POLITECNICO DI TORINO

Corso di Laurea Magistrale in Ingegneria Gestionale

Politecnico
di Torino

Tesi di Laurea Magistrale

La blockchain per la gestione delle malattie rare

Dal paradosso della privacy al trattamento dei dati in modo sicuro

Relatore

Prof. Luigi BUZZACCHI

Candidato

Enrico PASSANITI

A.A. 2020-2021

Sommario

Il presente lavoro di tesi punta a trovare delle evidenze che giustifichino l'utilizzo della blockchain per la gestione delle malattie rare.

Inizialmente, la trattazione analizza il fenomeno del paradosso della privacy, basato su *bias* comportamentali e psicologici che portano il cittadino a non valutare correttamente i rischi derivanti dalla condivisione dei propri dati. La letteratura disponibile, inoltre, suggerisce che la regolamentazione attuale ha aumentato le frizioni di mercato e che i *disclaimer* per il trattamento dei dati vengono classificati, dagli utenti, come noiosi e come perdita di tempo.

Successivamente, viene introdotta la blockchain come tecnologia che possa assicurare i dati degli utenti senza la necessità di confrontarsi con una terza parte. In un primo momento viene riportato il funzionamento delle blockchain pubbliche, tra cui la più nota Bitcoin, descrivendone i punti di forza e di debolezza, tra cui l'elevato consumo energetico. Da quest'ultima evidenza sono nate blockchain alternative, di tipo privato, che si prestano bene all'utilizzo in altri campi, tra cui quello medico. La letteratura attuale suggerisce che, anche, in campo medico è presente un paradosso riguardante l'utilizzo dei dati. Nello specifico, il medico deve scegliere tra garantire l'applicazione delle norme per la tutela dei dati personali e offrire cure di qualità. Questo problema è ancora più grave quando ci si approccia alla gestione delle malattie rare, in quanto il dato, se non trattato a dovere, è facilmente associabile al paziente, data la bassa incidenza delle patologie.

Infine, è stato sottoposto un questionario, composto da cinque sezioni, ai pazienti affetti da malattia di Behçet per indagare le loro percezioni riguardanti il trattamento dei dati personali e la loro disponibilità alla condivisione degli stessi. Emerge la necessità di disporre di un sistema che possa metterli in contatto con gli specialisti e che, soprattutto, possa garantire che le informazioni condivise siano trattate in modo anonimo e secondo gli utilizzi previsti. Si propone, quindi, un modello teorico di doppia blockchain che permetta di perseguire interessi comuni: al medico di garantire sia cure di qualità che la protezione dei dati, puntando anche a perseguire fini di ricerca attraverso l'aggregazione dei dati; al paziente di interagire con una rete di specialisti, attraverso un token dedicato, ed essere sicuro che i dati siano utilizzati per il giusto scopo ed in maniera anonima.

Ringraziamenti

Con la stesura del presente lavoro di tesi concludo il mio percorso di studi al Politecnico. In questi cinque anni ho avuto la possibilità di apprendere e di confrontarmi con i migliori professionisti. Mi ha permesso di crescere come persona e di mettere in risalto le mie conoscenze. È stato un percorso intenso, contrassegnato da difficoltà, stress, ma, sopratutto, da momenti di gioia. Ho conosciuto persone, che sono ormai parte integrante della mia vita, senza le quali non avrei superato alcune difficoltà e che lasceranno in me un ricordo sempre positivo dei miei anni accademici.

Sintetizzare i ringraziamenti in poche righe non è facile. Vorrei ringraziare, in primis, il mio relatore Luigi Buzzacchi: mi ha seguito attentamente nella stesura della tesi, dandomi preziosi consigli per migliorare il lavoro. Lo ringrazio per la disponibilità, la scrupolosità e la presenza che mi ha dedicato. È stato un importante punto di riferimento e mi ha permesso di valorizzare al meglio la tesi.

Ringrazio il Dottor Luca Cimino che mi ha fornito tutto il materiale necessario per trattare l'argomento delle malattie rare nel migliore dei modi. La ringrazio per la professionalità e la disponibilità che ha mostrato nei miei confronti.

Ringrazio mia Mamma e mio Papà per avermi dato la possibilità di affrontare questo percorso, per avermi supportato in ogni momento e per avermi dato fiducia. Sopratutto all'inizio, dopo il trasferimento, la vostra presenza è stata necessaria e mi ha permesso di continuare con serenità l'intero percorso.

Ringrazio i miei nonni che, nonostante la distanza, sono stati sempre presenti. Il vostro contributo è stato determinante e non lo scorderò mai.

Vorrei ringraziare anche i miei amici e colleghi con cui ho condiviso questo percorso. Ho avuto la fortuna di conoscere colleghi, che ora considero amici, che mi hanno dato consigli utili e permesso di vivere con più leggerezza i vari momenti universitari.

Infine, un ringraziamento speciale va a Giulia. Abbiamo affrontato, quasi, tutto il percorso insieme. Abbiamo condiviso ansie, preoccupazioni, dispiaceri, ma, soprattutto, gioie. Sei stata per me un punto fermo nel mio percorso. In ogni momento, in ogni situazione, sapevo che se avessi avuto bisogno tu saresti stata la a spronarmi e darmi aiuto. Sei indubbiamente la persona più importante che

ho conosciuto nella nostra università e senza di te non sarebbe, mai, stato così bello. Grazie per esserci stata e per aver condiviso con me tutto questo. Sei stata indispensabile.

