la blockchain Ethereum[25].

2.3 ETHEREUM

La rete Ethereum[26] nasce nel 2013 per opera di Vitalik Buterin[27], uno sviluppatore di origini russe e cresciuto in Canada.

Ethereum può essere definita come un grande computer condiviso, un *planetary scale computer*. Con questa rete, infatti, si passa dal concetto di distrubuted ledger a quello di distrubuted computing o anche world computing, cioè un computer mondiale virtuale che ha l'obiettivo di decentralizzare il modello client-server esistente ed è composto da tutti i computer connessi alla rete Ethereum ma, parallelamente, è autonomo da essi. Quindi, chi fa parte della rete ha accesso ad un archivio, immutabile e condiviso, di tutte le operazioni svolte. Ethereum, inoltre, è una programmable blockchain, cioè non si limita a mettere a disposizione operations predefinite e standardizzate, ma permette agli utenti di crearne delle proprie e di sviluppare diverse tipologie di applicazioni blockchain, non necessariamente circoscritte alle sole cryptocurrencies.

2.3.1 IL FUNZIONAMENTO DI ETHEREUM

Ogni partecipante lavora su una rete peer-to-peer e può sviluppare smart contract utilizzando le risorse computazionali della rete e l'utilizzo di tali risorse viene

[25] La criptovaluta che circola sulla blockchain Ethereum prende il nome di Ether. https://www.blockchain4innovation.it/esperti/cose-quali-gli-ambiti-applicativi-ethereum/ (consultato il 18/03/2022)

[26] https://ethereum.org/it/whitepaper/ (consultato il 10/06/2022)

[27] https://it.wikipedia.org/wiki/Vitalik_Buterin (consultato il 10/06/2022)

remunerato con una criptovaluta detta ether. Questa ha una funzionalità binaria, poiché rappresenta sia la potenza computazionale necessaria per la produzione dei contratti sia il compenso agli utenti per la loro realizzazione. Ogni transazione ha un costo che in Ethereum è detto "gas" e che risulta in stretta correlazione con la c.d. Ethereum Virtual Machine, motore della rete Ethereum e centro di calcolo che garantisce l'esecuzione degli smart contract, implementando il meccanismo di consenso della rete fornendo, in aggiunta, un ambiente protetto dal resto della rete locale. Le istruzioni all'interno di una transazione devono essere eseguite fino in fondo senza errori, onde evitare il fallimento dell'operazione. Ogni istruzione viene eseguita dai miner e contabilizzata con un'unità di gas. Non è stato direttamente assegnato un prezzo definito in ether alle istruzioni della macchina poiché si è voluto separare il costo computazionale da quello economico. In un certo senso il gas è una misura empirica di quanto costa alla rete eseguire un certo pezzo di codice. Un po' come calcolare il consumo di un'auto per percorrere un determinato tratto di strada. Tuttavia, quando creiamo una transazione possiamo decidere il parametro di gas limit massimo[28].

2.3.2 LA PROOF OF STAKE

Si intuisce che anche in Ethereum ci si affida al processo di mining e qui il tempo necessario affinché la rete generi un blocco è circa 12 secondi. Tuttavia, a causa dell'elevato costo dell'energia elettrica consumata dalla blockchain, è in atto un iter per evolvere dal proof of work al proof of stake[29], forma di consenso meno dispendiosa a livello energetico e più distribuita. Questa tipologia di consenso prevede l'introduzione

[28] Transazione Ethereum out of gas, etherevolution.eu

[29] Algoritmo di consenso utilizzato da diverse criptovalute e basato sulla selezione pseudo-casuale del nodo validatore del blocco successivo in base a uno o più parametri, come ad esempio lo staking, ovvero il "congelamento" di una quantità di token all'interno della rete.

di una figura detta *validator*. Questo viene scelto casualmente tra tutti i nodi della rete per creare un nuovo blocco. Per poter essere nominato validator è necessario dimostrare di possedere una certa quantità di token. Una volta che il blocco viene aggiunto alla catena, il validator riceve una ricompensa determinata dalle fee delle transazioni contenute in quel dato blocco. Per quanto concerne il meccanismo di fiducia nei confronti del validator è previsto che nel caso in cui venissero approvate delle transazioni fraudolente, il validator perderebbe parte del suo deposito, pertanto, è finanziariamente conveniente agire con onestà.

2.4 LA COMPLETEZZA DI TURING

Dopo aver introdotto Ethereum, conseguentemente si deve fare riferimento al linguaggio di Turing[30]. Tecnicamente si definisce Turing completo un sistema di regole, e quindi anche un linguaggio di programmazione, che abbia la capacità di eseguire qualunque logica eseguibile da una macchina di Turing che a sua volta è un modello di calcolo definito dal celebre scienziato Alan Turing. La macchina di Turing è una macchina ideale che con teoriche operazioni di scrittura è in grado di risolvere tutti i problemi calcolabili ed Ethereum tramite la sua ethereum virtual machine, è in grado di farlo.

L'innovazione rivoluzionaria di Ethereum è quella di combinare l'architettura di calcolo generale di una macchina in un programma memorizzato su blockchain, creando così un computer mondiale distribuito a stato singolo. I programmi di Ethereum funzionano "ovunque", ma producono uno stato comune che è garantito dalle regole del consenso. Quando un miner riceve una di transazione indirizzata ad un contratto, se tale richiesta è legittima, il contratto eseguirà il cambiamento del suo

[30] https://it.frwiki.wiki/wiki/Turing-complete (consultato il 10/06/2022)

stato. Lo stato di uno smart contract non è registrato nella memoria di un solo computer ma in quella di tutti i computer partecipanti. La rete nella sua interezza si comporta quindi come un computer globale e ogni programma anche composto da poche istruzioni viene eseguito da migliaia di computer in modo identico con lo scopo di poter raggiungere un consenso che tradotto in linguaggio umano apparirebbe come: "acconsento, siamo d'accordo sullo stato successivo del programma".

Questa esecuzione risulta essere praticamente inarrestabile, infatti una volta che il contratto è in esecuzione questo non può essere interrotto o sospeso da nessuno a meno che tali stati di interruzione e sospensione non siano stati previsti dai suoi programmatori. Questa caratteristica rende gli smart contract resistenti alla censura. Resistenza che in realtà dipende dalla capacità della blockchain sottostante di assorbire un attacco, anzi più ingenerale possiamo dire che uno smart contract potrà essere resistente al massimo quanto lo è la blockchain in cui viene eseguito.

Per quanto concerne la scrittura di smart contract, Ethereum si avvale di Solidity attualmente suo linguaggio di punta che consente e garantisce un maggior livello di flessibilità ed espressività nella programmazione[31].

2.5 GLI ORACOLI

La grande forza degli smart contract risiede, dunque, nella flessibilità e nelle loro numerose applicazioni. Infatti, qualsiasi contratto che abbia la necessità di essere immutabile nel tempo, accessibile da chiunque e verificabile, può essere creato attraverso uno smart contract e quindi "tradotto" in codici informatici che si attivano in automatico al soddisfarsi di determinate condizioni, preventivamente concordate.

[31] AA.VV., Documentazione ufficiale linguaggio solidity, https://solidity.readthedocs.io/en/v0.5.10/ (consultato il 02/06/2022)

È possibile, tuttavia, che le condizioni che attivino lo smart contract siano "esterne" alla blockchain. Quando le condizioni vengono soddisfatte, lo smart contract viene quindi attivato. Questo è possibile grazie a dei particolari strumenti chiamati oracoli.

Un oracolo è un servizio progettato specificamente per connettere una blockchain con il mondo esterno, fornendo agli smart contract tutte le informazioni necessarie per eseguire una computazione dopo averne verificato preliminarmente la correttezza. Gli oracoli sono particolarmente importanti per l'esecuzione degli smart contract complessi, che sono poi quelli la cui utilità è maggiore. Si pensi, ad esempio, ad un contratto assicurativo, che deve essere eseguito solo se c'è la conferma di particolari eventi esterni (eventi climatici, denunce, soglie economiche). Il dato deve necessariamente avere un elevatissimo livello di affidabilità, comparabile con il livello di affidabilità stesso della blockchain. Qualsiasi livello inferiore rischia di compromettere il funzionamento dell'intero sistema.

Gli oracoli possono essere basati su software, hardware o intermediari umani. Un oracolo basato su software può essere programmato per cercare e analizzare il testo da fonti online e può controllare gli eventi che si verificano su altre blockchain.

Gli oracoli hardware ottengono dati esterni, recuperati da sensori e dall'Internet of Things. Gli oracoli umani sono necessari per compiti che sono troppo costosi o troppo complessi per essere eseguiti dalle macchine.

La fonte da cui l'oracolo recupera i dati, del resto, potrebbe fornire dati errati deliberatamente (a causa di cattiva condotta, frode o collusione) o involontariamente Poiché gli oracoli e le fonti esterne di dati sembrano essere soggetti nuovamente al problema del single point of failure, è evidente che essi reintroducono nell'intero ecosistema blockchain la necessità di fiducia. Pertanto, ogni volta che uno smart contract richiede informazioni esterne tramite un oracolo, gli utenti sono costretti a fidarsi sia della fonte dei dati che dell'oracolo stesso. Con riferimento agli oracoli

(persone fisiche o giuridiche) che svolgono tale attività a livello professionale o imprenditoriale, i profili di responsabilità saranno evidentemente disciplinati nel contratto di servizio o, in assenza, nel Codice civile.

Per quanto concerne oracoli scelti dalle parti senza alcun rapporto contrattuale con l'oracolo stesso (si pensi a siti web che forniscono dati inerenti voli aerei), sarà opportuno che le parti disciplinino, a livello contrattuale, l'allocazione dei rischi inerenti dati errati, imprecisi o incompleti forniti.

2.5.1 CHAINLINK

Un contributo rilevante al tema degli oracoli è rappresentato da Chainlink che prevede un token nativo, il LINK, che retribuisce l'autore dell'informazione[32]. Chainlink ha una componente sulla blockchain, basata su smart contract, e componenti off-chain basate su una struttura decentralizzata, fatta da nodi. Per quanto riguarda la parte on-chain, ChainLink esegue un processo basato sulla selezione degli oracoli in grado di fornire l'informazione, sul reporting delle informazioni da parte dei nodi oracoli e sull'aggregazione dei risultati. A livello di selezione degli oracoli, i contratti on-chain si occupano di generare delle richieste di informazioni. I nodi off-chain di Chainlink possono quindi decidere se rispondere o meno alla richiesta, su quello che è in pratica un mercato di scambio. I nodi che decidono di rispondere mettono a deposito la pro-

[32] "Blockchain oracles are often viewed today as decentralized services with one objective:
to forward data from off-chain resources onto blockchains. It's a short step, though, from forwarding data to computing on it, storing it, or transmitting it bidirectionally. This observation justifies a much broader notion of oracles' functionality. So too do the growing service requirements of smart contracts and increasingly multifaceted technologies that rely on oracle networks. In short, an oracle can and will need to be a general-purpose, bidirectional, compute-enabled interface between and among on-chain and off-chain systems. Oracles' role in the blockchain ecosystem is to enhance the performance, functionality, and interoperability of smart contracts so that they can bring new trust models and transparency to a multiplicity of industries. This transformation will come about through broadening use of hybrid smart contracts, which fuse blockchains' special properties with the unique capabilities of off-chain systems such as oracle networks and thereby achieve far greater reach and power than on-chain systems in isolation". Astratto del whitepaper di ChainLink, https://chain.link/whitepaper (consultato il 03/06/2022)

pria reputazione e anche una somma come deposito. In cambio, essi puntano a ricevere un incentivo economico per il fatto di condividere un'informazione attendibile. Inoltre, il sistema di oracoli offerto da ChainLink implementa un meccanismo reputazionale basato sulle valutazioni degli utenti in merito alla verità e alla disponibilità degli oracoli.

Il progetto Chainlink, che ad oggi vanta anche una collaborazione con Google[33], è stato ritenuto uno dei più interessanti in termini di funzionalità, di possibile espansione sul mercato e per qualità dei servizi che offre nell'ecosistema blockchain e smart contract.

2.6 SMART CONTRACT E CONTRATTI TRADIZIONALI

Alla luce di quanto precede, è possibile affermare, quindi, che oggi gli smart contract sono considerati alla stregua di codici/programmi per computer inseriti in una blockchain o, più comunemente, come dei self-enforcing agreements. Essi possono contenere dei vincoli a carico delle parti che possono assumere anche rilievo giuridico. Di qui il noto interrogativo: "Gli smart contract sono dei contratti?".

Il sostantivo "contract" non deve essere ricondotto al concetto giuridico classico che con esse viene designato[34]. Lo smart contract è innanzitutto uno strumento informatico che governa in autonomia determinati accadimenti che incidono sulla relazione esistente fra due o più parti sulla base di istruzioni da esse decise. E pertanto, proprio per la necessità di istruzioni, si potrebbe affermare che non sia "intelligente" in senso proprio.

[33] https://cloud.google.com/blog/products/data-analytics/building-hybrid-blockchain-cloud-applications-with-ethereum-and-google-cloud (consultato il 10/06/2022)

[34] Lo stesso fondatore di Ethereum ha dichiarato di preferire un'espressione più tecnica come "persistent script" https://bitcoinist.com

Vengono piuttosto in luce indizi, approfonditi nel capitolo seguente specificatamente dedicato, che inducono a considerare lo smart contract uno strumento di esercizio dell'attività negoziale. Essi, potrebbero essere considerati dei contratti tradizionali che assecondano il principio della libertà contrattuale, ma per certi versi potrebbero essere dei mezzi di esecuzione del contratto.

CAPITOLO TERZO

PROFILI GIURIDICI

3.1 OSSERVAZIONI INTRODUTTIVE

Come premessa al seguente capitolo, si vuole precisare che a seconda che le blockchain siano pubbliche o private, cambieranno anche le relazioni giuridiche che si potrebbero instaurare con le medesime: le blockchain pubbliche non hanno proprietari. Risultano, infatti, dall'operare congiunto di tutti coloro che ne fanno uso. Il codice delle blockchain pubbliche è per definizione open source e la catena di blocchi si modifica continuamente in maniera automatica. Da questo punto di vista, questo tipo di blockchain sembrerebbe inquadrabile, secondo un'analisi economica del diritto, nel bene pubblico, essendo dotata delle caratteristiche di non rivalità e non escludibilità.

Discorso diverso invece per le blockchain private. In questo caso, il codice sorgente e il database sono certamente oggetto di proprietà intellettuale da parte di chi ne sia l'autore.

Per quanto riguarda gli smart contract, invece, ciò che più potrebbe rilevare sul piano civilistico, sarebbe che l'accordo qualificabile come contratto, verrebbe a perfezionarsi a monte dello smart contract, e che quest'ultimo possa rappresentare, quindi, una modalità di esecuzione del contratto.

3.2 RAPPORTI TRA BLOCKCHAIN E LEGGE: QUADRO GIURIDICO

Nei precedenti Capitoli, si è visto come la blockchain:

– sia caratterizzata dalla decentralizzazione della rete tecnologica (il software è presente su tutti i computer della rete simultaneamente);

– sia basata sulla pseudonimia di tutti gli attori (utenti, nodi, miner);

– sia basata su codice informatico open source;

– non sia soggetta al controllo unilaterale di un singolo utente/nodo/miner

essendo richiesto il consenso distribuito.

In altre parole, la tecnologia blockchain, quantomeno nelle versioni di cui al Whitepaper Bitcoin e al Whitepaper Ethereum (ossia pubblica senza permessi), consiste in un sistema decentralizzato dove gli attori coinvolti nel funzionamento, mantenimento e uso dell'infrastruttura di comunicazione, registrazione e scambio di dati sono dislocati in ogni angolo del Mondo con identità camuffate dietro stringhe alfanumeriche.

Tali caratteristiche e peculiarità pongono questioni giuridiche come, ad esempio, la responsabilità per eventi dannosi o inadempimento e la conseguente individuazione della legge applicabile.

Il quesito da porsi, dunque, è a quale tipo di responsabilità sono riconducibili i comportamenti posti in essere da, e i rapporti esistenti tra, utenti, nodi e miner tenendo presente ruoli e funzioni degli stessi:

– gli utenti usano la blockchain per trasferire e salvare dati;

– i nodi permettono il funzionamento della rete mantenendo una replica del registro;

– i miner validano le transazioni tra utenti registrandole in un blocco della blockchain attraverso il meccanismo di consenso distribuito.

Tuttavia, in un paradigma decentralizzato, disintermediato e pseudonimo, quindi, ogni utente è responsabile dei propri comportamenti e non ha la possibilità di far affidamento sull'intervento di un soggetto terzo garante per correggere propri errori o rimediare a comportamenti di altri utenti.

Risulta evidente come decentralizzazione, disintermediazione e pseudonimia comportino un cambiamento radicale dal punto di vista della responsabilità perché la blockchain trasferisce la responsabilità dai soggetti che permettono il funzionamento

della tecnologia (nodi e miner) ai soggetti che usano la tecnologia (utenti). In altre parole, è l'utente stesso a essere responsabile del proprio utilizzo e del proprio operato sulla blockchain. Questo è dunque l'elemento centrale del menzionato cambio di paradigma: l'utente non può chiedere assistenza a nessun terzo garante o intermediario che possa sopperire a un malfunzionamento, a un inadempimento o a un errore.

Le difficoltà e i dubbi giuridici qui visti in merito alle blockchain pubbliche senza permessi paiono di più facile superamento con l'utilizzo di blockchain di tipo permissioned o private. In queste, infatti, è richiesta l'identificazione degli attori partecipanti, circostanza che semplificherebbe l'attribuzione di responsabilità. Verrebbero superate anche le ambiguità giuridiche e le difficoltà pratiche viste per le ipotesi di malfunzionamento ed errore, e ciò in quanto i singoli nodi, i miner e gli utenti sarebbero identificati e in numero definito, sorretti da accordi contrattuali chiari con una riconducibilità apparentemente priva di asperità e frizioni rispetto ai principi di responsabilità tradizionali previsti nel nostro ordinamento giuridico.

Questa tecnologia consente strutture ed applicazioni sconosciute nel mondo del diritto, e le cui potenzialità innovative potrebbero portare benefici alla comunità. Pertanto, al fine di non frenare l'innovazione all'interno di schemi tradizionali, alcuni paesi hanno avviato delle iniziative specifiche (es. la UK Financial Conduct Authority inglese o il Global Blockchain Council istituito a Dubai) in cui le aziende ed i soggetti che utilizzano la tecnologia blockchain sono invitati a partecipare, all'interno di un contesto che non è ancora regolamentato, ma che viene supervisionato dalle autorità, per comprendere come intervenire e regolare le nuove fattispecie.

La stessa European Securities and Market Authority ("ESMA")[35] ha ritenuto che, considerato lo stadio di sviluppo di tale tecnologia, l'adozione di un testo normativo

[35] https://www.esma.europa.eu/press-news/esma-news/esma-assesses-usefulness-distributed-ledger-technologies (consultato il 12/06/2022)

specificatamente riservato alla disciplina delle applicazioni della blockchain sarebbe risultato controproducente e che dovrebbe trovare applicazione la normativa generale posta a salvaguardia del buon funzionamento del mercato[36]. Occorre però dire che gli Stati nazionali hanno ritenuto di procedere diversamente, promuovendo degli interventi normativi orientati a disciplinare alcune applicazioni di tale tecnologia. La matrice di tale interesse presso gli ordinamenti nazionali risiede con buona probabilità nell'intento di attrarre, attraverso la predisposizione di un quadro normativo e regolamentare specifico, gli investimenti legati all'evoluzione della tecnologia blockchain, soprattutto nel mercato finanziario (quali, in primo luogo, il mercato delle criptovalute). È possibile menzionare l'esperienza dello Stato americano del Tennesse, in cui si è recepito il bisogno di una definizione quanto più liberale possibile di questi nuovi fenomeni giuridici, definendo la tecnologia dei registri distribuiti come «qualsiasi protocollo di registro distribuito e infrastruttura di supporto, compresa la blockchain, che utilizza un ambiente distribuito, decentralizzato, libro mastro condiviso e replicato, sia esso pubblico o privato, autorizzato o senza autorizzazione e che può includere l'uso di valute elettroniche o tokens come mezzo di scambio elettronico»[37].