Indice

Elenco delle tabelle

Elenco delle figure

Glossario

AI

Intelligenza artificiale

BFT

Problema dei generali bizantini

BTC

Bitcoin

CA

Cambridge Analytica

dApp

App Decentralizzate

DP

Piattaforme digitali

DSCSA

Drug Supply Chain Security Act

EMA

European Medicines Agency

EMR

Cartella clinica elettronica

ETH

Ether

FB

Facebook

GPT

General purpose technology

HIPAA

Health Insurance Portability and Accountability Act

HPV

Infezione da papilloma virus umano

NSA

National Security Agency

ODA

Orphan Drug Act

POS

Proof of Stake

POW

Proof of Work

PTOY

Patientory

RS

Ricerca e sviluppo

SN

Social network

SSN

Sistema Sanitario Nazionale

UE

Unione Europea

Parte I

Il paradosso della privacy

Introduzione

La protezione dei dati degli utenti rappresenta una tematica importante, che i Regolatori stanno approfondendo per garantire la sicurezza di tutti i cittadini. A partire dal 2002, infatti, sono state emanate diverse direttive volte a limitare l'uso dei dati da parte degli esercenti online e che hanno introdotto l'obbligo di consenso, da parte dell'utente, nell'utilizzo dei propri dati personali. Nonostante ciò, il fenomeno del *paradosso della privacy* non si è ridotto. Al contrario, le direttive hanno creato frizioni di mercato e disincentivi all'acquisto per l'utente. I banner dei *cookies*, infatti, sono valutati come elementi di disturbo e nocivi per completare gli acquisti. Gli utenti tendono, a causa di *bias* psicologici e comportamentali, a non valutare correttamente i rischi derivanti dalla cessione, indiscriminata, dei propri dati ma, valutano unicamente i benefici.

La *blockchain*, tecnologia ampiamente discussa in questa trattazione, è una soluzione che permette di gestire i dati in maniera sicura e che riduce, al minimo, il paradosso della privacy. In ambiti come quello delle *malattie rare*, caratterizzato dalla bassa disponibilità di dati, è necessario attuare tutte le soluzioni possibili che tutelino la privacy dei pazienti, evitando il rischio possibile di *re-identificazione*, e che permettano ai medici di offrire cure di qualità, senza dover scegliere tra privacy e qualità. Attualmente, infatti, la maggior parte dei registri non rispettano i requisiti dettati dalla normativa in termini di protezione dei dati personali. Con la presente trattazione si evidenziano i benefici derivanti dall'implementazione di un sistema blockchain nell'ambito della gestione delle patologie rare.

Il presente lavoro di tesi è organizzato in tre sezioni: la prima sezione illustra la tematica del paradosso della privacy, la seconda si concentra sulla blockchain e la terza focalizza l'attenzione sulle malattie rare e l'implementazione della tecnologia per la gestione di tali patologie. Nella sezione I viene presentato il fenomeno del paradosso della privacy, facendo, inizialmente, riferimento alle asimmetrie informative e alla loro applicazione in era moderna, nel rapporto tra utente e sito web. Tale fenomeno è più evidente quando l'utente deve fare delle scelte di natura economica. In un secondo momento, sono indagate le percezioni che gli utenti hanno della loro privacy ed il rapporto che l'utente ha con i social network prima e dopo eventi di *data breach*. Si indagano, inoltre, le percezioni degli utenti sui

banner dei cookie e sulla loro efficacia nella protezione dei propri dati personali.

Nella sezione II viene approfondita la tecnologia blockchain, facendo, inizialmente, riferimento ai motivi storici che hanno indotto Satoshi Nakamoto, creatore di *Bitcoin*, ad investire sulla sua creazione. Vengono mostrati i punti di forza delle blockchain pubbliche, definite *trustless* perché non hanno bisogno di una terza parte che sorvegli sulla validità delle informazioni scambiate. Inoltre, attraverso un sistema basato sulla competizione dei nodi validatori, assicurano l'impossibilità di penetrazione della rete da parte di utenti malintenzionati. L'elevata potenza computazionale richiesta, però, rappresenta un punto di debolezza che viene approfondito nella trattazione. Da queste evidenze nascono altri tipi di blockchain, definite private, basate su un'unica entità con proprietà di scrittura e lettura che, però, viene controllata dagli utenti per verificare il rispetto delle condizioni d'uso concordate. Le blockchain private permettono di applicare la tecnologia in campi diversi da quello strettamente economico, tra cui quello medico. Per questo motivo, la blockchain è definita una *general purpose technology*, cioè una tecnologia che può essere applicata in svariati campi e che incoraggia l'innovazione. Viene descritta una prima applicazione, creata da IBM, per la gestione della distribuzione dei vaccini con l'utilizzo della blockchain e si discute sull'utilizzo della blockchain come mezzo di contrasto al paradosso della privacy in campo medico.