3.3 BLOCKCHAIN E GDPR

La più recente normativa in tema di trattamento e protezione dei dati personali, il Regolamento Europeo n. 679/2016 c.d. GDPR, è stato concepito per un sistema con intermediari centralizzati, i c.d. "titolari e responsabili del trattamento", che normalmente trattano dati, con una logica "one size fits all". Questo, del resto, è il paradigma fino ad oggi applicato all'intero ecosistema dell'economia digitale, popolato

[36] ESMA,The Distributed Ledger Technology Applied to Securities Markets, https://www.esma.europa. eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf
[37] Tennessee Law on 26 March 2018, https://legiscan.com/TN/text/SB1662/2017.

da variegate tipologie di service providers che offrono servizi agli utenti e, conseguentemente, trattano i loro dati. La tecnologia blockchain tenta di creare un'economia basata sui concetti, diametralmente opposti, di decentralizzazione e disintermediazione, secondo i quali ogni individuo è padrone di sé stesso e delle informazioni che lo accompagnano. Le divergenze appaiono evidenti.

Si tenga presente che i lavori preparatori del Regolamento Europeo sulla Protezione dei dati personali sono iniziati nel 2012, anno in cui la tecnologia blockchain non era ancora conosciuta dalla maggior parte degli utenti e non destava ancora un così forte interesse. Appare tuttavia evidente che la filosofia sottostante il GDPR si riferisca ad un ecosistema centrico e non decentralizzato, dato che in tutto il Regolamento si presuppone l'esistenza di un ente centrale che determina finalità e strumenti del trattamento ed è in grado di identificare, autorizzare, monitorare costantemente i suoi responsabili. Certo è che, data la natura decentralizzata delle più importanti e diffuse blockchain permissionless, risulta veramente difficile pensare che il loro utilizzo possa essere vietato o limitato in funzione di una mancata conformità a principi dell'ordinamento. L'auspicio è che il regolatore comunitario, resosi conto della ampia diffusione dello strumento e degli innegabili benefici che esso potrebbe apportare alle attività degli utenti, trovi il modo di eliminare possibili frizioni con l'impianto regolatorio e, così facendo, ne avalli una più proficua adozione di massa.

La conformità GDPR non riguarda la tecnologia in sé, ma il suo utilizzo[38]. Lo stesso GDPR non intende vietare, di principio, alcun trattamento, ma impone che per ciascun trattamento, anche potenziale, i titolari abbiano eseguito una "valutazione" e si siano prodigati per "minimizzare" eventuali rischi. La tecnologia è solitamente neutra ed

[38] Tema già affrontato anche da The European Union Blockchain Observatory & Forum, Blockchain and GDPR https://www.eublockchainforum.eu

autodeterminata e, conseguentemente, non risente delle norme: sono i soggetti che utilizzano tale tecnologia che si devono porre il problema e verificarne l'applicabilità.

Il GDPR, quindi, pur astrattamente applicabile, vedrebbe un difficile adattamento, soprattutto in riferimento alla pseudonimia garantita dai protocolli blockchain. Inoltre, per sua stessa natura, la blockchain non permetterebbe il soddisfacimento in maniera definitiva di alcuni diritti riconosciuti agli interessati dal GDPR, nello specifico il diritto alla cancellazione (c.d. diritto all'oblio) e alla rettifica dei dati, per via delle sue intrinseche caratteristiche di immutabilità e pubblicità.

Con l'intento di risolvere a monte questo problema, la CNIL (la Commission nationale de l'informatique et des libertés, cioè l'autorità garante per la protezione dei dati personali in Francia) nel documento esplicativo emesso a novembre 2018 e intitolato "Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data" ha ritenuto di poter applicare, nella maggioranza dei casi, l'esenzione dalle norme del Regolamento prevista all'art. 2 comma 2, lettera c) per i trattamenti cosiddetti domestici[39]: tale esenzione permetterebbe di non considerare i trattamenti svolti dai privati come ricadenti sotto le rigide disposizioni di cui al GDPR e, pertanto, di non dover considerare i nodi (ove gestiti da utenti non professionali) veri e propri responsabili del trattamento. Stesso ragionamento varrebbe per i c.d. miners, che, secondo tale interpretazione, sarebbero solo dei validatori di transazioni altrui e, in quanto tali, non essendo in grado di determinare né le finalità né i mezzi di trattamento, non ricoprirebbero alcun ruolo di responsabilità.

La presenza e lo sviluppo di nuovi operatori che forniscono servizi agli utenti dei sistemi blockchain pongono nuovi interrogativi e necessitano di soluzioni che non dovranno arenarsi sulla ricerca di figure simili in un sistema centralizzato, ma

[39] CNIL (Commission National Informatique et liberté), Premiers éléments d'analyse de la Blockchain, reperibile all'indirizzo https://www.cnil.fr/sites/default/files/atoms/files/lablockchain.pdf

comprenderne l'intima natura al fine di attualizzare e riempire di contenuto i principi alla base del GDPR quale applicazione della Carta dei Diritti Fondamentali dell'Unione Europea. Inoltre, come già è stato per la rete Internet, anche per la blockchain sarà necessario raggiungere la consapevolezza che si tratti di un luogo virtuale, impermeabile ai confini, nel quale ogni attore volontariamente decide di partecipare, così accettando di sottostare alle relative regole condivise.

Al contrario di una tradizionale applicazione web, i cui dati sono conservati in un server centrale, in *blockchain* le informazioni sono distribuite nel network. Quindi, mentre normalmente queste ultime sono disponibili solo alle parti del rapporto e ad un terzo intermediario, la trasparenza della *blockchain* le rende accessibili ad un più vasto numero di soggetti[40]. Se, dunque, come visto, natura distribuita e trasparenza possono fungere da elementi positivi per la tutela dei dati degli utenti, dall'altra ne possono divenire anche una minaccia. Più precisamente, la replica dei dati nelle varie copie della *blockchain*, scaricate nei server dei nodi estranei alle finalità per cui i medesimi sono stati condivisi: confligge con il principio di minimizzazione dei dati, per cui si richiede che essi siano "*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*"; rende più complesso per gli interessati esercitare un adeguato controllo sui propri dati. Ne deriva una tensione anche con i principi di *Data Protection by Design* e *Accountability*[41].

A riguardo è stato obiettato che: le chiavi pubbliche, che fungono da accounts per i partecipanti, appaiono sotto forma di lettere e numeri casualmente disposti, per cui l'identità del soggetto sottostante rimane nascosta; i dati contenuti nei blocchi sono normalmente criptati, oltre al fatto che ogni singolo blocco ed ogni singola transazione

[40] M. Berberich, M. Steiner, Blockchain technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers? op. cit., 425.

[41] H. Chang, Blockchain: Disrupting data protection? 150 Privacy Laws & Business International Report, SSRN, 2017, 2.

sono identificabili mediante *hash*. In sostanza, non si dovrebbe porre la questione della protezione dei dati personali, in quanto si tratterebbe di dati anonimi[42], come tali nemmeno sottoposti all'applicazione del GDPR[43].

Ora, se è vero che le informazioni non appaiono in chiaro, è anche vero che esistono delle tecniche, alcune più avanzate, altre banali, per risalire al dato.

Quanto alle chiavi pubbliche, non è remota la possibilità di ricollegare l'indirizzo ad una specifica identità[44]. Ad esempio: quando l'indirizzo viene pubblicizzato su una pagina personale, come un blog o un sito web, oppure su un forum o un social network; se l'operazione da compiere consiste nello scambio di criptomonete, quando queste vengono scambiate[45] con valuta corrente[46]. Ci sono, poi, forme sempre più evolute (ed efficaci) di *blockchain analytics*[47], che vengono anche utilizzate per scovare attività illecite che si celano dietro indirizzi apparentemente anonimi, quali il riciclaggio di denaro sporco[48]. Una volta rivelato il proprietario della chiave, è possibile risalire alla storia delle transazioni che lo riguardano[49].

---

42 Ex art. 1 Reg., oggetto dello stesso è la protezione dei "dati personali", i quali vengono definiti ex art. 4, par. 1, n. 1, come "qualsiasi informazione riguardante una persona fisica identificata o identificabile". Se la persona fisica non è identificata, né identificabile, il dato non è personale, ma anonimo. Pertanto, i dati anonimi non vengono tutelati dal GDPR, come anche esplicitato dal cons. n. 26 ("I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazione che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche e di ricerca"). V. C. DelFederico, A. R. Popoli, Disposizioni generali, in G. Finocchiaro (a cura di), Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali, op. cit., 65.

43 N. Fabiano, The Internet of Things ecosystem: the blockchain and privacy issues. The challenge for a global privacy standard, Advances in Science, Technology and Engineering Systems Journal, Vol. 3, No. 2, 2018, 5.

44 Esistono, infatti, piattaforme di exchange di criptovalute, di cui la più nota è Coinbase per i bitcoin.

45 J. Barcelo, User Privacy in the Public Bitcoin Blockchain, Journal of Latex Class Files, Vol. 6, No. 1, January 2007, 2.

46 Ad esempio, in Bitcoin si può sfruttare l'usuale comportamento dei portafogli di bitcoins e dei cd "change addresses" ("indirizzi per i resti"). Per un approfondimento v. J. Barcelo, User Privacy in the Public Bitcoin Blockchain, op. cit., p. 3.

47 Alcune aziende, come Coinalytics, Coinometrics o Elliptic ne hanno fatto una fonte di business. V. P. DeFilippi, The interplay between decentralization and privacy: the case of blockchain technologies, op. cit., 12.

48 S. Capaccioli, Criptovalute e bitcoin: un'analisi giuridica, op. cit., 29.

49 Article 29 DataProtectionWorkingParty, Opinion 05/2014 on Anonymisation Techniques, 10 aprile 2014, 20. Secondo il WP29, i dati criptati possono essere decifrati mediante la semplice conoscenza della chiave privata; per quanto riguarda la funzione di hash, seppure la reidentificazione sia più difficile (perché restituisce un output di dimensione fissa a partire da un input di qualsiasi dimensione, ed il

Per quanto concerne il contenuto dei blocchi, inoltre, occorre considerare che lo stesso Gruppo di lavoro articolo 29 ha escluso che tanto la funzione di *hash* che la crittografia siano completamente anonime, ritenendole piuttosto pseudoanonime[50].

La pseudonimizzazione si distingue dall'anonimizzazione perché la seconda non rende possibile *in toto* la re-identificazione, mentre la prima maschera l'identitaà, a cui si può però risalire utilizzando "*informazioni aggiuntive*"[51]. Per questo, secondo il nuovo Regolamento europeo sulla protezione dei dati personali, i dati pseudoanonimi ricadono sotto la sua applicazione[52].

In conclusione, si deve negare la tesi per cui i dati racchiusi in *blockchain* siano anonimi, dovendosi più correttamente discorrere di pseudoanonimato[53].

Il fatto che i dati siano pseudoanonimi significa dover prevedere anche per questi i principi di *Accountability*, di *Data Protection by Design* e di minimizzazione.

Per attenuare la tensione, di cui si è dato conto all'inizio del paragrafo[54], tra le caratteristiche della *blockchain* e i principi in questione, sono state avanzate varie proposte.

Un primo gruppo di proposte attiene a degli accorgimenti tecnici o a delle forme di implementazione della tecnologia. Per prevenire l'identificazione del titolare della chiave pubblica, si va dagli espedienti più semplici, quali l'utilizzo di indirizzi "usa e

processo non può essere invertito), sarebbe tuttavia ipotizzabile eseguendo l'hash di tutti i valori di input possibili e confrontando i risultati.

[50] Art. 4, par. 1, n. 5.

[51] La definizione di "pseudonimizzazione" è nuova.

[52] Di uguale avviso anche il Parlamento europeo, con la già citata Risoluzione 2017/2772 del 3 ottobre 2018 (v. cons. D e par. 28).

[53] Cioè si utilizza un account diverso per ogni operazione da compiere, cosicché sia più arduo ricostruire la storia delle transazioni di un medesimo soggetto. J. Barcelo, User Privacy in the Public Bitcoin Blockchain, op. cit., 3.

[54] BLOCKCHAIN E PROTEZIONE DEI DATI PERSONALI, Diritto dell'Informazione e dell'Informatica (Il), fasc.3, 1 GIUGNO 2019, pag. 619, Alberto M. Gambino,Chantal Bomprezzi

getta"[55], ad altre tecniche, come il ricorso a "*mixing systems*"[56], "*ring signatures*", "*zero-knowledge proofs*" o l'aggiunta di "rumore" ai dati[57]. Per mettere al sicuro il contenuto dei blocchi, invece, si potrebbe pensare di conservare i dati *off-chain*, creando un collegamento alla blockchain attraverso un puntatore di *hash*.

Un'altra soluzione potrebbe risiedere nell'adozione di *blockchain permissioned* invece che *permissionless*, in cui un'attenta selezione di chi accede alla piattaforma e di chi può visionare la *blockchain* rende l'intero sistema molto più facilmente controllabile[58].

Si ritiene che il rischio non risieda tanto nella distribuzione dei dati personali in molteplici copie, quanto nel fatto che tali copie sono rinvenibili in nodi detenuti da soggetti sconosciuti. Qualora la blockchain non si dimostrasse sufficientemente in grado di preservare la condizione di pseudoanonimoa dei dati personali *ivi* racchiusi, tali dati personali potrebbero essere trattati in modo indiscriminato, ben oltre le finalità legittime di trattamento.

Secondo quanto prescritto all'art. 4, par. 1, n. 5, del GDPR, le informazioni aggiuntive necessarie per la re-identificazione devono essere "*soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona identificata o identificabile*"; inoltre, a mente del considerando 26 del Regolamento, "*Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o*

---

[55] Con questi sistemi si spezza il legame tra portafoglio che esegue il pagamento (che ottiene le valute da più utenti) e portafoglio del soggetto pagante (UK GovernmentChiedScientificAdviser, Distributed Ledger Technology: beyond block chain, Government Office for Science, 2016, 51). Ad esempio, nella comunità Bitcoin si chiama CoinJoin.

[56] Con le "ring signatures" ogni firma digitale è riconducibile ad un gruppo di utenti, senza specificare quale. Quando si parla di "zero knowledge proof", invece, si intende una tecnica crittografica per cui è possibile provare che una proposizione è vera, senza dover rivelare alcuna informazione ulteriore; Zcash, ad esempio, è una blockchain pubblica che permette di evitare il problema del double spending money senza dover individuare mittente, destinatario e ammontare della transazione. Infine, si aggiunge "rumore" ai dati quando si raggruppano più transazioni per far sì che dall'esterno sia impossibile discernere le identità. M. Finck, Blockchains and Data Protection in the European Union, op. cit., 15.

[57] M. Finck, Blockchains and Data Protection in the European Union, op. cit., 11.

[58] Di questo avviso anche la Commission Nationale Informatique & Libertés francese (CNIL, La Blockchain: quelles solutions pour un usage responsable en présence de données personelles?, 2018, 6).

indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici". Dalle suddette disposizioni si deduce che, anche se i dati in *blockchain* sono pseudoanonimi, i principi di *Accountability*, *Data Protection by Design* e minimizzazione si possono ritenere soddisfatti qualora si possa valutare la *blockchain* sufficientemente sicura, tenuto conto di vari parametri obiettivi, quali, appunto, i costi e il tempo che si dovrebbero dedicare per riuscire nell'intento dell'identificazione, a seconda delle tecnologie disponibili nel dato momento storico.

Tenuto conto della giovinezza della tecnologia, e delle sperimentazioni ancora in corso, è ancora altamente improbabile che il ricorso ad una *blockchain permissionless* possa assicurare una ragionevole improbabilità di re- identificazione. A tal fine, per spronare gli investitori nello sviluppo di soluzioni di tal fatta nel rispetto del GDPR, occorrerà attendere maggiori indicazioni dalle istituzioni competenti.

Quel che risulta piuttosto chiaro al momento è che l'opzione di raccolta di dati personali in *blockchain* classiche è altamente sconsigliabile.

Si è già sottolineata, inoltre, l'importanza del ruolo e dei compiti di titolare e responsabile del trattamento, che con il nuovo Regolamento europeo sulla protezione dei dati personali assumono ancora maggior rilievo[59].

Il titolare del trattamento diviene tale di fatto, senza una specifica formalità prescritta dalla legge, per cui saranno le circostanze a far comprendere chi determini "*finalità e mezzi del trattamento*"[60], assumendo la responsabilità dell'osservanza delle norme a protezione dei dati personali. Con "*finalità*" si intende il "perché" del trattamento, mentre con "*mezzi*" il "come", vale a dire i mezzi tecnici ma anche organizzativi del

[59] G. Finocchiaro, Privacy e protezione dei dati personali, Zanichelli, 2012, 80.

[60] V. C. DelFederico, A. R. Popoli, Disposizioni generali, in G. Finocchiaro (a cura di), Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali, op. cit., 88-89.

trattamento (ad esempio, chi può avere accesso ai dati)[61]. È possibile che più soggetti siano titolari del trattamento (o contitolari)[62]. Il responsabile del trattamento, invece, è la figura che "*tratta dati personali per conto del titolare del trattamento*"[63], per cui si ritiene che non possa decidere le finalità o gli aspetti fondamentali del come del trattamento (che spettano esclusivamente al titolare)[64]. In sintesi, è un soggetto che agisce su delega del titolare, con funzioni a questo strumentali e di ausilio, attraverso un atto di designazione[65] ad opera del titolare che ne disciplina gli adempimenti.

Ciò premesso, l'individuazione del titolare del trattamento non è sempre immediata con riferimento alla *blockchain*, a mente del suo carattere distribuito, di disintermediazione e di pseudoanonimato dei partecipanti[66].

Per la verità, il compito non è così complicato qualora si sia optato per *blockchain* totalmente private, in cui il titolare del trattamento dovrebbe coincidere con il gestore dell'infrastruttura, a cui spetterebbe determinare finalità e mezzi del trattamento[67]. Nelle *blockchain permissioned*, il soggetto o i soggetti che stabiliscono i criteri di selezione negli accessi e il grado di trasparenza della *blockchain* sono in grado di monitorare i nodi e le loro attività. Si potrebbe affermare, dunque, che ai medesimi spetti il ruolo di titolari (contitolari in caso di più soggetti, come ad esempio un consorzio)[68]. Sia per le une che per le altre, il responsabile sarà poi nominato dal titolare del trattamento.

---

61 Art. 26 Reg.
62 Art. 4, par. 1, n. 8.
63 V. C. DelFederico, A. R. Popoli, Disposizioni generali, in G. Finocchiaro (a cura di), Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali, op. cit., 89 ss.
64 Art. 28 Reg.
65 T. Lyons, L. Courcelas, K. Timsit, Blockchain and the GDPR - a thematic report prepared by the European Union Blockchain Observatory and Forum, 16 ottobre 2018 (https://www.eublockchainforum.eu/reports), 17.
66 J. Moser, The Application & Impact of the European General Data Protection Regulation on Blockchains, R3 Reports, 2017, 9. Il titolare del trattamento potrebbe affidare ad un altro soggetto la costruzione dell'infrastruttura, che potrebbe assumere il ruolo di responsabile del trattamento.
67 J. Moser, The Application & Impact of the European General Data Protection Regulation on Blockchains, op. cit., 9.
68 C. Bomprezzi, Blockchain e assicurazione: opportunità e nuove sfide, in Diritto, Mercato, Tecnologia, 7 luglio 2017, 29.