Nella sezione III vengono approfonditi i problemi comuni nelle malattie rare, incentrando, inizialmente, la trattazione sull'assenza di standard tipica di questi disordini. A livello mondiale, ad esempio, non esiste una definizione univoca di malattia rara e gli investimenti, tra vari Paesi, risultano diversificati. Si descrive il paradosso della privacy rapportato a questi disordini, che comporta per il medico la scelta tra garantire cure di qualità ed attenersi alle norme in materia di trattamento dei dati personali. In questo ambito, caratterizzato da limitata disponibilità di dati, è necessario adottare soluzioni che permettano di determinare analisi statisticamente significative e che superino, concretamente, il paradosso della privacy in campo medico. Si propone uno studio effettuato sui pazienti italiani affetti da malattia di *Behçet*, una malattia rara con incidenza di 2,4 casi ogni milione di abitante. Nello specifico, attraverso la somministrazione di un questionario, si indagano le percezioni dei pazienti riguardo la condivisione dei loro dati e la privacy delle loro informazioni. Dalle risposte si evince la disponibilità degli utenti a condividere i propri dati personali se questi sono utili a migliorare la ricerca e se trattati in modo anonimo. Mostrano fiducia massima verso gli specialisti e sarebbero disposti a cedere i loro dati per essere in contatto, costante, con una rete di medici informati sulla patologia. Sulla base delle risposte ricevute e della letteratura analizzata, si propone un sistema di blockchain per la gestione delle malattie rare che permetta di superare i vincoli attuali:

- Il medico non dovrà più scegliere tra il dovere a fornire cure di qualità e il diritto alla privacy;

- Il paziente potrà interagire con una rete di specialisti ed essere sicuro che i dati siano trattati in maniera anonima ed utilizzati, unicamente, per il corretto scopo. Inoltre, attraverso l'uso di un token inflattivo, associato alla blockchain, si potrebbe creare un sistema di economia chiusa a lungo dibattuta nella letteratura attuale.

Capitolo 1

I fallimenti di mercato

Il fallimento di mercato rappresenta una situazione nella quale l'allocazione delle risorse in un sistema di mercato risulta inefficiente. Ciò accade, alla luce dei risultati dell'economia del benessere, quando le condizioni di funzionamento dei mercati non sono quelle prefigurate da un sistema in concorrenza perfetta, cioè quando il beneficio marginale di consumare un bene è uguale al prezzo del bene stesso.

Nello specifico, si può immaginare un contesto costituito da un unico consumatore che genera, attraverso la massimizzazione della sua funzione di utilità $u(x) + y$, la domanda di mercato $x(p)$ e da un'unica impresa che ha una funzione di costo $c(x)$, del tipo:

$$c' > 0, c'' > 0, c(0) = 0$$

In un mercato perfetto vale la condizione:

$$p = c'(x)$$

Poiché in equilibrio *domanda=offerta*, il livello di output di equilibrio è la soluzione dell'equazione:

$$u'(x) = c'(x)$$

L'allontanamento dalla condizione di concorrenza perfetta è da ricercarsi nelle inefficienze che affliggono i mercati attuali. Nonostante sembri un termine estremamente complesso, si apprezzano fenomeni di fallimento di mercato tutti i giorni. Essi sono dovuti, principalmente, alla presenza di potere di mercato, di asimmetrie informative e di esternalità.

L'illuminazione pubblica, ad esempio, è una chiara manifestazione di *market failure*, associabile al bene pubblico che genera esternalità. Il bene pubblico è un bene non esclusivo, cioè l'uso da parte di un consumatore non preclude che questo possa essere utilizzato anche da qualcun altro. Il problema sorge quando si può usufruire del bene pubblico anche senza pagare.

Alla base di ogni fallimento di mercato si possono individuare delle motivazioni economiche e delle motivazioni sociali. Nello specifico, questa trattazione si concentrerà sulle asimmetrie informative e su come queste condizionino una persona.

1.1 I fallimenti informativi

L'asimmetria informativa è una condizione nella quale uno dei due *player*, supponendo un'interazione singola, ha più informazioni. Per il cliente, se immaginiamo un modello fornitore-acquirente, riuscire a definire la qualità è un processo costoso. Più in generale, il cliente non dispone di tutta l'informazione esistente.

Il fallimento dell'informazione si può verificare in due situazioni:

- I partecipanti al mercato non hanno informazione perfetta;
- L'informazione è di tipo asimmetrico, uno dei partecipanti ha più conoscenza degli altri.

L'asimmetria informativa è, spesso, associata al problema *principale-agente*. Il principale non è in grado di osservare lo sforzo dell'agente e deve, il più delle volte, ricorrere a meccanismi d'incentivo affinché l'agente svolga al meglio le sue mansioni. Chiaramente, in base al contesto in cui operiamo, il principale o l'agente si trovano in una posizione dominante.

Nel settore delle assicurazioni, ad esempio, vi è un chiaro problema di *selezione avversa* e *rischio morale*. La selezione avversa si verifica in quanto il principale ha meno informazioni e non può definire, correttamente, ex-ante l'impegno dell'agente. Il rischio morale, invece, si verifica ex-post. Il principale non può sapere in che misura si è sforzato l'agente. Lo sforzo, in ogni caso, non è calcolabile ma è osservabile solo il risultato. Si ricorre, quindi, a *contratti incentivanti* in modo da massimizzare entrambe le funzioni di utilità.

In era moderna, il problema della mancanza d'informazioni può ricercarsi nel rapporto tra utente e sito web. Ogni volta che un utente naviga in un sito web accetta le politiche del sito stesso, nonostante sia diffusa l'idea che Google offra i suoi servizi gratuitamente. In realtà, attraverso l'accettazione, a volte anche silenziosa, delle sue *policies* si da il consenso al trattamento dei dati. Tale problema si origina perché si tende a pensare che gratuito sia equivalente a *mancato esborso monetario*: qualcosa può essere costoso ma non essere pagato tramite denaro.

I dati degli utenti, derivati dalla navigazione sul web, rappresentano al meglio la discrepanza appena descritta. L'utente presta attenzione alla propria privacy, anche quando il termine "prestare attenzione" è poco definito.

Bisognerebbe, infatti, classificare meglio la sfera comportamentale di un utente che naviga sul web.

L'autore nei primi capitoli proverà a fornire delle evidenze su questi aspetti, ponendo l'accento sui *bias comportamentali* in tema di protezione dei dati personali.

1.2 L'importanza della privacy per le persone

La parola *privacy* "fa riferimento all'insieme di informazioni personali che non vogliamo diventino di dominio pubblico senza il nostro consenso" [1].

In prima analisi, in base alla definizione, la privacy sembra che rappresenti una tematica importante per tutti gli individui. Il contrario, rifacendosi sempre alla definizione fornita sopra, sembrerebbe poco auspicabile.

L'individuo che naviga su internet tende a proteggere le proprie informazioni personali, definendo la privacy come una priorità. In questo paragrafo verrà introdotto il fenomeno del paradosso della privacy, mostrando i bias comuni nel comportamento umano.

Le persone agiscono diversamente da quanto comunicano. Sono capaci di vendere, per poco, le loro informazioni. Si può pensare, ad esempio, alle migliaia di *stories* che sono pubblicate quotidianamente su Instagram. Le persone hanno l'esigenza di mostrare la loro vita, andando contro la loro idea di *rispetto dei dati personali*. C'è, sostanzialmente, una profonda differenza tra quello che pensano e quello che compiono. Fenomeno che negli Stati Uniti chiamano *privacy paradox of attitudes and behaviour*.

Nonostante il pensiero critico di ogni consumatore sulla sua protezione, ricerche di mercato stimano che gli utenti valutano la loro cronologia poco più di 7 euro, l'equivalente del prezzo di un panino [2]. Da queste evidenze , che mostrano una differenza tra l'atteggiamento e il comportamento, deriva il detto *information privacy paradox*. Il paradosso della privacy nelle informazioni.

Alla base del paradosso vi è la difficoltà delle persone nel valutare, correttamente, le decisioni correlate alla privacy. L'informazione incompleta e i bias psicologici e razionali sono alla base del processo decisionale. Ad esempio, il problema principale che affligge l'utente nella sua decisione di comprare online riguarda il bias dell'immediata gratificazione. Non si valuta correttamente l'esperienza d'acquisto, in quanto si ha la tendenza a pensare che i benefici attuali siano maggiori dei futuri rischi, come avviene, ad esempio, con i data breaches [3]. Gli studi rivelano, inoltre, che la disponibilità a fornire informazioni dipende, anche, dall'età di chi naviga su internet.

Nel 2005 è stato condotto un interessante esperimento [4] per capire il valore che le persone danno ai propri dati. Nello specifico, ai profili intervistati veniva chiesto quale fosse il prezzo minimo che avrebbero accettato per comunicare il loro peso e la loro età. Lo studio ha rivelato che il prezzo cresceva al crescere dell'imbarazzo (ad esempio l'utente intervistato in sovrappeso chiedeva un prezzo medio superiore

rispetto all'utente in forma) e diminuiva al diminuire dell'età. Tendenzialmente, quindi, l'utente più giovane è più predisposto a condividere i suoi dati, ma è anche meno informato sui rischi derivanti dalla condivisione degli stessi.

Di seguito è riportato un esempio che si adatta bene alla presente trattazione.

Nel 2012 è stato condotto un esperimento [5] attraverso il quale si chiedeva ai consumatori di comprare un DVD da due negozi, in competizione tra loro, che non mostravano differenze significative che potessero far insorgere nel cliente una preferenza stretta. Quindi, hanno escluso in partenza effetti sistemici derivanti dall'importanza del brand e similari. Possono essere definiti, ai fini della ricerca, identici. La differenza, sostanziale, tra i due store erano le informazioni richieste al momento dell'acquisto. Il primo negozio richiedeva i guadagni e la data di compleanno, invece, il secondo domandava il colore preferito e la data di compleanno. Sicuramente le richieste del primo negozio minavano di più la privacy del cliente, in quanto la richiesta dei guadagni realizzati nell'arco dell'anno è un'informazione più significativa del colore preferito.