Maggiori difficoltà si rinvengono qualora la *blockchain* sia di tipo "*permissionless*", perché non è dato individuare un'entità deputata a governare il sistema e ad assumere decisioni strategiche[69]. I nodi sono uguali tra loro, senza limitazioni d'accesso, senza pre-identificazione, senza predeterminazione a monte degli usi (e quindi delle finalità) per cui la *blockchain* è stata concepita. Data la particolarità del caso, sono state teorizzate due ricostruzioni, opposte tra loro. Secondo la prima[70], tutti i nodi sarebbero titolari, indipendentemente l'uno rispetto all'altro, perché a questi corrispondono degli utenti che, in autonomia e volta per volta, inseriscono dati che vengono trattati per una particolare finalità; i nodi che non prendono parte alla singola operazione, invece, sarebbero da qualificarsi alla stregua di responsabili, giacché, detenendo copia dei dati e contribuendo al mantenimento di questi nel registro, sono strumentali e di ausilio al trattamento. In altre parole, ogni nodo sarebbe titolare per sé, e responsabile per gli altri[71]. Ad opinione della seconda[72], differentemente, titolare non sarebbe nessuno, perché nessun nodo è in grado di stabilire nel complesso le finalità del trattamento, né gli aspetti fondamentali riguardanti i mezzi, e parimenti nessuno di questi è posto nelle condizioni di poter gestire e dominare tutto il network; non ci sarebbero, dunque, le precondizioni per potersi assumere qualsiasi responsabilità o assolvere al principio di *Accountability*.

Caratteristica peculiare della *blockchain* è che i dati racchiusi in blocchi vengono dapprima aggiunti alla catena da un *validation node*, venendo successivamente replicati in copia tra i vari nodi. I suddetti nodi potrebbero infatti trovarsi ovunque[73]. La

---

[69] J. Moser, The Application & Impact of the European General Data Protection Regulation on Blockchains, op. cit., 10.

[70] W. Maxwell, J. Salmon, A guide to blockchain and data protection, op. cit., 11.

[71] M. Finck, Blockchains and Data Protection in the European Union, op. cit., 17; M. Berberich, M. Steiner, Blockchain technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers?, op. cit., 424.

[72] Si è detto, infatti, che la blockchain è unilateralmente immodificabile.

[73] Il GDPR non fornisce una definizione di "trasferimento", la quale è stata elaborata per differenza rispetto al concetto di "comunicazione": con il secondo, si intendono gli spostamenti di dati tra titolari, all'interno dell'Unione; con il primo, i movimenti di dati tra soggetti, titolari o responsabili, purché uno di essi localizzato fuori dai confini europei. V. M. C. Meneghetti, Trasferimenti di dati personali, in G.

domanda che sorge spontanea è, dunque, se si possa parlare di "trasferimento"[74] dei dati personali ivi contenuti, quando i nodi si trovino in un territorio *extra*-UE, ai sensi degli artt. 44 ss. del GDPR[75].

Si ritiene che sulla questione si possa operare un parallelismo rispetto alla vicenda indagata dalla Corte di giustizia europea nella sentenza *Bodil Lindqvist*[76].

Con il suddetto provvedimento, i giudici hanno stabilito che "*non si configura un trasferimento verso un paese terzo di dati...allorchè una persona che si trova in uno Stato membro inserisce in una pagina Internet — caricata presso il suo fornitore di servizi di ospitalità ("web hosting provider"), stabilito nello Stato stesso o in un altro Stato membro — dati personali, rendendoli così accessibili a chiunque si colleghi ad Internet, compresi coloro che si trovano in paesi terzi*". La Corte ha negato, in tale caso, che l'inserimento di dati personali in un sito web possa essere qualificato come "trasferimento" per il fatto che al medesimo possono avere accesso destinatari situati al di fuori dell'Unione europea, perché "*i dati personali che giungono al computer di una persona che si trova in un paese terzo, provenienti da una persona che li ha caricati su un sito Internet, non sono stati trasferiti direttamente tra queste due persone, ma attraverso l'infrastruttura informatica del fornitore di servizi di ospitalità presso il quale la pagina è caricata*"[77].

Il ragionamento potrebbe essere esteso alla *blockchain*. In blockchain i dati contenuti nei blocchi potrebbero essere acceduti da chiunque ne sia autorizzato, dai vari nodi in cui la *blockchain* è replicata, i quali potrebbero essere situati anche in Paesi terzi. Anche qui, i dati non sono trasferiti direttamente, ma all'esito di un processo di validazione e successiva replica nei nodi della *blockchain*.

Finocchiaro (a cura di), Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali, op. cit., 436.

[74] M. Finck, Blockchains and Data Protection in the European Union, op. cit., 19; M. Finck, Blockchain regulation and Governance in Europe, op. cit., 102-103.

[75] W. Maxwell, J. Salmon, A guide to blockchain and data protection, op. cit., 16.

[76] Corte di giustizia europea, C-101/01, Bodil Lindqvist, 6 novembre 2003, www.curia.europa.eu.

[77] M. C. Meneghetti, Trasferimenti di dati personali, in G. Finocchiaro (a cura di), Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali, op. cit., 441-442.

La decisione della Corte di giustizia europea è stata aspramente criticata. Oltretutto, essa non ha chiarito se il trasferimento sia escluso anche qualora: non ci si limiti all'*upload*, ma i dati vengano scaricati dal soggetto stabilito nel Paese terzo; il *server* dell'*hosting provider* sia situato in un Paese terzo[78]. Dare risposta a queste due domande sarebbe molto importante in ambito *blockchain*, posto che la copia della blockchain viene ottenuta mediante *download* del singolo nodo, mentre, come già affermato, il *validation node* che si occupa dell'inserimento del nuovo blocco potrebbe essere localizzato anche al di fuori dell'Unione europea.

Nel caso in cui si possa propendere per la tesi del trasferimento, si ripropone la distinzione tra *permissionless* e *permissioned blockchain*, posto che nel primo tipo la mancata conoscenza dell'identità dei soggetti che si celano dietro i nodi non è conosciuta, né la loro localizzazione, per cui non si potrebbe discernere tra Paese membro o Paese terzo[79]. Gli articoli 46 e 47 del GDPR non sarebbero applicabili. Uno studio[80] ha proposto in proposito l'applicazione delle deroghe di cui all'art. 49 del GDPR, in particolare la richiesta del consenso dell'interessato al trasferimento previa informativa dei rischi derivabili dal trasferimento medesimo. Lo studio ha altresì evidenziato che sarebbe comunque problematico acquisire detto consenso in presenza di una *blockchain permissionless*.

Inoltre, la conservazione perpetua dei dati in *blockchain* confligge con il principio di limitazione della conservazione, per cui i dati vanno "*conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per*

---

[78] J. Moser, The Application & Impact of the European General Data Protection Regulation on Blockchains, op. cit., 10.

[79] L'art. 46 del GDPR statuisce che "Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche".

[80] Probabilmente per l'asserita difficoltà di individuazione del titolare del trattamento che dovrebbe raccogliere il consenso dell'interessato al trasferimento.

le quali sono trattati"[81]. L'immutabilità di *blockchain* rende difficoltoso anche l'esercizio del diritto di cancellazione dei dati[82], di cui all'art. 17 Reg.

Dal lato informatico, si stanno sperimentando delle tecniche per ovviare all'immutabilità della blockchain. Ad esempio, l'uso di "*chameleon hash*" (o "*hash* camaleonte"), che consentirebbe di mantenere inalterato l'*hash* pur effettuando cambiamenti nel blocco[83]. Ma ciò potrebbe andare a discapito della sicurezza del sistema.

Va sottolineato che le problematiche derivanti dall'immutabilità unilaterale della *blockchain* qui esaminate vengono smorzate qualora si ricorra alla tipologia *permissioned*[84]. Sono di fatto annullate in presenza di blockchain private.

Le stesse considerazioni valgono anche per il diritto alla rettifica[85], che implica delle modifiche al contenuto della *blockchain*.

Infine, lo stesso esercizio dei già menzionati principi e diritti sarebbe precluso qualora si ammettesse l'impossibilità di identificare un titolare del trattamento[86].

Sul diritto di accesso, in caso di *blockchain permissionless* è stata evidenziata in primo luogo la già più volte ribadita difficoltà di individuazione del titolare del trattamento, a cui rivolgere richiesta di accesso ai dati personali. Nel caso ciò sia possibile, sarebbe poi complesso per il titolare del trattamento conoscere se, e in caso affermativo, quali dati personali siano trattati, poiché i medesimi sarebbero coperti dalla crittografia asimmetrica.

---

[81] T. Roughton, P. Bidewell, Smart insurance contracts, Pinsent Masons, 2017, 9.

[82] Per cui il diritto alla cancellazione sussiste se "i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati".

[83] A. Ricci, I diritti dell'interessato, in G. Finocchiaro (a cura di), Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali, op. cit., 198-199.

[84] Ex art. 16 Reg., "l'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo".

[85] M. Finck, Blockchains and Data Protection in the European Union, op. cit., 21 ss.; M. Finck, Blockchain regulation and Governance in Europe, op. cit., 104- 105.

[86] M. Finck, Blockchains and Data Protection in the European Union, op. cit., 29-30. M. Finck, Blockchain regulation and Governance in Europe, op. cit., 105- 106.

Sul punto, si obietta che la blockchain non dovrebbe ostacolare, ma anzi potrebbe garantire il diritto di accesso dell'interessato. Nell'ipotesi in cui un soggetto titolare del trattamento si ritrovi a raccogliere dati personali per una determinata finalità, infatti, sarebbe in grado di conoscerli per il fatto stesso di averli trattati. Come descritto in precedenza nell'enunciare le potenzialità della blockchain per una migliore protezione dei dati personali degli utenti[87], le caratteristiche di tracciabilità e trasparenza della tecnologia consentirebbero al titolare del trattamento di ripercorrere i trattamenti effettuati, in favore dell'interessato[88].

In conclusione, gli investimenti in applicazioni *blockchain* stanno crescendo in maniera esponenziale, tanto che il World Economic Forum ha stimato che entro il 2027 rappresenteranno il 10% del prodotto interno lordo globale. La *blockchain*, infatti, si pone in linea con i bisogni odierni di velocità, efficienza, semplificazione, ma anche di sicurezza e trasparenza propri della moderna società dell'Informazione.

Anche nell'ambito della protezione dei dati personali, sono già state evidenziate le potenzialità della tecnologia, in termini di un maggiore e migliore controllo dei propri dati personali da parte degli individui, oltre che di un più elevato livello di garanzia di integrità del dato. A queste, tuttavia, si affiancano delle possibili ripercussioni negative sulla protezione dei dati personali, a mente delle stesse caratteristiche della tecnologia, quali la natura distribuita e decentralizzata, o l'immutabilità[89].

Ciò non dovrebbe implicare un totale rifiuto della *blockchain*, il che è testimoniato anche dalla grande attenzione che le istituzioni europee stanno dimostrando verso il

---

87 L. D. Ibáñez, K. O'Hara, and E. Simperl, On Blockchains and the General Data Protection Regulation, op. cit., 11.

88 WorldEconomicForum, GlobalAgendaCouncilOnTheFutureOfSoftware & Society, Deep Shift, Technology Tipping Points and Societal Impact, Survey Report, settembre 2015, 24.

89 www.eublockchainforum.eu. L'Osservatorio ha organizzato a Bruxelles un primo workshop sul tema, dal titolo "Opposites attract: Reconciling GDPR and blockchain", il giorno 8 giugno 2018. Successivamente, è stato prodotto anche un report, in cui è stato affermato che il GDPR non può rappresentare la fine della blockchain, e che le tensioni possono essere allentate mediante l'intervento del legislatore, dello European Data Protection Board e della giurisprudenza (T. Lyons, L. Courcelas, K. Timsit, Blockchain and the GDPR - a thematic repot prepared by the European Union Blockchain Observatory and Forum, op. cit., 28).

fenomeno, con l'istituzione di un Osservatorio e Forum dell'Unione Europea sulla Blockchain[90] e una grande quantità di finanziamenti dal programma Horizon 2020 per la ricerca nel settore; inoltre, l'innovazione tecnologica rientra tra gli obiettivi dell'Unione europea al pari della protezione dei dati personali, per favorire la crescita economica e creare occupazione. Invero, come anche affermato dal Garante europeo della protezione dei dati nel Report annuale per l'anno 2017, e confermato nel 2018, occorrerebbe monitorare le nuove tecnologie, traendo da queste i maggiori benefici senza rinunciare ad un'opportuna regolamentazione[91]. In altri termini, si dovrebbe puntare a sviluppare delle soluzioni *blockchain* che siano *privacy-friendly*.

Tale obiettivo potrebbe essere perseguito lavorando a più livelli, dal lato tecnologico così come da quello legale.

Relativamente al primo, si è già fatto cenno alle evoluzioni della tecnologia che permetterebbero, ad esempio, di prevenire la re-identificazione, o di ovviare all'immodificabilità unilaterale di *blockchain*, talvolta dovendo rinunciare parzialmente agli aspetti cardine che ne hanno sorretto la nascita, come la disintermediazione o l'anonimato[92].

Quanto al secondo, occorrerebbe dapprima creare un vocabolario comune, che definisca cosa sia una *blockchain*, le sue caratteristiche e le sue varianti[93]. Ad oggi, infatti,

---

[90] La politica dell'innovazione dell'Unione europea trova le proprie basi giuridiche negli artt. 173 e da 179 a 190 del Tfue. Per creare un vero mercato unico dell'innovazione l'UE ha inserito tra le iniziative della strategia Europa 2020 l'"unione dell'innovazione". M. Finck, Blockchains and Data Protection in the European Union, op. cit., 29.

[91] EuropeanDataProtectionSupervisor, Annual report 2016, 43.

[92] H. Halpin, M. Pietraska, Introduction to Security and Privacy on the Blockchain, 2nd Ieee European Symposium on Security and Privacy Workshops, aprile 2017, Parigi, 1-3, (https://www.ieeesecurity.org/TC/EuroSP2017/).

[93] All'interno dell'Unione europea, alcuni Stati membri hanno avanzato delle definizioni di blockchain al fine del riconoscimento della tecnologia per determinate applicazioni, in particolare in ambito Fintech. Tra i primi, si ricordano Malta, che il 4 luglio 2018 ha approvato tre leggi in materia (Malta Digital Innovation Law Act, Innovative Technology Arrangement and Services Act, Virtual Financial Assets Act) e la Francia, con due Ordinanze sulla registrazione ed il trasferimento di titoli finanziari non quotati mediante blockchain (Ordonnance n. 2016-520 du 28 avril 2016 relative aux bons de caisse e Ordonnance n° 2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers).

è complesso sviluppare ragionamenti unitari circa il rapporto tra *blockchain* e GDPR, poiché infinite sono le architetture *blockchain*, create di volta in volta da sviluppatori o start-up per questo o quel caso d'uso. Timidi tentativi in tale direzione si stanno realizzando. In Italia, l'art. 8-*ter* della legge n. 12 dell'11 febbraio 2019 (di conversione del decreto-legge n. 135 del 14 dicembre 2018, denominato "Decreto Semplificazione") fornisce la definizione di "tecnologie basate su registri distribuiti"[94]. In aggiunta, le istituzioni competenti dovrebbero fornire maggiori indicazioni in termini di *compliance* della tipologia blockchain utilizzata con il GDPR, soprattutto se *permissionless,* le quali, come visto, sono quelle che al momento presentano i maggiori interrogativi. Ad esempio, occorrerebbe chiarire quali soluzioni *permissionless* garantiscano, a partire dal dato pseudonimizzato, una ragionevole improbabilità di re-identificazione. La determinazione di appositi *standards* potrebbe soccorrere al riguardo[95]. Iniziative in questo senso dovrebbero comunque essere concertate almeno a livello di Unione Europea.

3.4 LEGGE APPLICABILE AGLI SMART CONTRACT

Con il termine "*smart contract*", quindi, si intende l'incorporazione nel *software* di clausole contrattuali con esecuzione automatica ed indipendente dall'intervento umano. Caratteristiche che, unite a quelle della blockchain – decentralizzazione, distribuzione, immodificabilità – consentono un *"enforcement"* delle obbligazioni contrattuali rendendone impossibile l'inadempimento. È stata, quindi, la tecnologia blockchain a

[94] Nella Risoluzione del Parlamento europeo del 3 ottobre 2018, al par. 33, dopo aver sottolineato l'importanza della conformità degli usi della blockchain rispetto alla legislazione europea in materia di protezione dei dati personali, in primis al GDPR, si invitano la Commissione e il Garante europeo della protezione dei dati a fornire ulteriori orientamenti sul punto.
[95] Citando ancora la Risoluzione del Parlamento europeo del 3 ottobre 2018, i paragrafi 41 e 42 sottolineano l'importanza della collaborazione con le organizzazioni internazionali.

dare piena attuazione a quella che nel 1996 era una visione da parte di Szabo, in quanto il network, con le sue caratteristiche intrinseche, assicura l'esecuzione del contratto trasposto nel codice software.

Le prime discipline, in ambito smart contract, sono state emanate negli USA, dove in generale si registra una reazione positiva all'uso di nuove tecnologie. Discipline sono state emanate, o sono in corso di emanazione, negli stati del Vermont, Ohio, Arizona. Soprattutto nello stato del Tennesse, la Senate Bill n. 1662 del 26 marzo 2018, modificando il Tennesse Code, ha inserito la definizione di "Distributed Ledger technology" e regolato anche gli smart contract. Essi sono definiti programmi informatici basati su eventi, eseguiti su un registro elettronico, distribuito, decentralizzato, condiviso e replicato, ed utilizzati per automatizzare le transazioni, incluse, ma non limitatamente, le transazioni che:

- custodiscono o trasferiscono asset sul registro;
- creano e distribuiscono asset elettronici;
- sincronizzano informazioni;
- gestiscono l'identità e l'accesso degli utenti alle applicazioni.

In merito alla loro validità la disposizione chiarisce genericamente che essi devono ritenersi validi e che non si può negare efficacia legale ad un contratto unicamente perché eseguito tramite uno smart contract.

Anche il Consiglio degli Stati della Svizzera ha approvato una legge inerente DLT e blockchain. Il dispositivo normativo prende il nome di "Legge federale sull'adeguamento del diritto federale agli sviluppi della tecnologia di registro distribuito" ed è entrato in vigore il 1° agosto 2021. Questa nuova legge rappresenta un'armonizzazione fra impianti normativi già esistenti, tra cui il diritto privato internazionale, il diritto delle obbligazioni e il diritto dei titoli intermediari. Una delle novità centrali è l'autorizzazione dei sistemi di negoziazione TRD (tecnologia su

registro distribuito). Si tratta di un tipo di infrastruttura del mercato finanziario per il commercio di valori mobiliari TRD che, oltre agli intermediari finanziari, può ammettere al commercio altre imprese e persone. Con il disciplinamento esplicito della rivendicazione dei beni crittografici dalla massa fallimentare, in caso di fallimento viene aumentata anche la certezza del diritto in materia di insolvenza[96].

Attualmente, a livello internazionale, la Svizzera è tra i primi paesi a disporre di una normativa chiara, specifica e moderna che disciplini queste innovative tecnologie sul mercato finanziario.

3.5 L'INTERVENTO DEL LEGISLATORE ITALIANO

Anche il nostro legislatore ha tentato di "normare" le definizioni delle tecnologie in esame. Definizioni specifiche sono state date con l'art 8-ter del Decreto Semplificazioni del 2019, legge di conversione del D.l. 135/2018[97]. Tale articolo, rubricato "Tecnologie basate su registri distribuiti e smart contract", stabilisce quanto segue ai seguenti punti:

1) Si definiscono "tecnologie basate su registri distribuiti" le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili.

2) Si definisce "smart contract" un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti

[96] https://www.efd.admin.ch/efd/it/home/il-dff/nsb-news_list.msg-id-84035.html
[97] https://www.gazzettaufficiale.it/eli/id/2019/02/12/19A00934/sg

sulla base di effetti predefiniti dalle stesse. Gli smart contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto.