In una prima fase, quando il prezzo dei DVD era lo stesso per entrambi i negozi, i consumatori compravano da entrambi gli store. Si può dire che la distribuzione fosse equamente divisa. Al diminuire del prezzo dei DVD venduti dal primo negozio, di solamente 1 €, quasi tutti i consumatori decisero di comprare dallo store più conveniente. Alla fine della fase di acquisto è stato richiesto a tutti i partecipanti di compilare un questionario riguardo le loro considerazioni sulla privacy: il 95 % ha dichiarato di essere interessato alla protezione dei propri dati personali. È evidente che c'è un bias comportamentale. I consumatori hanno agito in maniera opposta a quello che hanno dichiarato, preferendo risparmiare 1 euro piuttosto che mantenere certi dati sicuri.

Gli individui decidono di condividere le proprie informazioni quando i *profitti potenziali* superano le *perdite potenziali* [6]. In generale, si evince che la privacy per gli utenti sia importante, ma la componente economica è determinante nella scelta finale. In presenza di valutazioni economiche, l'atteggiamento non corrisponde con il comportamento dell'utente finale. Di seguito, la Tabella 1.1 riporta alcuni studi effettuati che supportano l'idea di un esistente *privacy paradox* [7] .

Studio	Contesto	Partecipanti
Acquisti et al. (2005)	e-Commerce	Studenti
Carrascal et al. (2013)	Intrattenimento	Utenti web
Egelman et al. (2012)	App per smartphone	Utenti smarphone
Norberg et al. (2007)	Servizi finanziari	Studenti
Reynolds et al. (2011)	Social Networks	Utenti Facebook
Zafeiropoulou et al. (2013)	Dati di localizzazione	Utenti internet

Tabella 1.1: Studi che provano l'ipotesi del paradosso della privacy

Capitolo 2

Il prezzo nascosto dei Social Network

I social networks (SNs) rappresentano, sicuramente, una delle innovazioni del secolo. Attraverso l'utilizzo di un computer o uno smartphone si riesce a comunicare con persone da tutte le parti del mondo. È proprio questa estrema semplicità che ha permesso ai SNs di *esplodere* e diventare, ad oggi, insostituibili nella vita di tutti i giorni.

In questo capitolo verranno presentati i social network, spiegando perché sono gratuiti ed indagando il problema della protezione dei dati personali. Nello specifico, il paradosso della privacy sarà mostrato descrivendo lo scandalo che ha coinvolto Facebook e Cambridge Analytica.

Oltre alla semplicità, bisogna considerare che i SNs sono gratuiti, dal punto di vista monetario. L'utente che si iscrive ottiene gratuitamente l'accesso alla piattaforma e usufruisce, sempre gratuitamente, delle varie features (app, assistenza via e-mail e similari). Seppur gratuiti e utili, molti utenti sottovalutano i rischi derivanti dall'uso dei SNs. Generalmente i motivi per cui non si valutano correttamente i rischi derivanti dall'uso dei social sono riferibili a tre paradossi [8]:

- Gli utenti non si prendono cura della propria privacy;
- Gli utenti non conoscono le implicazioni delle loro azioni sulla loro privacy;
- Gli utenti hanno a cuore la propria privacy e conoscono abbastanza ma "semplicemente" i controlli non sono applicabili.

Da un punto di vista strettamente economico, il vero vantaggio di queste nuove piattaforme digitali (DP) risiede nell'uso innovativo dei dati.

Le DP rendono, di fatto, nullo il prezzo pagato dall'utente in modo da appropriarsi di quanti più consumatori possibili (Figura 2.1). L'enorme mole di utenza,

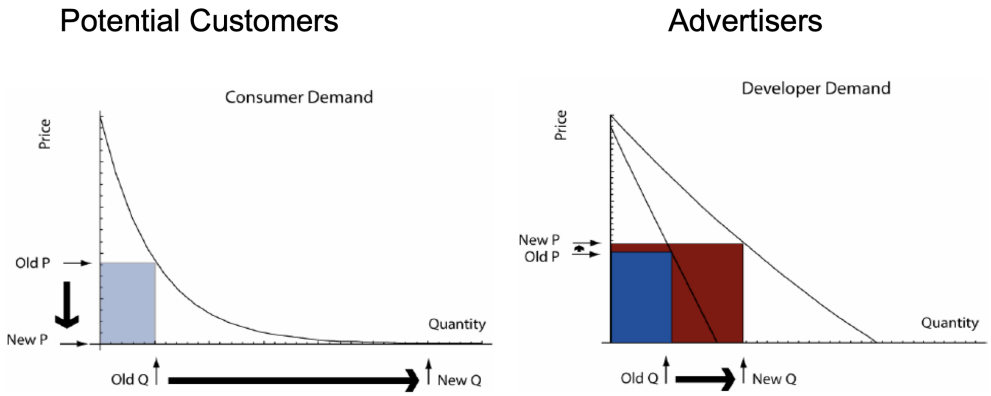

Figura 2.1: La targhetizzazione degli utenti tramite incentivi di prezzo.

e quindi di dati, spinge le aziende a pagare a caro prezzo gli spazi pubblicitari all'interno dei SNs. Questo, sicuramente, è dovuto alla corretta targhetizzazione dei dati da parte del proprietario della piattaforma che permette all'inserzionista di far fluire verso sé soltanto l'utenza interessata.

Bisogna interrogarsi su quanto, a favore di un prezzo totalmente nullo, gli utenti rinuncino alla segretezza dei propri dati.

2.1 Il caso Facebook

Il paradosso della privacy, denominato in tal modo da Barnes e Norberg nel 2006, è evidente nei social network, e in maggior misura su Facebook (FB). Ad oggi, FB rappresenta il più grande Social network operante a livello mondiale con 2,60 miliardi di utenti attivi al mese [9].

Facebook è un SN fondato nel 2004 con l'obiettivo di connettere le persone e dare la possibilità di creare delle comunità digitali. Quando ci si registra su FB, o più in generale su ogni SN, sono richiesti, prima dell'approvazione, molti dati personali e sensibili quali:

- Nome e cognome;
- Data di nascita;
- Orientamento politico;
- Preferenze sessuali.

Queste informazioni servono all'utente per potersi connettere, ed essere rilevato, con altri utenti e creare dei gruppi di interazione. Per come è strutturato, FB *incoraggia* l'utente a condividere i suoi dati promettendogli dei grossi vantaggi [10].

Fino a pochi anni fa si parlava unicamente di beneficio nell'uso di FB, come mezzo altamente innovativo che riduceva, e minimizzava, le difficili distanze. Oggi, invece, sempre più persone si interrogano e si domandano quando si può parlare di beneficio e quando, invece, di rischio. La divisione non è netta e il filo sottilissimo.

Il più delle volte quando ci si iscrive ad un SN non si leggono le politiche di gestione dei dati, ritrovandosi, solo nel futuro, ad interrogarsi su come tali dati siano gestiti e quali siano i rischi concreti della loro dispersione.

È notizia di questi giorni che FB sia stato violato, cioè che i suoi server siano stati compromessi e, quindi, i dati siano stati divulgati illecitamente. Non per volere di FB, sia chiaro [11].

Nella situazione più ottimistica questi sono sfruttati per "ricattare" FB stesso ed ottenere un ingente capitale. Nella situazione più probabile, invece come già successo a molti utenti, i dati sono usati per incentivare il cosiddetto "effetto pesca" (quello che gli americani chiamano *phishing*). In tal modo, i malintenzionati, avendo a disposizione moltissimi dati dell'utente, fingono di essere delle persone fidate o enti finanziari in modo da *pescare* informazioni sensibili come, ad esempio, i codici bancari.

In seguito all'aumento dei numerosi attacchi informatici, sempre più persone si interrogano su come poter proteggere i propri dati e se, magari, fosse stato meglio informarsi prima di accettare delle policies *al buio*. Alcuni studi evidenziano che i ragazzi universitari siano soliti cancellare dalla propria bacheca i commenti degli amici, che ritengono possano influenzare negativamente la loro immagine, o eliminare foto ritenute estremamente private [12]. Altri, invece, pongono l'attenzione su cosa fanno concretamente gli utenti dopo aver subito una violazione del loro profilo FB. La prima azione che intraprendono è rendere il profilo *friends-only*, cioè aperto unicamente agli amici.

2.1.1 Lo scandalo Cambridge Analytica

Cambridge Analytica (CA) è stata una società di consulenza, fondata nel 2013 in Gran Bretagna con l'intento di sfruttare al massimo i dati forniti dagli utenti nei SNs. Utilizzavano qualunque tipo di dato, in modo da creare un profilo psicometrico di ogni utente. Il profilo era tanto più preciso quante più informazioni erano disponibili nel SN. Un solo "mi piace" in più, che potrebbe sembrare una metrica poco significativa, permetteva di caratterizzare, e targhettizzare, meglio l'utilizzatore di FB. Dall'analisi dei dati, CA riusciva a fornire pubblicità mirate, soprattutto di stampo politico.

Il modello CA, a differenza dei competitors, era basato su un sistema di *microtargeting comportamentale*: CA non faceva leva solo sui gusti degli utenti ma anche sulle loro emozioni. Questo gli permetteva di creare pubblicità altamente personalizzate.

Ritornando al concetto del "like" di cui si parlava in precedenza, Michal Kosinski, un ricercatore e sviluppatore dell'algoritmo di CA, sostiene che con, soli, 300 mi piace loro fossero in grado di sapere molte più informazioni sul soggetto rispetto al proprio partner.

Christopher Wylie ha definito CA come: "lo strumento psicologico di Steve Bannon per fottere il cervello della gente". Per inciso, Wylie è l'informatico ventenne che ha fornito informazioni necessarie per rivelare al mondo il cosiddetto "scandalo Cambridge Analytica-Facebook".

È bene precisare che un lavoro che CA svolgeva egregiamente era quello di recepire dati, anonimi, da più piattaforme, ad esempio i SNs, compattarli e risalire all'identità degli utenti. Questo non è illegale. È stato illecito il modo in cui sia arrivata ai dati e il modo in cui, CA, li abbia utilizzati.