3) La memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all'articolo 41 del regolamento (UE) n.910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014.

4) Entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, l'Agenzia per l'Italia digitale individua gli standard tecnici che le tecnologie basate su registri distribuiti debbono possedere ai fini della produzione degli effetti di cui al comma 3.

Dalla lettura della norma, tuttavia, sorgono dubbi interpretativi legati probabilmente ad una definizione troppo restrittiva degli argomenti.

Una parte della dottrina[98] ha rilevato che dalla lettura del secondo comma dell'articolo 8-ter, emergerebbe il principio secondo il quale questo tipo di contratto avrebbe forza di legge fra le parti, ex art 1372 c.c. solo dal momento in cui esso verrebbe eseguito. Secondo questa interpretazione, l'accordo tra le parti circa gli effetti sarebbe un evento antecedente a quello in cui lo smart contract diventa vincolante per le parti.

Se questa interpretazione fosse accettata, ci si troverebbe davanti ad un tertium genus di formazione del contratto, ovvero la conclusione del contratto per effetto della validazione diffusa da parte dei nodi della blockchain[99]. Si deve precisare che, al

[98] Stefano CERRATO, Contratti tradizionali, diritto dei contratti e smart contract, in Blockchain e Smart Contract, a cura di Raffaele BATTAGLINI, Marco GIORDANO, Giuffrè Francis Lefebre, Milano, 2019, pagg. 300-301

[99] Stefano CERRATO, Contratti tradizionali, diritto dei contratti e smart contract, cit., pag. 301

momento in cui scrivo, questa normativa, in attesa dell'emanazione delle linee guida tecniche dell'AgID, risulta ancora non attuata. L'ampio ritardo sulla tabella di marcia non pare esser comunque giustificato da ragioni di osteggiamento politico. Infatti, a sostegno di ciò, il Presidente del Consiglio Mario Draghi, ha affermato di essere "molto interessato" alla tecnologia blockchain, definita "promettente", in quanto capace di implementare alcuni processi. Draghi aggiunge che questa "nuova promettente tecnologia probabilmente sosterrà l'economia e creerà molti benefici" ancorché risultino necessari molti approfondimenti. È pertanto auspicabile che i lavori possano concludersi celermente.

3.6 IL CONTRATTO IN FORMA SMART CONTRACT

Si può compiere una distinzione tra gli smart contract che danno esecuzione ad un accordo già intervenuto fuori dalla rete, trovandosi in questo caso dinanzi ad un mero atto di esecuzione, e smart contract che costituiscono un contratto vero e proprio. Questi potrebbero anche essere programmati da una sola delle parti.

In quest'ultima categoria potrebbero rientrare gli smart contract contenenti offerte al pubblico, i quali, ex art 1336 c.c. qualora contenessero gli estremi essenziali del contratto al quale l'offerta indirizza la conclusione, potrebbero essere considerati come delle proposte contrattuali. Tali smart contract, in quanto proposte contrattuali, diventerebbero vincolanti dal momento in cui la proposta contenuta nel codice viene accettata dall'oblato. Per esempio: se uno smart contract prevede il trasferimento di 1 BTC (then) a chiunque trasferisca all'indirizzo dello smart contract 1 ETH (if), l'accettazione in questo caso si avrebbe mediante uno jactus pecuniae (virtuale) che manifesta la volontà dell'oblato di accettare l'offerta. In tal caso la normativa di riferimento sarebbe il quarto comma dell'art 1325 c.c.: "Qualora il proponente richieda

per l'accettazione una forma determinata, l'accettazione non ha effetto se è data in forma diversa". In ogni caso, si deve notare che l'incontro delle volontà, per quanto lo smart contract sia automatico, non è automatizzabile e richiede un'attività umana che lo manifesti, attraverso l'apposizione della firma digitale (chiave privata)[100]. Tornando alla libertà della forma, inoltre, la norma dell'art 8-ter sembra comunque opportuna dal momento in cui chiarisce che uno smart contract può soddisfare il requisito della forma scritta. Essendo un programma per elaboratore, infatti, potrebbero sorgere dubbi, in assenza di un'espressa previsione, circa la conformità di uno smart contract al requisito dell'immodificabilità di cui all'art. 3, comma 2, del DPCM 13 novembre 2014 ed a quanto previsto dall'art. 4, comma 3 del DPCM 22 febbraio 2013 secondo cui non può considerarsi immodificabile un documento informatico che contiene macroistruzioni o codici eseguibili (questi ultimi contenuti, per definizione, in uno smart contract). In assenza di una previsione espressa lo smart contract, pertanto, potrebbe non essere in grado di rientrare nell'ambito della categoria di documento informatico immodificabile, con la conseguenza che ne verrebbe meno la validità[101].

Nel nostro ordinamento, oltre al principio della libertà della forma, vige anche quello dell'autonomia contrattuale e negoziale delle parti ex art 1322 c.c. Naturalmente questa libertà è limitata dalla legge e dai dettami Costituzionali.

Detto ciò, nel caso, ad esempio, di illiceità dell'oggetto del contratto, non sarà lo smart contract ad essere illegale, bensì lo sarà il contratto che lo ha generato o quello in cui esso è contenuto. In caso di contratto invalido, anche se esso sia già stato eseguito tramite smart contract, rimangono inalterati i diritti alla ripetizione delle prestazioni già eseguite secondo i criteri di legge ordinari[102].

---

[100] Stefano CAPACCIOLI, Smart contracts: traiettoria di un'utopia divenuta attuabile, cit., pag. 40

[101] M. Nicotra, l'Italia prova a normare gli smart contract, ecco come: pro e contro www.agendadigitale.eu

[102] Fulvio SARZANA di S. IPPOLITO, Massimiliano NICOTRA, Diritto della blockchain, Intelligenza artificiale e IoT, cit. pag. 99

3.6.1 FORME DI INTERAZIONE DI SMART CONTRACT

Possiamo considerare, alla luce di quanto emerso, uno smart contract come un meccanismo automatico che automatizza un contratto, o parti di esso, costituendo di fatto una codificazione digitale del contratto che lo presuppone. Una condivisibile corrente dottrinale sostiene che, dal punto di vista della valutazione legale, sarebbe applicabile per gli smart contract il diritto corrispondente al contratto che esso di fatto rappresenta in forma informatica[103].

I contratti "intelligenti" potranno assumere, quindi, le seguenti forme:

- Contratto interamente in codice informatico che disciplina ed esegue gli accordi sussistenti tra le parti.
- Contratto interamente in codice informatico che prevede la predisposizione unilaterale delle condizioni contrattuali. Di fatto esso consiste in qualcosa di analogo all'offerta al pubblico.
- Contratto in codice informatico e linguaggio naturale.
- Contratto in linguaggio naturale che prevede per l'esecuzione l'utilizzo di uno smart contract (in codice informatico).

3.6.2 IL LINGUAGGIO DEGLI SMART CONTRACT

In quanto software, a differenza dagli accordi tradizionali, lo smart contract è scritto in "linguaggio macchina". Perciò potrebbe essere compreso solo da una cerchia ristretta di persone competenti in informatica. Parte della dottrina[104], riflettendo sulla questione, sostiene che sarebbe possibile inserire per ogni stringa di codice la traduzione in linguaggio umano di ciò che rileva, in quella specifica parte, dal punto di

[103] Andrea STAZI, Automazione contrattuale e "contratti intelligenti". Gli smart contracts nel diritto comparato, cit., pag. 124.
[104] Stefano CERRATO, Contratti tradizionali, diritto dei contratti e smart contract, cit., pagg. 296, 297

vista legale. Infatti, le caselle di testo sono quasi sempre inseribili all'interno di un algoritmo.

Il problema del linguaggio informatico si potrebbe anche analizzare dal punto di vista della tutela di una delle parti contrattuali che, non conoscendo il linguaggio tecnico, potrebbero non comprenderne il contenuto. Va detto tuttavia che il linguaggio informatico, essendo un linguaggio tecnico-operativo, non lascia spazio a interpretazioni flessibili. Sarebbe quindi una buona pratica quella di redigere un contratto tradizionale in coppia con lo smart contract così da poter cristallizzare, anche al fine della prova, l'autentica volontà delle parti. Resterebbe salva, per la parte che non ha la percezione del significato del contratto che sta concludendo, la domanda di annullamento per errore nei termini ex art 1477 c.c. In dottrina si ipotizza anche l'applicabilità dell'art 1433 c.c. nel caso in cui il consulente informatico, autorizzato della parte a redigere il codice, avesse commesso un errore nel codificare correttamente la volontà della parte[105].

3.6.3 VICENDE PATOLOGICHE E DIRITTO DI RECESSO

È possibile argomentare il verificarsi di eventuali vicende patologiche, calandoci nella specifica realtà dello smart contract inteso come diversa forma di redazione di un contratto, sulla base che esso sia una porzione di codice informatico che, opportunamente programmato, produce degli effetti informatici predeterminati dalle parti con l'intento di modificare, creare o estinguere uno stato di cose suscettibili di valutazione economica, tanto nel mondo digitale quanto nel mondo reale.

Sappiamo che i requisiti di un contratto sono sanciti dall'art 1325 c.c. e che specificatamente, ex art 1418 c.c., il contratto è nullo quando, ad esempio, è contrario a norme imperative. Uno smart contract quindi sarà certamente nullo se contrario a

[105] Stefano CERRATO, Contratti tradizionali, diritto dei contratti e smart contract, cit., pagg 298-300

norme imperative. Gli effetti dovranno essere posti nel nulla, con il ripristino della situazione generata dal contratto. Tuttavia, il vantaggio che lo smart contract potrà avere, rispetto ad un contratto non autoeseguibile, è quello di poter potenzialmente già avere in sé una sorta di "antidoto" ad un suo ipotetico malfunzionamento, o ad un vizio che lo gravi: ovviamente il caso della contrarietà a norme imperative è un caso limite, in cui si presume che l'autore dello smart contract si guarderà dal programmare in contrario a norme imperative, oppure, intervenuta nullità, ripristini gli effetti. Ciò non toglie validità alla considerazione generale per cui lo smart contract, poiché preprogrammabile, possa contenere in sé già un'azione inversa volta al rimedio di una eventuale patologia.

Tra gli aspetti più caratteristici degli smart contract, inoltre, occorre considerare la loro irrevocabilità che scatta nel momento in cui gli stessi sono inseriti all'interno della piattaforma blockchain, da cui segue l'automatica esecuzione delle prestazioni che rende inutilizzabile l'eccezione di inadempimento. Un espediente per la risoluzione di questa problematica potrebbe essere offerto da una specifica funzione, introdotta dalle blockchain più avanzate (es. Ethereum), la c.d. *kill* o funzione di autodistruzione dello smart contract che punta a rimuovere i programmi non più impiegati, con la finalità di rendere più efficiente le *performance* della blockchain. Tale funzione è attivabile solo dal nodo che ha creato lo smart contract, attraverso l'inoltro di una transazione e immettendo nella blockchain il corrispondente codice elettronicamente firmato, ovvero, le parti potrebbero anche inserire la funzione di autodistruzione all'interno dello smart contract e nell'eventualità prevedere, in un accordo *a latere*, i casi di attivazione della medesima.

Tutto questo permette alla parte adempiente, nel caso in cui la prestazione non venisse erogata, di ricorrere alle vie legali per ottenere la risoluzione contrattuale o addirittura

"l'eliminazione" del contratto dalla blockchain mediante la funzione di autodistruzione.

Facendo poi cenno al Codice di Consumo, nella regola contenuta nell'art 59, è stabilito che il diritto di recesso è escluso relativamente a "la fornitura di contenuto digitale mediante un supporto non materiale se l'esecuzione è iniziata con l'accordo espresso del consumatore e con la sua accettazione del fatto che in tal caso avrebbe perso il diritto di recesso". Si deve osservare che allo stato dei fatti risulti difficile acquisire, all'interno di uno smart contract, l'accordo espresso del consumatore e la sua accettazione relativa alla perdita del diritto di recesso. Si evidenzia, inoltre, che pur riuscendo a superare tali limiti, la regola non riuscirebbe a trovare applicazione nell'ipotesi in cui non si fosse in presenza di beni digitali. Si pensi, ad esempio, a uno smart contract che consentisse il pagamento di una somma di denaro in caso di ritardo dell'aereo. Resterebbe la possibilità per il consumatore di far valere il rimedio al di fuori della blockchain. In tal caso però verrebbe meno, per un verso, l'efficacia del recesso pensato per evitare di far gravare sul consumatore l'obbligo di adempiere e, per altro verso, il rimedio risulterebbe gravoso con riferimento alla fornitura eseguita di un contenuto digitale mediante un supporto non materiale.

Il problema, pertanto, non è tanto quello dell'astratta applicabilità delle discipline esistenti ma piuttosto quello della ragionevolezza nel pensare di continuare ad applicare discipline ideate per alcuni contesti significativamente mutati. Se da un alto non si può accettare l'idea della totale non applicabilità del diritto, dall'altro non si può non evidenziare come alcune regole possano, o debbano, necessariamente essere adeguate.

3.7 TECNICHE INVESTIGATIVE SULLA BLOCKCHAIN

La blockchain permette diverse tipologie d'indagine, mirate a rispondere a diverse domande. Anticipiamo fin d'ora che la domanda circa l'identità del proprietario di un indirizzo Bitcoin (ad esempio) è la più ardua: spesso non trova risposta e in diversi casi richiede numerose analisi incrociate – non soltanto sulla blockchain – per arrivare a una soluzione o a un insieme di candidati. Partiamo però dalla principale modalità con la quale si percorre il primo passo verso la deanonimizzazione degli indirizzi e delle transazioni: la clusterizzazione dei wallet. La tecnica del "clustering" consiste nell'identificare e raggruppare gli indirizzi Bitcoin in wallet, cioè in gruppi d'indirizzi appartenenti presumibilmente a una singola entità, che non necessariamente coincide con un soggetto fisico. Spesso i wallet possono appartenere a un individuo ma anche a un negozio, un exchange, un mixer, una organizzazione o persino essere aggregati ma non appartenere alla stessa entità. Ricordiamo che un wallet è una "collezione" di indirizzi Bitcoin, generati singolarmente, indipendentemente e aggregati dal sistema utilizzato (hardware, software, web, etc.) oppure generati in modo sequenziale tramite tecniche gerarchiche deterministiche a partire da un unico "seme" che diventa quindi una sorta di master key da cui derivano poi tutte le altre. In ogni caso, raramente gli utenti fanno uso di un singolo indirizzo Bitcoin o comunque di singoli indirizzi: per la quasi totalità degli utilizzatori, ciò che riceve o trasferisce criptomoneta è il wallet.

La clusterizzazione avviene tramite un'analisi della blockchain e l'utilizzo di alcuni approcci basati sull'esperienza, descritti efficacemente da Jonas David Nick nel suo lavoro "Data-Driven De-Anonymization in Bitcoin"[106]. Sostanzialmente, tramite questa tecnica è possibile, dato un indirizzo Bitcoin appartenente a un'entità, localizzare eventuali altri indirizzi facenti parte del suo stesso portafoglio. Per fare un

[106]Jonas David Nick, "Data-Driven De-Anonymization in Bitcoin" https://jonasnick.github.io/papers/thesis.pdf (consultato il 30/05/2022)

esempio pratico fuori dal mondo delle criptovalute, sarebbe come riuscire a identificare tutti i conti correnti intestati a un soggetto – anche quelli che vorrebbe mantenere riservati – conoscendone soltanto uno. Lo scenario tipico i cui la clusterizzazione ha finalità investigative di rilevanza è quello nel quale con un indirizzo sono stati commessi degli illeciti in modo anonimo e gli inquirenti tentano di trovare altri indirizzi tramite i quali, si spera, il soggetto abbia invece operato alla luce del sole. Pensiamo ad esempio a un criminale che riceve dei fondi a fronte della vendita di materiale illecito sul dark web e, utilizzando un unico wallet anche se mediante indirizzi diversi, acquista delle gift card facendosi spedire le carte al proprio domicilio. Una buona attività di clusterizzazione permette di collegare gli indirizzi utilizzati per ricevere fondi illeciti nel dark web con quelli utilizzati per acquistare gift card arrivando a identificare persino il domicilio del soggetto. Il primo metodo per clusterizzare un indirizzo è quello di ricercare tutte le transazioni in cui tale indirizzo compare, insieme ad altri, come TXIN, cioè come transazione in ingresso. Ricordiamo infatti che una transazione Bitcoin può prelevare fondi da più di un indirizzo riversandoli su uno o più indirizzi: la parte che interessa in questo caso è il fatto che una singola transazione può prelevare, in contemporanea, fondi da diversi indirizzi. Tutti quegli indirizzi saranno, quindi, di proprietà (o meglio, all'interno dello stesso wallet) della stessa entità o, talvolta, soggetto. Trasponendo nella realtà questo metodo, potremmo immaginare che se da un PC partono quattro bonifici da conti diversi verso lo stesso conto (ma anche verso conti diversi, fa poca differenza) in contemporanea, con buona probabilità i quattro conti di provenienza appartengono alla stessa persona o società. Applicando questo sistema a tutte le transazioni (con un lavoro lungo e oneroso) si possono identificare gruppi d'indirizzi afferenti tutti alla stessa entità.

La teoria di cui abbiamo letto al paragrafo precedente viene implementata in diversi strumenti e servizi a disposizione degli investigatori. Alcuni sono gratuiti, altri a

pagamento, alcuni s'installano sul proprio PC o server mentre altri vengono forniti come servizi esterni.

Ormai noti a chiunque, i block explorer sono il punto di partenza per osservare la blockchain senza bisogno di scaricarne l'intero contenuto in locale sul proprio PC, cosa sempre più complessa dato che le transazioni occorse dal 2009 occupano ormai circa 200 GB di spazio. Siti come blockchain.com[107], blockexplorer.com[108] o blockcypher.com[109] sono il punto di partenza per sviscerare le transazioni e analizzarne il contenuto. Per poter operare ricerche complesse sulla blockchain (es. filtrare per cifre transate, indirizzi coinvolti, periodo, etc.) uno dei siti migliori è blockchair.com[110], anch'esso gratuito ma ottimo per attività investigativa perché fornisce anche la possibilità di esportare i risultati[111].

3.8 FORO COMPETENTE

Sulla base di quanto precedentemente espresso, è lecito anche domandarsi come le parti potrebbero risolvere le controversie che dovessero insorgere nella esecuzione di uno smart contract.

Una prima risposta, proveniente dai sostenitori della blockchain, consisterebbe nel negare radicalmente il problema all'origine e nel sottolineare come lo smart contract sarebbe infallibile ed immediatamente eseguibile e che, pertanto, non è possibile che sorgano dei problemi nel momento della esecuzione dello stesso. Sarebbe tuttavia più realistico pensare che le parti possano operare una scelta, prevedendo una clausola di scelta del foro nello smart contract stesso, ovvero tramite accordo esterno.

---

[107] https://www.blockchain.com/ (consultato il 30/05/2022)
[108] https://blockexplorer.com/ (consultato il 30/05/2022)
[109] https://www.blockcypher.com/ (consultato il 30/05/2022)
[110] https://blockchair.com/ (consultato il 30/05/2022)
[111] P. Dal Checco "Blockchain analysis, digital forensics e indagini digitali attraverso blockchain" 2019

Laddove le parti non avessero previsto una scelta simile, potrebbero trovare applicazione al caso specifico, alcune regole di carattere europeo e internazionale[112].