Nel 2014 Aleksandr Kogan aveva realizzato un'applicazione, "this is your digital life" (letteralmente questa è la tua vita digitale), che prometteva la valutazione della propria personalità attraverso un sistema di quiz. Per utilizzarla bastava fare il login, cioè accedere, attraverso FB. In tal modo l'applicazione aveva la possibilità di salvare dati personali dell'utilizzatore, quali e-mail, data di nascita, sesso oltre al nome e al cognome. Si iscrissero all'applicazione circa 300 mila utenti, quindi milioni di dati personali raccolti [13].

Fino a poco tempo fa FB consentiva alle app di terze parti di raccogliere informazioni, anche, sugli amici dell'utente (la rete di contatti che si era costruito sul social). In totale, il New York Times stima che siano stati raccolti dati su 50 milioni di profili FB.

Il problema, grave, che ha coinvolto FB riguarda l'uso dei dati da parte di CA (condivisi da Kogan), in quanto il regolamento del social network vieta alle app, che raccolgono i dati degli utenti, di condividerli con società terze, pena la sospensione dell'account. Facebook, da quanto ha rivelato Wylie, era a conoscenza del problema da 2 anni prima dell'inizio delle indagini ma non si è mossa per difendere la privacy degli utenti.

Tali dati, insieme a numerosi account fasulli e bot, furono utilizzati, in prevalenza, per condizionare le elezioni americane del 2016, pro-Trump, e diffondere informazioni contro Hilary Clinton. Il tutto condizionato ai "risultati live" del momento [14].

Capitolo 3

Dai Social Network all'attuale fallimento nel data tracing

In questo capitolo verrà, inizialmente, analizzata la percezione del rischio che hanno gli utilizzatori dei social networks, facendo un confronto con l'app Immuni. Successivamente, verrà analizzata l'efficacia dei disclaimer dei cookie e la percezione che hanno gli utenti.

Nei primi sei mesi del 2019 ci sono stati 3800 *data breaches* (letteralmente furto massivo di dati) che hanno coinvolto i dati di circa 4 miliardi di persone globalmente [15]. È evidente che, ormai, non si tratta più di fenomeni isolati ma ricorrenti che mettono a serio rischio la protezione delle informazioni personali degli utenti sul web. Lo scandalo CA-FB, che ha coinvolto almeno 87 milioni di persone, ha creato un precedente e ha posto le basi per una maggiore attenzione alla salvaguardia della privacy, rivalutando il potere di mercato delle piattaforme digitali.

Le prime reazioni sono state degli utenti che hanno diffuso sui social gli hastags #DeleteFacebook e #Faceblock [16] come mezzo di protesta. Tali reazioni, però, sono risultate inefficaci perché le persone sono riluttanti nell'abbandonare i SNs in quanto è difficile rinunciare agli enormi vantaggi derivanti dal loro uso, come ad esempio la possibilità di poter interagire facilmente con gli amici o l'avviso sui compleanni dell'intera rete [17]. Oltre questo, numerosi studiosi si sono interrogati sulla necessità di regolare e definire degli standard, minimi, di sicurezza per l'intelligenza artificiale (AI) [18].

Uno dei grossi problemi, non risolti, dei SNs è il cosiddetto *networked privacy*, cioè la possibilità degli amici della rete di poter condividere un post, una foto o qualunque altro tipo di informazione personale, di un terzo, con tutta la sua rete. In tal modo si eludono tutte le protezioni che il terzo potrebbe decidere di

attuare. Il *tag* in una foto è un chiaro esempio del fenomeno: esso è visibile a tutti nonostante il profilo abbia poche interazioni [19]. L'esempio, appena presentato, descrive perfettamente la modalità con la quale CA è riuscita a reperire così tante informazioni.

Uno studio [20], condotto subito dopo lo scandalo CA-FB, ha evidenziato la reale percezione del rischio degli utilizzatori di internet. È importante notare che, nonostante lo studio sia stato effettuato in seguito allo scandalo, questo non sia stato minimamente menzionato nelle pagine dell'intervista per osservare se gli utenti lo nominassero e in che misura. L'indagine è stata condotta intervistando 30 persone appartenenti alla vita universitaria o con una buona reputazione accademica, in modo da isolare il bias della mancata istruzione.

La ricerca ha evidenziato che molti utenti hanno una concezione contraddittoria della loro privacy online e nonostante lo scandalo pensavano che tutto questo non sarebbe potuto capitare a loro. Poiché avevano impostato il profilo come "privato" pensavano di essere immuni al rischio. Al tempo stesso, però, non capivano come mai dopo aver visitato eBay ricevessero pubblicità mirate su FB. Lo trovavano *creepy*, cioè raccapricciante, ma non pericoloso.

3.1 Il caso Immuni

Immuni è l'app scelta dal Governo italiano, progettata da Bending Spoons, per tenere traccia di tutti i contagi da Covid-19 (Figura 3.1).

Poiché non si tratta di un dispositivo medico, che obbligherebbe il Ministero della salute (MS) ad una procedura di certicazione [21], il download e relativo utilizzo dell'app è facoltativo. Nonostante l'importante obiettivo che si prefigge, l'app non ha riscosso successo ottenendo un numero di download totali di, soli, 4 milioni e mezzo al 20 luglio 2020. Quindi, solo, il 12% della popolazione ha scaricato l'app dopo più di un mese dal suo rilascio ufficiale. Alla base di questo "fallimento" c'è la diffidenza delle persone nel fornire i propri dati personali.