È altresì opportuno domandarsi se le parti dello smart contract tenderanno ad 'evitare' la giurisdizione delle corti nazionali, proprio in virtù delle sopra ricordata vocazione alla costruzione di un sistema di regole autonomo rispetto al diritto e alla giurisdizione nazionale. Per tale motivo, le parti dello smart contract potrebbero ricorrere, con buona probabilità, ai sistemi di risoluzione alternativa delle controversie, come l'arbitrato: strumento flessibile, che ben si adatta alle caratteristiche dello smart contract. Peraltro, lo smart contract può prevedere una clausola compromissoria che stabilisca che ogni eventuale controversia derivante dall'esecuzione del contratto sia demandata alla competenza esclusiva di una procedura arbitrale fisica o virtuale, stabilita ad hoc. Ora, in tale prospettiva, lo smart contract potrebbe attivare automaticamente il meccanismo di risoluzione della lite e potrebbe, a sua volta, utilizzare l'infrastruttura blockchain. Il lodo sarebbe registrato nel mondo virtuale ed eseguito sulla stessa blockchain, tramite l'esecuzione di un codice che preveda il trasferimento delle somme riconosciute come dovute dal lodo arbitrale dal conto riconducibile alla parte condannata a quello riconducibile alla parte vincitrice. Simili soluzioni, per quanto futuribili, sono oggetto dell'attenzione dei giuristi.

Resta però necessario evidenziare che queste tecnologie sono destinate a non essere segregate nell'ambito del nostro Paese, ma, come evidenziato anche dal Parlamento Europeo, esse potrebbero avere ampia diffusione in tutta l'Unione Europea. Ciò pone problemi dal punto di vista normativo anche in riferimento ai possibili conflitti che potrebbero sorgere tra i diversi principi ed istituti giuridici applicati nei Paesi membri.

---

[112] In particolare, il riferimento è al Regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio, del 12 dicembre 2012, concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale, in GU L 351, 20 dicembre 2012, 1-32. Si veda anche la Convenzione della Conferenza dell'Aia di diritto internazionale privatosugliaccordidisceltadelforodel30giugno2005https://assets.hcch.net/docs/131f1153-ef61-4016-8e60-845316a4b054.pdf

Allo stato dell'arte, quindi, un approccio efficace di politica legislativa dovrebbe tener conto di tali aspetti, non cercando di regolare nel dettaglio requisiti e validità degli smart contract, ma ponendo quelle regole necessarie ad incentivarne l'utilizzo eliminando le incertezze degli operatori senza però dare adito a conflitti interpretativi. In tale ottica uno smart contract dovrebbe essere definito per quello che semplicemente è, ossia un programma per elaboratore che opera su tecnologie basate su registri distribuiti che può rappresentare, in tutto o in parte, l'accordo di due o più soggetti per costituire, regolare o estinguere tra loro un rapporto giuridico patrimoniale, idoneo a soddisfare il requisito della forma scritta qualora formato ai sensi dell'art. 20, comma 2 del d.lgs n. 82/2005[113].

3.8.1 IL REGOLAMENTO ROMA I

In tema di eventuali conflitti tra diversi istituti giuridici, il principale strumento ai fini della determinazione della legge applicabile ai contratti internazionali dell'Unione Europea, è il Regolamento Roma I[114].

Il Regolamento si applica alle obbligazioni contrattuali in materia civile e commerciale, nelle circostanze in cui si verifichi un conflitto di leggi.

L'ambito di applicazione sarebbe così ampio da ritenere di poter ricomprendere anche lo smart contract, nel caso in cui fosse possibile rinvenire un accordo giuridicamente vincolante. Solitamente, lo smart contract consiste in un software che monitora o documenta l'esecuzione di un contratto. In tal caso, il Regolamento si applicherà al contratto stipulato dalle parti nel mondo fisico.

[113] https://www.agid.gov.it/sites/default/files/repository_files/leggi_decreti_direttive/dl-7-marzo-2005-82_0.pdf (consultato il 12/06/2022)

[114] Regolamento (CE) n. 593/2008 del Parlamento europeo e del Consiglio, del 17 giugno 2008, sulla legge applicabile alle obbligazioni contrattuali (Roma I)

Il Regolamento precisa che la legge applicabile è innanzitutto quella scelta dalle parti e in particolare specifica, all'art 3.1, che la scelta deve essere espressa o risultare chiaramente dalle disposizioni del contratto.

Allo smart contract poi è sicuramente applicabile anche il principio dell'autonomia delle parti, favorendo, in tal modo, una certezza del diritto applicabile. Tuttavia, la trasmutazione di una eventuale scelta in linguaggio algoritmico non sarebbe cosa facile. Di conseguenza, la scelta di legge potrebbe essere effettuata nel contratto che poi verrà eseguito virtualmente, oppure in un accordo esterno.

Ad ogni modo, una parte della dottrina sembra convergere sull'idea che il Regolamento Roma I possa trovare applicazione allo smart contract laddove tale accordo possa qualificarsi alla stregua di un contratto giuridicamente vincolante[115].

Tuttavia, è evidente come lo smart contract non abbia ancora trovato una chiara collocazione nell'ambito del diritto esistente e pertanto, sarebbe forse prematuro ritenere pienamente applicabile tale Regolamento.

3.9 DISCIPLINA EUROPEA

Anche l'UE dimostra grande interesse nella materia.

Come provvedimenti si ricorda, in primo luogo, la Risoluzione del Parlamento Europeo del 3 ottobre 2018 sulle tecnologie DLT e blockchain: "creare fiducia attraverso la disintermediazione", che sottolinea come l'Unione disponga di una grande opportunità per divenire un attore primario nello sviluppo nei mercati globali, indicando possibili linee di intervento nel favorire l'implementazione di queste tecnologie.

[115] G. RUHL, Blockchain Networks and European Private International Law http://conflictoflaws.net/2018/blockchain-networks-and-european-private-internationa-law (consultato il 13/06/2022)

Interesse altresì testimoniato dalla Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione con riguardo alla legge sui servizi digitali: "adeguare le norme di diritto commerciale e civile per i soggetti commerciali che operano online". Con tale risoluzione, il Parlamento Europeo ritiene che, nella regolamentazione degli aspetti civili e commerciali in ambito blockchain e smart contract, si debbano prevedere:

- misure che garantiscano l'esistenza di un adeguato quadro normati vo per lo sviluppo e la diffusione dei servizi digitali, fra cui tecnologie di registro distribuito come le blockchains e i contratti intelligenti;
- misure atte ad assicurare che i contratti intelligenti siano dotati di meccanismi in grado di arrestarne e invertirne l'esecuzione, in particolare alla luce delle preoccupazioni private della parte debole o delle preoccupazioni pubbliche, per esempio quelle legate agli accordi di cartello e ai diritti dei creditori in caso di insolvenza e ristrutturazione;
- misure che garantiscano equilibrio e parità adeguati tra le parti per quanto riguarda i contratti intelligenti, tenendo conto in particolare degli interessi delle piccole imprese e delle PMI, per le quali la Commissione dovrebbe prendere in esame le possibili modalità;

il Parlamento europeo ha, a più riprese, affermato che «le tecnologie DLT e blockchain possono costituire uno strumento che rafforza l'autonomia dei cittadini, dando loro l'opportunità di controllare i propri dati e decidere quali condividere nel registro, nonché la capacità di scegliere chi possa vedere tali dati» e, per tale ragione si «necessita di un quadro favorevole all'innovazione che consenta e incoraggi la certezza del diritto e rispetti il principio della neutralità tecnologica». In aggiunta, ha sottolineato «che la DLT riduce i costi di intermediazione in un ambiente di fiducia tra le parti di una transazione e consente scambi di valore tra pari suscettibili di rafforzare l'autonomia

dei cittadini, destrutturare i modelli tradizionali, migliorare i servizi e ridurre i costi lungo le catene del valore in un'ampia gamma di settori chiave», ponendo l'accento «sull'ampia gamma di applicazioni basate sulla DLT che potrebbero potenzialmente interessare tutti i settori dell'economia». Alla luce di ciò ha sottolineato «che qualsiasi approccio regolamentare nei confronti delle DLT dovrebbe essere favorevole all'innovazione, consentire un sistema di "passaporto" ed essere improntato ai principi di neutralità tecnologica e neutralità dei modelli aziendali», ha chiesto «alla Commissione e agli Stati membri di mettere a punto iniziative comuni di sensibilizzazione e di formazione rivolte a cittadini, imprese e amministrazioni pubbliche e intese ad agevolare la comprensione e la diffusione di questa tecnologia», ha dichiarato «che l'Unione dispone di un'eccellente opportunità per divenire leader mondiale nel campo delle DLT ed essere un attore credibile nel guidarne lo sviluppo e i mercati livello globale, in collaborazione con i partner internazionali»[116].

Inoltre, la Commissione ha lanciato numerose iniziative per l'esplorazione delle tecnologie di registro distribuito, tra le quali: La "European Blockchain Partenership" e lo "European Union Blockchain Observatory and Forum".

3.9.1 EUROPEAN BLOCKCHAIN PARTNERSHIP

Per cercare di favorire e stimolare questa innovazione, alcuni paesi europei, tra cui anche l'Italia, hanno deciso di dare vita alla European Blockchain Partnership[117], una iniziativa che punta a favorire la collaborazione tra gli Stati membri per lo scambio di esperienze, sia sul piano tecnico sia su quello della regolamentazione. Il punto più

[116] Risoluzione «del 3 ottobre 2018 sulle tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione (2017/2772(RSP))» disponibile al seguente indirizzo: http://www.europarl.europa.eu/doceo/document/TA-8-2018-0373_IT.html (consultato il 13/06/2022)

[117] The European Blockchain Partnership (EBP) is an initiative to develop an EU strategy on blockchain and build a blockchain infrastructure for public services.
https://digital-strategy.ec.europa.eu/en/policies/blockchain-partnership (consultato il 13/06/2022)

importante di questa partnership riguarda la progettazione e il lancio di una Blockchain dell'Unione Europea da sviluppare in sinergia con i piani del Digital Single Market come base e infrastruttura per il settore pubblico e per le imprese private.

La tecnologia è già stata testata con successo in tante situazioni, ad oggi primariamente per i servizi finanziari, ma è destinata a diventare operativa e integrata in un numero crescente di servizi digitali, come l'agrifood, la notarizzazione, la certificazione, l'energia e la logistica. La European Blockchain Partnership ha anche lo scopo di garantire all'Europa nel suo complesso un ruolo di rilievo nello sviluppo e nella diffusione di soluzioni basate sulla blockchain.

3.9.2 EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM

L' EU Blockchain Observatory and Forum"[118] è nato su iniziativa della Commissione Europea per dare impulso alle innovazioni introdotte dalla blockchain e contribuire allo sviluppo di un ecosistema all'interno del territorio comunitario, in modo che l'Ue possa rafforzare il proprio ruolo di leader globale in questo campo. I suoi principali obiettivi consistono nel: monitorare le iniziative sulla blockchain che si sviluppano all'interno dell'Unione europea, introdurre una fonte attendibile e completa di informazione sulle potenzialità di questa nuova tecnologia, creare una sede di discussione autorevole e trasparente per diffondere informazioni e opinioni sull'argomento, formulare suggerimenti e raccomandazioni sul ruolo che l'Unione europea potrà giocare sul terreno della blockchain.

Tra le prime iniziative dell'osservatorio ci sono la creazione di una piattaforma di dibattito e condivisione delle conoscenze, con il lancio di una community online,

[118] The EU Blockchain Observatory & Forum is an initiative sponsored by the European Commission, Directorate-General of Communications Networks, Content & Technology. https://www.eublockchainforum.eu/ (consultato il 13/06/2022)

eublockchain.mobilize.io, i cui canali di discussione includono l'innovazione, in Gdpr e le politiche sui dati, i servizi governativi, l'identità, la scalabilità e l'interoperabilità. La community conta oggi su oltre 700 partecipanti ed è in rapida crescita. L'osservatorio ha inoltre lanciato la nuova veste grafica del proprio sito web, dove mette a disposizione report e materiali educativi, oltre a una nutrita collezione di "frequently asked questions". È stata anche realizzata una "Eu blockchain map", la versione iniziale di una rappresentazione dinamica dei progetti ed eventi che riguardano la blockchain su tutto il territorio comunitario, aperta al contributo dei singoli player in modalità "crowdsourcing".

Con questi strumenti, in particolare con questo osservatorio previsto ad hoc, l'Unione Europea dimostra un grandissimo interesse e mira, senza dubbio, a divenire un global leader del settore.

CAPITOLO QUARTO

APPLICAZIONE E CASI D'USO DELLA TECNOLOGIA

4.1 BLOCKCHAIN APPLICATA AI PROCEDIMENTI GIURIDICI

La blockchain, come funzione certificatrice, può essere dunque impiegata per conferire data certa al documento, scrittura privata o atto pubblico, nonché al contratto, digitale o smart, ivi registrato. In verità, sistemi di certificazione dei documenti generati e sottoscritti in forma digitale già esistono: quasi ogni ordinamento giuridico ha introdotto previsioni di legge volte a conferire espressa funzione di certificazione ad alcuni mezzi tecnologici. In Italia, ad esempio, il d.lgs. 80/2005, c.d. Codice dell'Amministrazione Digitale, riconosce validità giuridica a determinati strumenti e mezzi tecnologici di comunicazione. La tecnologia blockchain andrebbe dunque ad aggiungersi, a quella attualmente diffusa. La ragione si rinviene nella maggiore certezza che potrebbero garantire i sistemi distribuiti, rispetto a quelli centralizzati e/o decentralizzati. Da ciò consegue che, la tecnologia blockchain può divenire strumento di dialogo tra le corti e le parti solo se sarà introdotta una normativa ad hoc ovvero se quella attualmente esistente sarà adattata ai nuovi strumenti.

Alcuni ordinamenti giuridici si stanno dotando dello schema normativo idoneo per facoltizzare le parti a trasmettere le prove documentali attraverso tecnologia blockchain. Per quanto riguarda l'ordinamento italiano, il già menzionato Decreto Semplificazioni ha introdotto l'art. 8-ter che riconosce, tra l'altro, che «la memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all'art. 41 del Regolamento UE n. 910/2014 del Parlamento Europeo e del Consiglio del 23 Luglio 2014». In tal senso, una volta "memorizzato" il documento su blockchain, verrebbe a riconoscersi un preciso timbro temporale dello stesso con la

conseguenza che quest'ultimo potrebbe fungere come elemento di prova da poter produrre in giudizio.

4.2 BLOCKCHAIN PER LA CORPORATE GOVERNANCE

Le peculiarità di questa innovativa tecnologia consentono di gettare nuova luce su problematiche di corporate governance delle società per azioni che affondano radici nell'incapacità di tenere registrazioni accurate e tempestive in merito alla titolarità delle azioni, nei costi delle assemblee generali, nelle catene di intermediazione e nel voto per deleghe degli azionisti. L'utilizzo della blockchain e degli smart contract apre a scenari quali assemblee generali condotte esclusivamente online; una più efficiente implementazione del voto elettronico, anche per questioni delicate come le deliberazioni concernenti fusioni e acquisizioni o l'elezione dei membri del consiglio di amministrazione; nonché l'automatizzazione nella distribuzione dei dividendi. L'idea di fondo è che sia possibile rendere taluni processi decisionali più sicuri e trasparenti, migliorando altresì la tracciabilità nel trasferimento di titoli e nell'esercizio di diritti, così determinando importanti vantaggi nella gestione della società da un lato e creando un ambiente più attraente per gli investitori dall'altro.

L'Assemblea costituisce il momento in cui tutti gli azionisti, e in particolare quelli con diritto di voto, esprimono una qualche forma di potere o contributo al governo societario. Di conseguenza è sentita l'esigenza di migliorare i meccanismi esistenti o implementarne di nuovi che possano rendere l'Assemblea il più efficiente possibile. È ragionevole sostenere che implementare la blockchain in determinate procedure, quali il voto elettronico e il tracciamento della titolarità delle azioni o di altri strumenti finanziari partecipativi, condurrebbe ad una modernizzazione dell'Assemblea. Il voto via blockchain consentirebbe di abbattere taluni costi e rendere più accurata la

tabulazione dei voti, motivando quindi gli azionisti a impegnarsi maggiormente nel governo societario.

Venendo al voto assembleare degli azionisti, è ragionevole sostenere che l'espressione del voto tramite blockchain possa risolvere il problema della manipolazione dei dati ambigui, dal momento che i voti immagazzinati sarebbero dati approvati dal meccanismo di validazione su base algoritmica della blockchain in uso e non manipolabili per via della immutabilità delle registrazioni effettuate nei blocchi.

La tecnologia blockchain, quindi, offre un'alternativa ai classici libri mastri, in quanto fornisce un nuovo modo di creare, scambiare e tracciare la proprietà di asset finanziari su base P2P. Tali implementazioni potrebbero risolvere molte questioni controverse relative all'incapacità delle società di tenere registrazioni accurate e tempestive di chi è titolare delle azioni. Più precisamente, un registro blockchain pubblico permetterebbe di osservare in tempo reale i trasferimenti di azioni da un titolare all'altro, il che significherebbe operazioni di vendita di azioni più rapide, meno costose e più trasparenti tra acquirenti e venditori, riducendo al tempo stesso i rischi di manipolazione del mercato azionario, poiché ciò che è registrato su blockchain è immutabile e non riscrivibile.

4.3 SOLUZIONI PER LA PROPRIETÀ INTELLETTUALE

Degno di nota è sicuramente il progetto francese BlockchainyourIP[119], che offre una soluzione per attribuire "proof of existence" a tutti gli intangible assets, permettendo direttamente a ciascun autore o creativo di ancorare le proprie informazioni proprietarie a un blocco su blockchain. Saldamente focalizzato sul Bitcoin, il servizio BlockchainyourIP evidenzia la chiara impronta dei legali che prendono parte al suo

[119] Per approfondimenti: https://blockchainyourip.com/ (consultato il 20/06/2022)

progetto, poiché prevede accurati tutorial di natura giuridica sulla tutela delle opere dell'ingegno, delle invenzioni, dei segni distintivi, dei software, dei disegni e modelli, del know how e soprattutto dei segreti industriali. In particolare, il lavoro dietro BlockchainyourIP analizza in maniera approfondita le difficoltà connesse ai tradizionali sistemi di ammissione dei mezzi di prova nei procedimenti giurisdizionali e il servizio offre un chiaro supporto su questo fronte, anche con l'ausilio di ufficiali giudiziari in combinazione con la soluzione tecnologica. BlockchainyourIP opera in quattro fasi: crea il foot print di un documento attraverso il browser, richiede la compilazione di un modulo con le informazioni sul titolare e sul contenuto oggetto di protezione, àncora la digital print del documento alla blockchain con una transazione Bitcoin e rilascia all'utente un certificato con le informazioni relative al bene immateriale, in particolare la marca temporale.

Sempre basati sul medesimo principio di associazione di un contenuto a un digital foot print e al suo successivo ancoraggio alla blockchain sono Binded[120] e Blocknotary[121], dedicati alle fotografie e ai media file, e quindi legati all'ambito del diritto d'autore.

Tutti questi servizi sono già fruibili e soprattutto operano con modalità particolarmente semplici di accesso. Tanti progetti sono prototipi ma vi sono concrete possibilità che alcuni di essi, come quelli menzionati, diventino veri e propri punti di riferimento capaci di superare, quanto a comodità d'uso e fruibilità globale, alcuni sistemi tradizionali di registrazione e tutela dei diritti di proprietà intellettuale e industriale.

[120] Per approfondimenti: https://binded.com/ (consultato il 20/06/2022)
[121] Per approfondimenti: https://www.blocknotary.com/ (consultato il 20/06/2022)

4.4 IDENTITÀ DIGITALE: LA SOLUZIONE "UPORT"

Sin dal 2016, il Parlamento Europeo ha incoraggiato la sperimentazione della blockchain e delle DLT, in generale, al fine di ottimizzare la prestazione dei servizi ai cittadini ed aumentare la condivisione di dati, la trasparenza e la fiducia tra il governo e i cittadini stessi. La Commissione Europea, nel raccogliere l'invito del Parlamento UE a mettere a punto casi d'uso concreti e progetti pilota basati su tali tecnologie, ha indicato tra gli obiettivi prioritari il potenziamento dell'accesso ai servizi di e-government con identità digitale decentralizzata[122]. L'Osservatorio e forum europeo sulla blockchain nell'analizzare i vantaggi derivanti dell'impiego di tali tecnologie nei servizi pubblici, in termini di efficienza e semplificazione dei processi burocratici, ha invero sottolineato che per beneficiare veramente del potenziale della blockchain per la fornitura di servizi ai cittadini, i governi devono essere in grado di sviluppare sistemi di identità digitali che possano essere utilizzati in piattaforme basate su tale tecnologia, creando un modello decentralizzato di proprietà, gestione, rappresentazione ed attestazione dell'identità di una persona. A parere dell'Osservatorio, la blockchain offre la possibilità di superare a monte tutti i problemi connessi attualmente all'identità digitale attraverso il concetto di identità autosufficiente o sovrana, basato sull'idea che le informazioni relative alle identità delle persone non sono detenute da terze parti, ma sarebbero le persone stesse a fare in modo che tali informazioni siano verificate. A tal fine, l'Osservatorio suggerisce la possibilità che i governi emettano in favore dei loro cittadini o residenti certificati firmati digitalmente attestanti: nome della persona, indirizzo, data di nascita, luogo di residenza, patente di guida, titoli di proprietà immobiliare o fondiaria, la registrazione del voto e così via. Le persone, quindi, potrebbero utilizzare queste credenziali come se fossero documenti di identità al pari

[122] Risoluzione del Parlamento europeo del 3 ottobre 2018 sulle tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione, http://www.europarl.europa.eu/doceo/document/TA-8-2018-0373_IT.html?redirect. (consultato il 20/06/2022)

di passaporti e patenti di guida. Il rischio di furto o falsificazione di tali informazioni sarebbe quasi nullo, atteso che la blockchain permette agevolmente di verificare l'autenticità delle informazioni.

L'Osservatorio ritiene che, per assicurare a tutti un'identità certa ed inconfutabile, le istituzioni europee e quelle nazionali, a più livelli, devono necessariamente concentrarsi su due obiettivi: 1) l'elaborazione di efficaci strategie per risolvere il problema di cd. awareness inevitabilmente connesso all'identità autosovrana; 2) l'elaborazione di soluzioni univoche per: garantire il rispetto della normativa europea sulla privacy e protezione dei dati personali; stabilire i casi in cui sia possibile per gli utenti agire on line in completo anonimato; permettere l'accesso all'identità digitale su blockchain a coloro per i quali allo stato ciò non sia possibile o che non sono in grado di utilizzare questa tecnologia.

L'Osservatorio ed il JRC[123] hanno segnalato come caso d'uso interessante e promettente in tema di identità digitale decentralizzata l'esperimento di Zug, la città svizzera che per prima nel novembre 2017 ha certificato la registrazione dell'identità digitale dei residenti su blockchain di Ethereum. Gli utenti hanno potuto registrare le proprie identità sull'app mobile chiamata uPort per creare il cd.ID uPort, un indirizzo pubblico unico a livello globale collegato ad uno smart contract. Una volta registrato il codice, l'utente accede al portale Web Zug ID del Comune di Zug, si identifica ed inserisce i propri dati personali, incluso un numero ID Zug rilasciato in precedenza, come informazioni verificabili. A questo punto, ID uPort si collega automaticamente ad un ID personale presente nel registro digitale cittadino di Zug. Al fine di evitare eventuali frodi, resta come passaggio obbligato per completare la registrazione

[123] Il Centro comune di ricerca (JRC) è il servizio scientifico interno della Commissione Europea e fornisce supporto tecnico indipendente al processo decisionale dell'UE mediante consulenze basate su evidenze scientifiche. Tutte le attività del JRC sono disponibili in https://ec.europa.eu/info/departments/joint-research-centre_it.

l'esibizione dei documenti di identità da parte dell'utente, che deve a tal fine recarsi personalmente all'Uffico preposto del Comune di Zug, titolare dei diritti di amministratore nell'app uPort[124]. Dopo la verifica finale, fatta ad personam, il Comune firma crittograficamente l'ID e la invia automaticamente all'app uPort, riconoscendo quindi l'ID Zug associato all'app medesima quale identità ufficiale rilasciata dal governo. Una volta creato, l'indirizzo pubblico di Ethereum, che corrisponde all'identità dell'utente, non può essere cancellato. È garantita al cittadino che smarrisce lo smartphone con la chiave privata, la possibilità di recuperare l'accesso di identità attraverso la sostituzione della propria chiave pubblica nel contratto di identità, con la nuova chiave privata che corrisponde al nuovo dispositivo mobile. Una volta trasferita al singolo cittadino la proprietà dell'identità e riconosciuta la stessa ufficialmente dal governo, non risulterebbe più necessario ospitare server e database con le informazioni personali, con il conseguente venir meno altresì del rischio di cd. data breach, ovvero della perdita di grosse quantità di dati personali. Per i cittadini, il beneficio immediato derivante dall'operatività della soluzione Uport è da rinvenire nell'ampia ed agevole accessibilità ai servizi e quindi nell'efficienza di questi ultimi, soprattutto nei casi in cui si tratti di servizi integrati.

Inoltre, i cittadini che abilitano il loro ID Zug per uPort hanno la possibilità di utilizzare le proprie credenziali anche per il voto elettronico e per il noleggio di bici elettriche, tramite un servizio di bike-sharing denominato AirBie. Il progetto si estenderà anche ad altri servizi pubblici gestiti dalle autorità locali, quali: sondaggi, prestito di libri, dichiarazioni fiscali o pagamenti di parcheggi.

[124] J. NATION,Zug and uPort see first citizens identity registered on the ethereum blockchain, https://www.ethnews.com/zug-and-uport-see-first-citizens-identity-registered-on-the-ethereum-blockchain. (consultato il 20/06/2022)

4.5 BLOCKCHAIN E PUBBLICA AMMINISTRAZIONE

La Pubblica Amministrazione ha intrapreso un percorso di innovazione tecnologica e di digitalizzazione, iniziando a sperimentare l'utilizzo delle nuove tecnologie in contesti storicamente "tradizionali", spesso caratterizzati da stringenti vincoli normativi e burocratici. Tra le tante tecnologie disponibili, la blockchain rappresenta oggi uno dei temi di maggiore interesse per la Pubblica Amministrazione (PA) perché sono stati analizzati e compresi i benefici che possono derivare dal suo utilizzo. I concetti di trasparenza, tracciabilità e verificabilità applicati ai processi della PA consentono di migliorare l'efficienza e la qualità dei servizi offerti con vantaggi sia per gli attori interni sia nei confronti dei cittadini, i quali rappresentano gli "utenti finali" dei servizi offerti dalle Pubbliche Amministrazioni.

Le nuove tecnologie si diffondono sempre più rapidamente; l'adozione di tecnologie innovative non è più una scelta, ma una necessità per poter continuare a essere competitivi nel proprio settore di business. Anche la Pubblica Amministrazione sta intraprendendo questo percorso di "rinnovamento" non semplice; rispetto a qualche anno fa, oggi esistono fattori esogeni ed endogeni che ne incentivano fortemente l'utilizzo, abilitando un percorso di innovazione tecnologica più veloce e sicuro. D'altra parte, non potrebbe essere altrimenti; la tecnologia si evolve rapidamente e altrettanto rapida deve essere la capacità di sapersi adattare alle nuove tecnologie e di governare il processo di cambiamento.

Tuttavia, nel caso della blockchain non si tratta solo di un'innovazione tecnologica, ma di un paradigma rivoluzionario che cambia il modo di operare dal punto di vista sociale, metodologico ed applicativo. Il valore di questa tecnologia e delle sue possibili applicazioni è all'attenzione dei principali enti italiani, europei ed internazionali; da qui nascono i progetti EBSI e IBSI, rispettivamente acronimi di *European Blockchain Service Infrastructure* e *Italian Blockchain Service Infrastructure*. Entrambi hanno come obiettivo

principale quello di creare una rete blockchain in grado di supportare e valorizzare i servizi erogati dalle Pubbliche Amministrazioni, generando trasparenza e tracciabilità nei confronti dei cittadini.

L'adozione della tecnologia blockchain nella PA determina un cambio di paradigma, ma apre anche degli scenari molto interessanti; in particolare, la tecnologia consente di valorizzare il concetto di *amministrazione trasparente* e pone il cittadino al centro dell'ecosistema PA e dei relativi servizi erogati.

Le caratteristiche di immodificabilità e tracciabilità, intrinseche nella blockchain, consentono di rendere la gestione dei dati sempre trasparente nei confronti dei cittadini, delle altre PA e di altri Enti interessati; si ottiene quindi una trasparenza amministrativa e gestionale che genera fiducia tra tutti gli stakeholders dei servizi erogati dalla PA. Ciò incentiva la collaborazione tra Enti e la condivisione dei dati, rendendo i servizi sempre più efficienti e generando nuove opportunità di business per le organizzazioni. Si passa quindi da una gestione fortemente centralizzata a una gestione decentralizzata e distribuita, incentivando i concetti di interoperabilità e collaborazione; ciò consente di generare un nuovo approccio alla gestione dei dati per migliorare i modelli di business attuali e per crearne di nuovi.

Dall'altra parte il cittadino diventa *owner* dei suoi dati, supportato e tutelato dalla tecnologia blockchain che garantisce la veridicità e l'immodificabilità dei dati da lui posseduti; ciò lo rende unico proprietario dei suoi dati abilitandolo alla condivisione degli stessi, ove necessario.

Il percorso di adozione di nuove tecnologie è sempre stato ostacolato da vincoli economici e normativi, soprattutto nel contesto PA; oggi c'è la possibilità di superare tali vincoli e di accelerare un percorso di innovazione che non è più una scelta, ma una necessità. Una necessità per offrire servizi sempre più competitivi e per assicurarne una qualità sempre maggiore. La blockchain si configura come una tecnologia

abilitante che supporta tale percorso, creando un sistema basato sui concetti di trasparenza e tracciabilità e incentivando la condivisione, la collaborazione e l'interoperabilità.

4.6 LOTTA ALLA FRODE IVA

Dalle ricerche ed analisi allo stato disponibili, emerge quale riflessione convinta e condivisa quella secondo cui la blockchain è in grado di efficientare notevolmente il sistema di recupero dell'IVA, ridurre i costi di verifica e migliorare i rapporti tra i governi. Non a caso l'Osservatorio individua, quale caso di studi di interesse, l'impiego della blockchain nella lotta alle frodi IVA.

L'Osservatorio segnala come soluzione blockchain allo stato promettente, nata con l'obiettivo del contrasto alle frodi IVA, quella messa a punto da «summitto», una startup olandese. Quest'ultima sta elaborando una piattaforma blockchain autorizzata basata sul time stamping cifrato di ogni fattura e la messa a disposizione dei dati di fatturazione aggregati alle autorità fiscali. La blockchain, quindi, contiene il registro cifrato delle fatture, con indicazione temporale, il che conferisce trasparenza ed efficienza all'interno processo di verifica delle entrate da IVA, perché non solo favorisce il rilevamento delle frodi, ma permette anche di automatizzare gli obblighi di dichiarazione IVA[125].

Inoltre, i ricercatori Ainsworth & Shact e Van Engelenburg, Janssen e Klievink, si sono distinti nel sostenere i rimedi a questo tipo di frode intracomunitaria, basati su blockchain, che potrebbero portare ad una riduzione della frode IVA per un importo pari a circa 50/60 miliardi all'anno. Ainsworth & Shact nel 2016 hanno proposto un

[125] European Union Blockchain Observatory & Forum, Blockchain for governement and public services.

sistema basato su uno smart contract tra le parti del processo (venditore, acquirente con rispettive banche e l'autorità fiscale), tale per cui il sistema stesso registri i dettagli dello scambio e regoli il flusso di lavoro delle transazioni tra tutti gli attori coinvolti. Van Engelenburg, Janssen e Klievink nel 2017 hanno elaborato una soluzione che sfrutta la tecnologia blockchain nel settore e-commerce B2G, business-to-government. Tale progetto introduce una tassazione automatica e permette una condivisione rapida delle informazioni. In base a questo sistema, l'ufficio delle imposte verrebbe a conoscenza dell'ammontare delle imposte derivanti da una nuova transazione prima del pagamento, al momento dell'emissione della fattura. Per fare ciò, si richiede la registrazione sia delle transazioni che includono beni o servizi soggetti ad IVA, sia del flusso dei pagamenti, che potranno essere effettuati non su blockchain, ma off chain, tramite sistema bancario, a condizione che siano sempre elettronici e che le banche di venditore ed acquirente siano parti dello smart contract. Una volta effettuato il pagamento, quest'ultimo viene contrassegnato da un hash di transazione registrato su blockchain. A questo punto, la banca dell'acquirente scorpora l'IVA dalla somma dovuta e la trasferisce all'ufficio delle imposte corrispondente. Al venditore sarà corrisposta solo la cifra netta, unitamente alla parte dell'IVA eventualmente resa in compensazione trasferita dalla banca dell'acquirente. Il contratto intelligente, ricevute le firme digitali dei pagamenti dalle banche e dall'ufficio delle imposte, completa la transazione, cambiando lo stato di una fattura da pro-forma a fattura definitiva. Il JRC ritiene che la vera efficacia nella lotta alle frodi IVA derivante dall'operabilità di un simile sistema di registrazione degli scambi di beni/servizi e dei pagamenti IVA sia rappresentata dal fatto che la compensazione IVA in entrata e in uscita non sarebbe più effettuata dalle aziende con la trasmissione delle dichiarazioni IVA, come avviene attualmente, ma direttamente dall'ufficio delle imposte, il quale per ciascuna azienda eseguirà il proprio saldo IVA in entrata e in uscita, continuamente

aggiornato con nuove transazioni registrate su blockchain. La compensazione IVA può essere automatizzata soltanto se la banca del venditore ha accesso allo stato attuale del suo saldo IVA con l'ufficio delle imposte.

Attraverso un simile sistema, quindi, gli uffici fiscali fungeranno da nodi completi e le banche fungeranno da oracoli che certificano che è stata eseguita la scissione dei pagamenti[126].

4.7 INSURANCE BLOCKCHAIN

Una piattaforma collaborativa, in formato "sandbox", per comprendere in che modo la digitalizzazione e la tecnologia blockchain possano contribuire all'evoluzione del mercato assicurativo, in particolare alla diffusione di polizze smart e istantanee. È questo l'obiettivo di un progetto di "insurance blockchain sandbox" avviato da Cetif Università Cattolica e Reply che mette insieme un gruppo di banche e compagnie assicurative, sotto la guida di Aon Reinsurance Solutions. All'interno della Sandbox è in fase di sperimentazione una nuova piattaforma blockchain che abilita le imprese assicurative a creare nuove polizze smart parametriche che consentono di rispondere alle esigenze dei clienti con prodotti innovativi.

Una nuova concezione di prodotto grazie alla blockchain, agli smart contract e agli oracoli che abilitano la creazione di una polizza parametrica, a rimborso garantito e autoliquidante. La piattaforma permette alle imprese di personalizzare la configurazione dei prodotti e di gestire il ciclo di vita della polizza end-to-end in maniera più efficiente e veloce. La polizza, inoltre, garantisce la massima trasparenza verso il cliente che è già a conoscenza dell'importo che verrà rimborsato[127].

[126] P. Di Stefano "Blockchain e servizi pubblici", 2019.
[127] Per approfondimenti: https://www.insuranceblockchainsandbox.com (consultato il 20/06/2022)

Una prima fase del progetto prevede la creazione di tre diverse categorie di polizze *smart* legate al mondo del viaggio, a copertura del maltempo, del ritardo del volo aereo e del de-routing del bagaglio. Le polizze saranno emesse dalle imprese e, per questa fase pilota, saranno sottoscrivibili a partire da luglio da parte di un target controllato di clienti identificato dalle banche e dai distributori. Il meccanismo, già sperimentato in alcuni prodotti sul mercato, prevede la liquidazione rapida e automatica del danno agli assicurati mediante uno smart contract che utilizza gli oracoli per la verifica dell'accadimento del sinistro relativo al maltempo o al ritardo del volo. In questo modo l'assicurato non dovrà più occuparsi di tutti i passaggi burocratici per la denuncia del sinistro e il riconoscimento dell'ammontare del danno: l'importo sarà automaticamente accreditato entro il giorno successivo all'evento dannoso.

La tecnologia blockchain, quindi, può abilitare processi automatici e trasparenti a supporto dell'intera catena del valore anche per la filiera assicurativa, portando benefici a tutti in termini di efficienza e qualità del servizio. Oltre agli aspetti tecnologici, la sperimentazione darà l'opportunità di valutare l'attuale quadro normativo e regolamentare, in modo da poter verificare gli elementi di garanzia e di semplificazione per il consumatore[128].

4.8 BLOCKCHAIN PER LA TRACCIABILITÀ IN FILIERA

L'attitudine intrinseca di questo tipo di tecnologia a rendere sostanzialmente immutabili i dati in essa contenuti ed in particolare l'impossibilità per gli agenti esterni di intervenire a posteriori sui dati in questione, pone la blockchain come sistema di certificazione privilegiato per l'archiviazione dei dati di prodotto nell'ambito della

[128] https://www.ilsole24ore.com/art/aon-via-piattaforma-collaborativa-le-applicazioni-blockchain-assicurazioni-ACPUftO?refresh_ce=1 (consultato il 15/06/2022)

certificazione non solo dei beni finiti ma anche dell'intera filiera di produzione e di distribuzione di qualunque asset fisico e non solo. Il motivo per cui la blockchain può considerarsi uno strumento utile nell'ambito delle certificazioni di filiera, risiede nelle caratteristiche tecnologiche dell'infrastruttura stessa che, come si è già visto nelle parti precedenti, sono particolarmente inclini a rispondere alle garanzie di certezza, trasparenza e tracciabilità necessarie a consentire all'utente finale di avere piena consapevolezza delle caratteristiche del prodotto acquistato. In sintesi, si può dire che l'uso combinato dell'algoritmo di hash e di blockchain (che fonda la gran parte delle proprie operazioni sul medesimo algoritmo) rende i dati registrati nelle transazioni opponibili ai terzi sia dal punto di vista dei contenuti che dal punto di vista dei tempi.

4.8.1 BLOCKCHAIN NELLA SUPPLY CHAIN

L'indagine sull'applicabilità della tecnologia blockchain sembra aver trovato uno dei maggiori ambiti di applicazione nella cosiddetta supply-chain. Una questione particolare è rappresentata, innanzitutto, dalla scelta di utilizzare blockchain pubbliche o private nell'ambito della tracciabilità. Ad oggi i vari player che hanno adottato blockchain come sistema di tracciabilità hanno fatto scelte diverse tra loro (alcuni, come Carrefour in un primo momento, hanno scelto blockchain pubbliche mentre altri, come COOP, hanno optato per soluzioni a matrice privata), resta il fatto che laddove il tema della tracciabilità abbia un fondamento di natura normativa particolarmente importante così come accade, ad esempio, per il settore del food, le soluzioni pubbliche sembrano essere certamente preferibili. Ragionamento analogo vale poi per l'affidabilità dei controlli di filiera: necessariamente il dato contenuto in una blockchain pubblica tende a soddisfare maggiormente le aspettative del pubblico più attento e/o delle associazioni di categoria che si aspettano la più totale trasparenza e accessibilità del dato.

L'effettivo vantaggio dell'adozione di tecnologie basate su blockchain per l'attestazione di filiera, infatti, risiede nel fatto che tale tecnologia, specie se relativa ad un registro pubblico, offre una garanzia che nessun altro sistema, allo stato, fornisce e cioè l'impossibilità di intervenire a posteriori sui dati inseriti: ogni dato che non corrisponde alla realtà dei fatti resta attestato sul sistema e può essere, al più, oggetto di una rettifica contenuta in un blocco diverso ma mai oggetto di modifica.

Ad oggi chi ha adottato soluzioni blockchain per la certificazione delle filiere ha, sostanzialmente, trasportato su blockchain riferimenti relativi al complesso documentale già presente per la gestione del business ma diverse realtà tecnologiche sono già pronte con sistemi IoT capaci di tracciare il percorso e le condizioni di trasporto di un determinato bene. Si pensi ad esempio all'importanza della tracciabilità delle condizioni di trasporto del vino: l'adozione di un chip di rilevazione agganciato al collo della bottiglia che rilevi inclinazione, temperatura e spostamento consentono, all'arrivo della bottiglia sulla tavola, di verificare che quel prodotto è stato correttamente conservato e gestito e che eventuali problematiche legate al gusto o alla composizione organolettica vanno ricercate altrove rispetto alle modalità di trasporto.

4.8.2 BLOCKCHAIN NEL MONDO DEL FOOD

Prima di esaminare il rapporto che intercorre tra questa tecnologia e il food, è importante menzionare qualche dato economico. In Italia, Coldiretti, secondo gli ultimi dati, ha denunciato che il valore del falso "Made in Italy" agroalimentare nel mondo supererebbe i 100 miliardi di euro.

Sul tema della sicurezza agroalimentare sin dal 2002 è vigente il Regolamento (CE) n. 178/2002[129], recante "Principi e requisiti generali della legislazione alimentare,

[129] https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002R0178:20060428:IT:PDF

istituzione dell'Autorità europea per la sicurezza alimentare e indicazione di procedure nel campo della sicurezza alimentare" che contiene le regole sulla sicurezza di alimenti e mangimi nell'Unione Europea e vieta la vendita di alimenti pericolosi per la salute.

Il citato Regolamento si applica a tutte le fasi della catena alimentare (produzione, trasformazione e trasporto, distribuzione e fornitura) e, sul tema della tracciabilità, lascia pochissimi margini interpretativi. Tuttavia, i dati dimostrano che i casi di frodi e di irregolarità dei prodotti alimentari sono ancora presenti in buona parte, ecco perché risulta necessario sviluppare un meccanismo di riposta per prevenirli e combatterli. Non soltanto per tutelare la salute pubblica, ma anche perché gli attori della filiera che producono e commerciano i prodotti alimentari dipendono dalla fiducia dei consumatori; se la fiducia viene meno, la loro attività è a rischio[130]. Tecnologie come la blockchain, l'Internet of Things (IoT) e l'etichettatura intelligente possono diventare modalità molto più sofisticate e trasparenti di tracciare la supply chain 37 alimentare. Offrono il vantaggio aggiuntivo di una conformità normativa più semplice e di un utilizzo ottimizzato dei dati, garantendo al tempo stesso la sicurezza dei prodotti per il consumo umano.

Tutte le transazioni relative a un prodotto alimentare possono essere convalidate in ogni momento sulla blockchain. Questa trasparenza significa che qualsiasi tentativo di manomettere un prodotto alimentare lungo la supply chain può essere rapidamente identificato e il prodotto fermato prima che raggiunga la sua destinazione. Ecco perché la tecnologia Blockchain potrebbe essere un ottimo strumento per contrastare i fenomeni della contraffazione, dell'adulterazione e della sofisticazione dei prodotti, garantendo la certificazione della corretta conservazione durante il trasporto delle merci, la registrazione dei prodotti da commercializzare, e un monitoraggio lungo

[130] Tesi di Laurea Magistrale in scienze e tecnologie alimentari "Il concetto di frode alimentare e l'attività di repressione dell'ICQRF: norme e casi" di Arianna Cacciotti

l'intera supply chain, fornendo un utile aiuto per contrastare i pericoli di possibili manipolazioni. L'utilizzo della blockchain garantirebbe così l'integrità delle informazioni documentali. Si potrebbero identificare rapidamente lotti specifici in qualsiasi fase, rintracciare eventuali prodotti scaduti o contaminati, eliminandoli dalla distribuzione.

La blockchain è in grado di compiere un ulteriore passo avanti e di fornire informazioni alimentari direttamente al consumatore. Tramite un codice QR e uno smartphone, i consumatori possono scansionare un prodotto in negozio e ricevere una cronologia completa della sua provenienza come registrata nella blockchain.

Un sistema di rintracciabilità piena, in direzione della massima trasparenza, con ridotte criticità, potrebbe essere realizzato, ricorrendo alla blockchain e alla combinazione di algoritmi appropriati. Difatti, ci sonno alcune sperimentazioni in corso.

Nel 2018, per esempio, Carrefour è stato il primo rivenditore europeo ad introdurre la tecnologia blockchain per i prodotti alimentari, in particolare per i polli allevati all'aperto della linea Carrefour Quality Auvergne. Il segretario generale di Carrefour Laurent Vallée ha confermato che il gruppo estenderà l'uso del sistema ad altri prodotti freschi in tutto il mondo entro il 2022, garantendo una supply chain sicura e trasparente, consentendo ai clienti di avere fiducia nel loro cibo. Un altro esempio è Wine Blockchain EY, sviluppata da EY Italia, in collaborazione con la startup EZ LAB e con la Cantina Volpone[131]. Si tratta di un progetto blockchain a tutela dal Made in Italy agroalimentare in grado di difendere la qualità colturale e offrire una soluzione di supporto alla trasparenza del ciclo produttivo.

Di fatto, è la prima soluzione al mondo per la tracciabilità della filiera di produzione del vino: grazie all'utilizzo di un'etichetta intelligente, posta sulla bottiglia di vino, il consumatore verifica, tramite smartphone o altri "mobile device", la "carta d'identità

[131] https://www.ezlab.it/it/i-nostri-casi-di-studio/wine-blockchain/ (consultato il 22/06/2022)

digitale" del prodotto, dalla proprietà all'intero processo di coltivazione, di produzione e di trasformazione del vino, fino alla sua distribuzione.

Il settore ad oggi è in grande fermento e diversi marchi nazionali e internazionali corrono verso un cambio di rotta che contempla la tecnologia blockchain come asse del business della distribuzione.

4.8.3 BLOCKCHAIN NEL MONDO DEL FASHION

Anche per il "fashion" è bene partire dai numeri: l'OCSE, a partire dai dati forniti dalle autorità doganali, ha quantificato in circa 461 miliardi di dollari il valore del commercio internazionale di merci contraffatte nel 2013, pari a circa il 2,5% del totale degli scambi mondiali.

Anche in questo caso, dunque la tecnologia di cui si discute interviene in un contesto che coinvolge interessi economici che hanno le cifre di una manovra economica. La tutela della provenienza dei beni, in Europa, è disciplinata, in via principale, dall'art. 60 del Regolamento (UE) n. 952/2013 a norma del quale «Le merci alla cui produzione hanno contribuito due o più paesi o territori sono considerate originarie del paese o territorio in cui hanno subito l'ultima trasformazione o lavorazione sostanziale ed economicamente giustificata, effettuata presso un'impresa attrezzata a tale scopo, che si sia conclusa con la fabbricazione di un prodotto nuovo o abbia rappresentato una fase importante del processo di fabbricazione». Anche in questo caso, dunque per i produttori diventa centrale poter dimostrare in qualunque momento non solo la provenienza delle materie prime o dei semilavorati ma anche il luogo e le modalità di lavorazione dei prodotti finiti, pena l'applicazione delle pene introdotto dall'articolo 4 comma 49 della legge n. 350 del 2003 con la quale è stata attribuita rilevanza penale alle ipotesi di importazione, esportazione e commercializzazione di prodotti recanti false o fallaci indicazioni di origine. Nel settore del "fashion", dunque la tracciabilità

diventa parte integrante della c.d. "user experience" e contribuisce a stringere ancor di più il legame tra il brand e l'acquirente laddove quest'ultimo possa contare sulla possibilità di verificare non solo l'autenticità del prodotto ma anche tutti i passaggi della lavorazione.

Ad oggi i grossi brand del luxury parlano di blockchain senza sbilanciarsi troppo o riferendosi ad un futuro prossimo mentre invece altre realtà meno blasonate ma particolarmente attive, combinando tecnologie NFC e RFID, stanno già sperimentando tale tecnologia nel loro approccio al mercato: è il caso della cinese Babyghost, unearly adopter che già dalla fine del 2016, utilizzando la tecnologia VeChain, consentiva la completa tracciabilità di prodotti e lavorazioni per alcuni dei capi commercializzati; altra esperienza interessante che, pur collocandosi ai margini del mondo del fashion inteso in senso stretto, sta realizzando un progetto interessante è la start up bulgara KingFootball che, tra le altre cose, si propone di utilizzare la tecnologia blockchain per garantire l'autenticità degli acquisti fatti dai tifosi di capi o gadget appartenuti alle star del calcio o realizzati dai brand sportivi.

La tracciabilità dei beni insomma è, ad oggi, un progetto che corre veloce su diversi fronti e che è suscettibile di modificare in maniera sensibile la nostra percezione dei consumi e forse anche il modo in cui consumiamo beni e servizi in un sistema win windove il produttore si avvantaggia, tra le altre cose, anche della trasparenza con cui si pone nei confronti dell'utente che sarà più libero di orientare in maniera consapevole le proprie scelte[132].

4.8.4 BLOCKCHAIN NEL MANUFACTURING: L'INDUSTRIA 4.0

La digitalizzazione avanzata all'interno delle fabbriche sta portando sempre più un ecosistema omnicomprensivo, che connette direttamente il prodotto che viene

[132] P. Lessio "Blockchain e tracciabilità in filiera", 2019.

realizzato alle fabbriche stesse, fabbriche che sono a loro volta interconnesse, alle supply chain, ai clienti e a vari altri stakeholder definiti olisticamente come il Mondo connesso. La combinazione di tecnologie Internet e altre tecnologie orientate alla gestione ed elaborazione dei dati è pronta a provocare un cambio di paradigma nella produzione industriale che definisce oggi la cosiddetta industria 4.0[133].

L'Industria 4.0 ci offre una visione di business principalmente basata sull'automazione, inclusi servizi, prodotti e fabbriche smart, dove molte sono le opportunità per lo sviluppo di idee rivoluzionarie nella produzione industriale. La creazione di un ambiente così automatizzato richiede la connettività ad Internet di un gran numero di oggetti insieme, sfruttando ovvero l'internet of things (IoT). Per ovvi motivi, tali oggetti potrebbero essere pericolosamente esposti agli aggressori hacker, ed è per questo che, da alcuni decenni, molte tecniche crittografiche vengono utilizzate per proteggere le informazioni sensibili nella comunicazione o nella memoria. Inizialmente queste tecniche erano utilizzate solo nei sistemi di sicurezza delle informazioni, ma poi sono state impiegate per lo sviluppo di una tecnologia dirompente, qual è la blockchain, così da permettere la gestione e lo scambio dei dati in via decentralizzata.

L'idea della tecnologia blockchain ha suscitato molto interesse perché, senza il coinvolgimento di terzi, fornisce integrità, sicurezza e anonimato dei dati. L'implicazione della blockchain nell'Industria 4.0 ha generato una grande quantità di innovazioni che ci rendono ora in grado di adattarci a un nuovo modello di business ottimizzato, flessibile e più efficiente, basato sulla fiducia e la sicurezza di tutte le parti interessate[134]. In particolare, tale tecnologia è di grande aiuto ove i consumatori finali

---

[133] Il termine Industria 4.0 è la propensione dell'odierna automazione industriale ad inserire alcune nuove tecnologie produttive per migliorare le condizioni di lavoro, creare nuovi modelli di business, aumentare la produttività degli impianti e migliorare la qualità dei prodotti. Sul miglioramento delle condizioni di lavoro non vi è un sostanziale accordo tra gli studiosi. Per alcuni, infatti, il miglioramento delle condizioni di lavoro sarebbe solo una promessa, peraltro non inedita, che ogni trasformazione tecnico-organizzativa porta con sé. https://it.wikipedia.org/wiki/Industria_4.0

[134] https://www.blockchain4innovation.it/mercati/industria4-0/industria-4-0-come-e-dove-arriva-il-valore-della-blockchain/ (consultato il 23/06/2022)

sono sempre più interessati a scoprire l'esatta tracciabilità dei prodotti acquistati e per le istituzioni sempre più severe nei controlli di filiera e dei processi di produzione.

Oltre ai dati dei fornitori, i dati e i movimenti di prodotti e materiali possono essere registrati sulla blockchain, mantenendo in memoria anche i dati storici e dichiarando l'origine del prodotto, la qualità, la quantità, i proprietari e il tempo intercorso tra un passaggio e l'altro. Queste informazioni assicurano che i clienti siano consapevoli della produzione e del trasporto di merci sicure e sostenibili. La capacità di tracciare la fonte dei prodotti per affrontare le preoccupazioni relative alla biodiversità e il contributo dei prodotti all'esaurimento delle risorse naturali sono due casi che dimostrano il ruolo delle blockchain nel garantire la sostenibilità dei prodotti. Utilizzando la tecnologia blockchain, l'analisi del ciclo di vita dei prodotti può essere completata utilizzando i dati del prodotto reale, piuttosto che stimando i valori, come negli attuali metodi di analisi del ciclo di vita.

Per essere veramente efficace, l'azione di registrazione dei dati su blockchain dovrebbe essere espletata a tutti i livelli della catena di approvvigionamento. Le industrie con catene di fornitura incredibilmente complesse dovranno affrontare una battaglia molto più grande in termini di implementazione di tale tecnologia come garanzia di qualità dei propri prodotti, in quanto fare ciò significherebbe richiedere a ogni singolo fornitore e distributore di condividere e adottare tali pratiche. Le aziende con catene di fornitura più semplici o che gestiscono la produzione di un prodotto dall'inizio alla fine, saranno invece facilitate quando la blockchain diventerà più diffusa.

Inoltre, dal 21 settembre 2022 le imprese e i centri di ricerca pubblici o privati, anche in forma congiunta tra loro, potranno richiedere agevolazioni per realizzare progetti di ricerca e innovazione tecnologica finalizzati al sostegno e allo sviluppo delle tecnologie

e delle applicazioni di intelligenza artificiale, blockchain e internet of things nei settori strategici prioritari[135].

Infatti, è stato pubblicato dal Ministero dello sviluppo economico (MISE) il decreto che rende note le modalità e i termini di presentazione delle domande per richiedere i finanziamenti del "Fondo per lo sviluppo delle tecnologie e delle applicazioni di intelligenza artificiale, blockchain e internet of things", istituito dall'art. 1, comma 226 della legge di bilancio 2019, con una dotazione complessiva pari a 45 milioni di euro.

A partire dal 21 settembre 2022, quindi, le imprese e i centri di ricerca pubblici o privati, anche in forma congiunta tra loro, potranno richiedere le agevolazioni per realizzare progetti di "ricerca industriale", "sviluppo sperimentale", "innovazione dell'organizzazione" e "innovazione di processo" legati al programma Transizione 4.0.

Nei percorsi di sviluppo dell'Industria 4.0 la Blockchain è chiamata a svolgere un ruolo sempre più importante e appare ormai chiaro che questa tecnologia può permettere a tante imprese di trovare nuove forme di efficienza e nuova competitività.

4.8.5 BLOCKCHAIN PER L'AGRICOLTURA

In agricoltura è in corso una rivoluzione tecnologica che negli ultimi anni è proseguita nonostante la pandemia spinta soprattutto dai miglioramenti promessi sul piano dell'efficienza e della sostenibilità. Negli ultimi due anni, infatti, in Italia gli investimenti in tecnologie di Agricoltura 4.0[136] sono esplosi passando da un fatturato di 540 milioni

[135] https://www.blockchain4innovation.it/istituzioni-e-associazioni/mise-45-milioni-di-euro-di-incentivi-per-blockchain-ia-e-iot/ /(consultato il 15/05/2022)

[136] L'agricoltura 4.0 è il risultato dell'applicazione di una serie di tecnologie innovative nel campo dell'agrifood, e può essere considerata come un "upgrade" dell'agricoltura di precisione. Questo grazie all'automatizzazione della raccolta, dell'integrazione e dell'analisi dei dati che provengono direttamente dai campi grazie a sensori e altre fonti.
Le tecnologie digitali 4.0 in questo contesto sono utili per supportare – grazie all'analisi dei dati – l'agricoltore nella sua attività quotidiana e nella pianificazione delle strategie per la propria attività, compresi i rapporti con tutti gli anelli della filiera, generando un circolo virtuoso in grado di creare valore per la singola azienda e a cascata per i suoi partner. Grazie a queste nuove soluzioni e all'applicazione delle tecnologie digitali così, dall'IoT all'intelligenza artificiale, dall'analisi di grandi quantità di dati ai trattori a guida autonoma fino all'utilizzo dei droni, le aziende agricole possono aumentare la profittabilità e la sostenibilità economica, ambientale e sociale della propria attività.

di euro nel 2019 agli 1,3 miliardi del 2020 per poi approdare a 1,6 miliardi di euro a fine 2021 con un ulteriore balzo del 23% in 12 mesi.

A livello mondiale si stima un giro d'affari dell'agritech di circa 15 miliardi di dollari e oltre 750 startup attive. In questo contesto l'Italia è nella top ten dei paesi che contano il maggior numero di startup.

A guidare gli investimenti la spesa per macchine e attrezzature agricole nativamente connesse che coprono una quota di quasi la metà (il 47%) del mercato delle tecnologie di Agricoltura 4.0 e hanno registrato un progresso del 17%. A seguire il segmento dei sistemi di monitoraggio e controllo applicabili a mezzi e attrezzature agricole post-vendita (35%)[137].

È quanto emerge dal rapporto 2022 su Agricoltura 4.0 messo a punto dall'Osservatorio Smart AgriFood della School of Management del Politecnico di Milano e del Laboratorio Rise (Research & Innovation for Smart Enterprises) dell'Università degli Studi di Brescia, presentata nel corso del webinar "Smart agrifood: raccogliamo i frutti dell'innovazione digitale!".

Tra i progressi registrati dalla ricerca c'è l'incremento, in Italia, delle superfici coltivate con strumenti di Agricoltura 4.0 che nel 2021 hanno toccato il 6% del totale, il doppio dell'anno precedente. «Il 60% degli agricoltori italiani – si legge nella ricerca – utilizza almeno una soluzione di Agricoltura 4.0, +4% rispetto al 2020, e oltre quattro su dieci ne utilizzano almeno due, in particolare software gestionali e sistemi di monitoraggio e controllo delle macchine. Si segnala anche la crescente attenzione ai sistemi di analisi dei dati e supporto delle decisioni, confermata dal 26% di aziende agricole che prevede investimenti in questo ambito per il prossimo futuro».

[137] https://www.ilsole24ore.com/art/agricoltura-40-investimenti-16-miliardi-2021-23percento-AEBw7lIB (consultato il 26/06/2022)

Sempre più centrale sarà il ruolo dei dati e la loro valorizzazione lungo tutta la filiera. E del resto, l'indagine sui consumatori finali conferma che gli italiani sono sempre più attenti alla tracciabilità e alle caratteristiche di ciò che mettono nel piatto. E, in questa linea, il settore agroalimentare continua a guardare con forte interesse alle tecnologie blockchain. Ma sarà necessario incrementare la cultura digitale e la fiducia nelle potenzialità delle tecnologie. Oggi, infatti, solo una minoranza degli italiani impiega in modo sistematico strumenti digitali per informarsi su ciò che acquista e meno della metà di quelli che conoscono la blockchain hanno fiducia nelle sue potenzialità per la sicurezza.

4.9 L'IMPIEGO DELLA BLOCKCHAIN IN AMBITO SANITARIO

L'utilizzo della blockchain potrebbe rivelarsi strategico per la gestione dei dati sanitari per molteplici ragioni: in primo luogo, i dati sui pazienti sono di grande interesse per il Servizio Sanitario Nazionale - SSN (che dispone di grandi quantità di *feedback* sull'erogazione del suo servizio), risultando utili anche per le imprese, per le compagnie di assicurazione (che con i *Big Data* possono migliorare la valutazione del rischio clinico di ciascun assicurato) e per i ricercatori.

Nell'attuale contesto sanitario possono contemplarsi diversi scenari di trattamento e di scambio informatizzato di informazioni, senza che i dati vengano verificati in modo standardizzato. In tal senso la blockchain potrebbe offrire un modello di condivisione sicura delle cartelle cliniche con un controllo intelligente dell'accesso ai record senza che si debbano creare funzionalità personalizzate per ciascun produttore di informazioni sanitarie[138].

[138] Halamka, J. D., Lippman, A., & Ekblaw, A. (2017). The potential for blockchain to transform electronic health records. Retrieved from https://hbr.org/2017/03/the- potential-for-blockchain-to-transform-electronic-health-records.

Come è noto, l'analisi dei dati può risultare strumentale al godimento dei diritti fondamentali alla salute e alla integrità della persona, consentendo incrementi qualitativi dell'assistenza sanitaria e delle decisioni cliniche. Rapportata ai parametri costituzionali degli articoli 32 e 97, le inflessioni potrebbero sintetizzarsi in un incremento qualitativo della sorveglianza delle malattie e, più in generale, della gestione della salute pubblica, muovendo verso un radicale riassetto del sistema di prevenzione, diagnosi e cura. Tra i possibili risvolti applicativi, in questi casi, la *blockchain* potrebbe soddisfare esigenze di certezza dell'identità digitale (per esempio del paziente), oltre che di tracciamento certo e sicuro, anche dal punto di vista cronologico, di operazioni come le prescrizioni mediche, le somministrazioni di farmaci e la corretta applicazione dei protocolli terapeutici. L'utilizzo di algoritmi per personalizzare le condizioni che determinano il trasferimento di informazioni o l'automatica generazione di eventi, che vengono tracciati con garanzia di immodificabilità, soddisfa le esigenze tipiche delle cartelle cliniche elettroniche e, più, in generale della gestione EHR (*Electronic Health Record*), fino ad arrivare ad applicazioni più elaborate nell'assistenza sanitaria, come le autorizzazioni preventive e l'elaborazione automatica dei dati. Si pensi, inoltre, alla possibilità di tracciamento del corretto funzionamento dei dispositivi medicali, attraverso una sorta di scatola nera basata sulla *blockchain*.

Nonostante lodevoli iniziative straniere[139], in partenariato tra pubblico e privato, per lo sviluppo di soluzioni basate su blockchain per l'industria e il mercato sanitario, in Europa il contesto è ancora parzialmente impreparato ad affrontare la transizione verso un'utilizzazione più intensiva delle nuove tecnologie: invero, l'impegno manifestato dalle istituzioni europee si è ripiegato sulla predisposizione di direttive che

[139] Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016). A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical researchdata, White paper. MIT Media Lab, Beth Israel Deaconess Medical Center; Health Data Management. (2017). FDA, IBM Watson health to study application of blockchain technology. Fred Bazzoli, 12(5), 1.

interessano la *e- health*[140] e i problemi connessi alla privacy. Già dal 2016, a questo proposito, è stato pubblicato un *white paper* intitolato "*How Blockchain Technology Can Enhance EHR Operability*"[141], nel quale si evidenzia la necessità di modernizzare la gestione delle cartelle cliniche elettroniche, favorendo una migliore e più sicura condivisione tra i soggetti autorizzati, così da migliorare l'interazione tra operatori sanitari e pazienti. Nel documento si evidenzia l'eterogeneità dell'attuale sistema informativo sanitario e la necessità di una cartella clinica digitale e unificata. Una condivisione connotata da interoperabilità, che sia sufficientemente flessibile a consentire l'accesso istantaneo ai dati sanitari, sulla base delle esigenze del momento e che protegga da accessi non autorizzati o da tentativi di intrusione.

Per gli autori del *white paper*, l'impiego proficuo della blockchain in sanità può conseguirsi in relazione al verificarsi di tre *conditiones sine qua non*: (i) l'immutabilità dei file, (ii) la sicurezza informatica e (iii) l'interoperabilità.

Nell'ordine, la prima può essere ottenuta attraverso le funzionalità di integrità dei record in essi contenuti; la sicurezza informatica può invece essere garantita dalla gestione puntuale dell'accesso ai dati; l'interoperabilità, infine, assicura il controllo condiviso e collaborativo delle diverse versioni del file.

Nell'attuale contesto storico di bulimia dei dati, la tecnologia *blockchain* può permettere di organizzare l'accesso ai dati in modo tale che questo possa avvenire solo previo il consenso (implicito) di tutte le parti coinvolte, al fine di realizzare un sistema interconnesso tra ospedale e territorio. Riflettendo sulle possibili dinamiche operative, i dati sanitari completi potrebbero non essere memorizzati nella blockchain, la cui

---

[140] Si pensi alla direttiva 2011/24/UE, che istituisce una rete volontaria di autorità nazionali responsabili dell'assistenza sanitaria online.

[141] Chris Burniske, Emily Vaughn, Jeff Shelton, Alex Cahana, "*How Blockchain Technology Can Enhance EHR Operability*" (2016) consultabile al seguente link: https://www.hyperledger.org/wpcontent/uploads/2016/10/ARKInvest_and_GEM_Blockchain_EHR_Fina l.pdf

operatività potrebbe limitarsi alla mera raccolta delle informazioni minime utili a convalidare i contenuti, per definire la topologia dei punti (corrispondenti ai singoli blocchi) nei quali sono stati suddivisi i diversi elementi del documento completo.

Rispetto alle soluzioni precedenti, tese alla modernizzazione del settore, la *blockchain* si differenzia per la sua capacità di facilitare lo scambio di informazioni sanitarie attraverso un'architettura decentralizzata, insuscettibile di manomissione e flessibile rispetto alle soluzioni unificate. Questo permetterebbe di creare una libreria sicura e condivisa di dati sanitari richiamabili dai diversi soggetti interessati: i medici, anzitutto, che grazie alle *blockchain* hanno la facoltà di condividere i dati inseriti in una EHR; quest'ultima sarà quindi disponibile per i fornitori autorizzati (come le compagnie di assicurazione) e i membri del gruppo ospedaliero. I pazienti, che sono in grado di monitorare le proprie informazioni di salute approvando, negando o condividendo le modifiche ai propri dati, il tutto con la garanzia di un altissimo livello di privacy con una forma reale di telemedicina che permette di creare nuove progettualità per la *Smart Health*. I ricercatori, che potranno beneficiare di una migliore integrità e affidabilità dei dati ottenuta attraverso la creazione di una piattaforma di fiducia (trust) per la loro condivisione. I contribuenti, infine, che sperimenteranno una migliore riconciliazione dei dati, con un deciso abbattimento di errori e tentativi di frode e una riduzione dei costi di elaborazione amministrativa dei sinistri.

4.10 VOTO ELETTRONICO (E-VOTING) TRAMITE BLOCKCHAIN

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. 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[142] (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

[142] EPRS | Servizio Ricerca del Parlamento europeo Autore: Philip Boucher Unità Prospettiva scientifica (STOA) PE 581.948

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).

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.

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).

CONCLUSIONI

Nessuno poteva immaginare un così articolato sviluppo della blockchain alla nascita di Bitcoin nel 2009 e, soprattutto, nessuno avrebbe immaginato come tutti i settori dell'economia sarebbero stati interessati a questa "rivoluzione" tecnologica.

La tecnologia blockchain, con le sue caratteristiche cardine di decentralizzazione, disintermediazione e pseudonimia, rappresenta un vero cambio di paradigma relazionale che, di conseguenza, non può che sollevare aspetti di rilievo giuridico del tutto nuovi e inesplorati.

All'esito della disamina compiuta nell'elaborato, appare evidente che i sistemi giuridici che hanno accolto con maggior fervore questa tecnologia, siano quelli di common law, i quali, non avendo mai avuto sistemi di questo genere, vedono in questa tecnologia la possibilità di implementare efficaci sistemi di tracciamento. Tuttavia, si è evidenziato che anche negli ordinamenti di civil law, nei quali la presenza di registri pubblici dotati di caratteristiche simili sia già presente, non stiano mancando tentativi lodevoli di approccio giuridico il che è certamente dimostrazione di forte attenzione verso questa dirompente tecnologia che avrà sicuri impatti positivi sul modo di gestire i rapporti contrattuali a livello nazionale e internazionale.

I profili giuridici sollevati, come notato, meritano un'attenzione non arrendevole. Sarà arduo compito dei giuristi e dei legislatori trovare la via maestra per una congrua simbiosi fra il diritto e la tecnologia.

Si tratta chiaramente di un tema sul quale saremo chiamati a discutere a lungo negli anni che verranno. Certamente, le teorie più libertarie della blockchain consentono di immaginare una sorta di nuovo ordine di respiro globale e capace di guardare al futuro. Inoltre, i principali vantaggi della blockchain, come evidenziato, si riscontrano all'interno dell'industria 4.0. Vi è, infatti, la particolare versatilità e la possibilità di

utilizzare questa tecnologia anche per certificare i diversi passaggi dei prodotti lungo le filiere. In particolare, la blockchain consente di realizzare obiettivi di decentralizzazione, trasparenza, sicurezza e immutabilità dei dati.

La tecnologia Blockchain potrebbe essere anche utilizzata per contrastare i fenomeni della contraffazione, dell'adulterazione e della sofisticazione dei prodotti, garantendo la certificazione della corretta conservazione durante il trasporto delle merci, la registrazione dei prodotti da commercializzare, e un monitoraggio sicuro lungo l'intera *supply chain*, fornendo un utile aiuto per contrastare i pericoli di possibili manipolazioni, garantendo, quindi, l'integrità delle informazioni documentali.

La tracciabilità dei beni e delle merci, quindi, è ad oggi un processo che corre veloce e che è suscettibile di modificare sensibilmente la nostra percezione dei consumi, in un sistema in cui il produttore si avvantaggia, tra le altre cose, della trasparenza con cui si pone nei confronti dell'utente che sarà più libero di orientare in maniera consapevole le proprie scelte di consumo.

La strada è certamente ancora lunga e molte altre pagine dovranno scriversi per questo fenomeno e per un futuro che sarà, di certo, sempre più decentralizzato, più trasparente, più sicuro.

Insomma, più Blockchain.

BIBLIOGRAFIA

- AQUARO D., Smart contract: cosa sono le clausole su blockchain https://www.ilsole24ore.com/art/smart-contract-cosa-sono-e-come-funzionano-clausole-blockchain-ACsDo2P , 2019.
- BARCELO J., User Privacy in the Public Bitcoin Blockchain, Journal of Latex Class Files, Vol. 6, No. 1, January 2007.
- BATTAGLINI. R., GIORDANO M., Blockchain e smart contract: funzionamento, profili giuridici e internazionali, applicazioni pratiche, 2019.
- BELLINI M., Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia, 2022. https://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosi-importante/
- BELLINI M., Che cos'è la European Blockchain Partnership https://www.blockchain4innovation.it/istituzioni-e-associazioni/cose-la-european-blockchain-partnership/#Limpegno_dellEuropa_si_sviluppa_anche_con_lEU_Blockchain_Observatory_and_Forum , 2017.
- BERBERICH M., M. STEINER, Blockchain technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers?, 2016.
- BIANCONI A., Smart contract e blockchain: l'Italia prova a guidare in Europa https://www.blockchain4innovation.it/esperti/smart-contract-e-blockchain-litalia-prova-a-guidare-in-europa/ , 2019.
- BOMPREZZI C., Blockchain e assicurazione: opportunità e nuove sfide, in Diritto, Mercato, Tecnologia, 7 luglio 2017.
- BURNISKE C., VAUGHN E., JEFF SHELTON, ALEX CAHANA, "How Blockchain Technology Can Enhance EHR Operability", 2016.

- CACCIOTTI A., Tesi di Laurea Magistrale in scienze e tecnologie alimentari "Il concetto di frode alimentare e l'attività di repressione dell'ICQRF: norme e casi".
- CAMPOBASSO, GIAN FRANCO, Diritto Commerciale 3: Contratti, Titoli di credito, Procedure concorsuali, Torino, 2014.
- CERRATO S., Contratti tradizionali, diritto dei contratti e smart contract, in Blockchain e Smart Contract, a cura di Raffaele BATTAGLINI, Marco GIORDANO, Giuffrè Francis Lefebre, Milano, 2019.
- CHANG H., Blockchain: Disrupting data protection?, 150 Privacy Laws & Business International Report, SSRN, 2017.
- CHAUM D.,:"Security without Identification: Transaction Systems to Make Big Brother Obsolete", pubblicato nel 1985.
- CIACCI G., Blockchain e privacy, Corso blockchain, Camera Civile Roma, 2022.
- CIARAVINO C., TRIDICO T., Protocollo Bitcoin: la più grande rivoluzione dopo internet. Come la blockchain e le crypto stanno cambiando il mondo, 2022.
- CNIL (Commission National Informatique et liberté), Premiers éléments d'analyse de la Blockchain, reperibile all'indirizzo https://www.cnil.fr/sites/default/files/atoms/files/lablockchain.pdf
- COMANDINI G.L., Da zero alla luna: quando come perché la blockchain sta cambiando il mondo, 2020.
- DAL CHECCO P., "Blockchain analysis, digital forensics e indagini digitali attraverso blockchain" 2019.
- DE FILIPPI V.P., The interplay between decentralization and privacy: the case of blockchain technologies.

- DELFEDERICO V.C., A. R. POPOLI, Disposizioni generali, in G. Finocchiaro (a cura di), Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali.
- DELFINO D., Blockchain e Smart contract, https://www.filodiritto.com/blockchain-e-smart-contract , 2021.
- DELL'OREFICE G. Agricoltura 4.0, investimenti a 1,6 miliardi nel 2021 https://www.ilsole24ore.com/art/agricoltura-40-investimenti-16-miliardi-2021-23percento-AEBw7lIB
- DI STEFANO P., "Blockchaine servizi pubblici", in Blockchain e Smart Contract, a cura di Raffaele BATTAGLINI, Marco GIORDANO, Giuffrè Francis Lefebre, Milano 2019.
- EKBLAW, A., AZARIA, A., HALAMKA, J. D., & LIPPMAN, A. (2016). A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical researchdata, White paper. MIT Media Lab, Beth Israel Deaconess Medical Center; Health Data Management, 2017.
- FABIANO N., The Internet of Things ecosystem: the blockchain and privacy issues. The challenge for a global privacy standard, Advances in Science, Technology and Engineering Systems Journal, Vol. 3, No. 2, 2018.
- FERRONETTI F. e SACCO V., Blockchain e smart contract, servono regole chiare: lo scenario, https://www.agendadigitale.eu/documenti/blockchain-e-smart-contract-servono-regole-chiare-lo-scenario/ , 2021
- FINCK M., Blockchains and Data Protection in the European Union, 2018.
- FINOCCHIARO G., Privacy e protezione dei dati personali, Zanichelli, 2012.
- FLORINDI E., Criptovalute: manuale di sopravvivenza. [ebook]

- GAMBINO A. M., BOMPREZZI C., BLOCKCHAIN E PROTEZIONE DEI DATI PERSONALI, Diritto dell'Informazione e dell'Informatica (Il), fasc.3, 2019.
- GUIDA G., Blockchain e smart contract: benefici e limiti, https://www.altalex.com/documents/news/2020/10/21/blockchain-smart-contract-benefici-limiti , 2020
- HALAMKA, J. D., LIPPMAN, A., & EKBLAW, A. (2017). The potential for blockchain to transform electronic health records.
- HALPIN H., M. PIETRASKA, Introduction to Security and Privacy on the Blockchain, 2nd Ieee European Symposium on Security and Privacy Workshops, aprile 2017.
- LESSIO P., "Blockchain e tracciabilità in filiera", in Blockchain e Smart Contract, a cura di Raffaele BATTAGLINI, Marco GIORDANO, Giuffrè Francis Lefebre, Milano 2019.
- LYONS T., COURCELAS L., TIMSIT K., Blockchain and the GDPR - a thematic report prepared by the European Union Blockchain Observatory and Forum, 16 ottobre 2018.
- MARCHESONI E. Industria 4.0 come e dove arriva il valore della blockchain https://www.blockchain4innovation.it/mercati/industria4-0/industria-4-0-come-e-dove-arriva-il-valore-della-blockchain/
- MAUGERI M. *Smart contracts e disciplina dei contratti,* 2021.
- MIOZZI L. blockchain: le possibili applicazioni nella PA https://www.blockchain4innovation.it/mercati/pubblica-amministrazione/blockchain-le-possibili-applicazioni-nella-pubblica-amministrazione/

- MORELLI C. Smart contract. Il codice equivale alla forma scritta https://www.altalex.com/documents/news/2021/11/08/smart-contract-codice-equivale-forma-scritta#p6
- MOSER J., The Application & Impact of the European General Data Protection Regulation on Blockchains, R3 Reports, 2017.
- NAKAMOTO, Satoshi *Bitcoin: a Peer-to-Peer Elettronic Cash System*; https://bitcoin.org/bitcoin.pdf , 2009.
- NICK J.D., "Data-Driven De-Anonymization in Bitcoin", 2015.
- NICOTRA M., L'Italia prova a normare gli smart contract, ecco come: pro e contro, https://www.agendadigitale.eu/documenti/litalia-prova-a-normare-gli-smart-contract-ecco-come-pro-e-contro/ , 2019.
- NIGRO R. Smart contract profili di qualificazione giuridica https://www.altalex.com/documents/news/2021/06/29/smart-contract-profili-di-qualificazione-giuridica
- PINNA A., RUTTENBERG W., Distributed ledger technologies in securities post-trading, in ECB Occasional Paper, 2016.
- ROUGHTON T., BIDEWELL P., Smart insurance contracts, Pinsent Masons, 2017.
- SALERNO A. Agricoltura 4.0: cos'è, incentivi e tecnologie abilitanti https://www.agrifood.tech/precision-farming/agricoltura-4-0-cose-incentivi-e-tecnologie-abilitanti/
- SARZANA F. DI S. IPPOLITO, NICOTRA M., *Diritto della Blockchain, Intelligenza Artificiale e IoT*, Milano, 2018.
- SPOTO G., *Gli utilizzi della Blockchain e dell'Internet of Things nel settore*
- SZABO N., Smart Contracts: Building Blocks for Digital Markets, 1996.

- TETI V.A., Bitcoin: la criptomoneta del Cyberspazio che sfida banche e governi, Rivista Mondo Digitale, n. 46, giugno 2013.
- Whitepaper Ethereum https://ethereum.org/it/whitepaper/
- https://blockchair.com/
- https://blockexplorer.com/
- https://chain.link/whitepaper
- https://it.cointelegraph.com/news/chainlink-releases-new-whitepaper-for-smart-contract-computations
- https://www.agid.gov.it/sites/default/files/repository_files/leggi_decreti_direttive/dl-7-marzo-2005-82_0.pdf
- https://www.blockchain.com/
- https://www.blockchain4innovation.it/eventi-e-convegni/si-avvicina-lappuntamento-con-lindustry-4-0-360-summit/
- https://www.blockcypher.com/
- https://www.datamanager.it/2019/04/soluzioni-hi-tech-per-combattere-le-frodi-nel-settore-alimentare/
- https://www.esma.europa.eu/press-news/esma-news/esma-assesses-usefulness-distributed-ledger-technologies
- https://www.gazzettaufficiale.it/eli/id/2019/02/12/19A00934/sg
- https://www.ilsole24ore.com/art/aon-via-piattaforma-collaborativa-le-applicazioni-blockchain-assicurazioni-ACPUftO?refresh_ce=1
- https://www.insuranceblockchainsandbox.com