Da un punto di vista giuridico, analizzando i termini e condizioni, l'app è basata su un modello di dati pseudonimizzati, cioè uno spazio intermedio tra gli infiniti consensi che si accettano *al buio* delle app commerciali e i dati anonimi. Dati, importante ricordarlo, gestiti dal MS ed utilizzati, unicamente, per prevenire la diffusione del contagio.

In ogni caso, la cancellazione degli indirizzi IP è immediata e l'archiviazione dei dati è, al massimo, fissata al 31 dicembre 2021 (data definita dal decreto-legge di ottobre). Gli esperti hanno definito tale app *low risks* [22] e, in confronto ai competitors (termine che non è correttamente etico riferendosi ad una pandemia), una con gli standard di sicurezza più alti. Giusto per fare un confronto, l'app

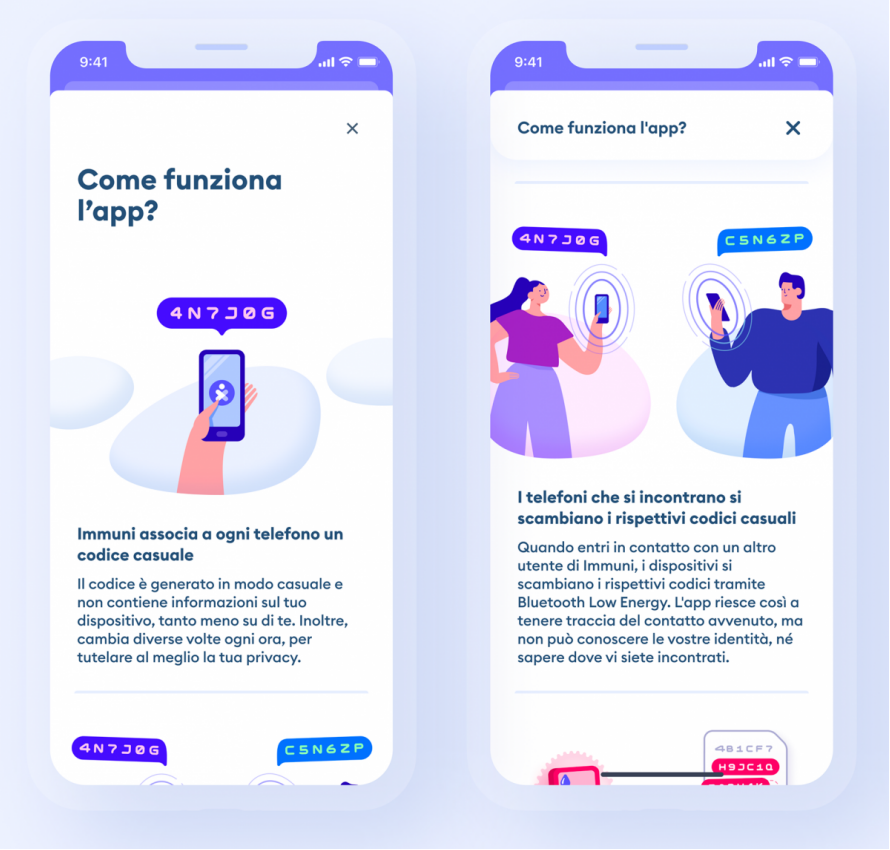

Figura 3.1: Funzionamento dell'app Immuni.

inglese *NHS- Covid-19* è classificata con un livello di rischio moderato ma ha, al 7 ottobre 2020, 16,5 milioni di download [23].

Gli utenti, in Italia, hanno protestato molto per l'attivazione di questa app in quanto definita troppo invasiva, creando moltissimi post di lamentele sui social. Gli stessi SNs di cui non si sa, letteralmente, niente di come utilizzino le informazioni degli utenti.

3.2 L'uso dei cookies nella navigazione online

I cookies sono frammenti di dati degli utenti che sono stati, originariamente, introdotti per fornire una migliore esperienza di navigazione nei siti utilizzati. Successivamente, invece, l'uso del cookie si è trasformato in un collettore di informazioni volto a personalizzare le pubblicità mostrate a ciascun sottogruppo di utenti. Proprio per questo, l'Unione Europea (UE), con la direttiva del 2009 [24], prima, e con il GDPR del 2018 [25], ha difatti regolato tale mercato visti i

potenziali rischi per la privacy degli utenti visitatori. Il cambiamento riguarda tutti gli utenti europei e comporta il consenso esplicito nell'accettazione dei cookies.

L'UE riteneva che, in tal modo, l'utente sarebbe stato meno esposto ai rischi del web e, allo stesso tempo, avrebbe impiegato qualche secondo in più per salvaguardare i suoi dati, visto l'obbligo per il sito di fornire informazioni riguardo l'uso delle informazioni raccolte.

In questa trattazione non sarà spiegata la differenza tra i vari tipi di cookies esistenti, ma le considerazioni saranno indirizzate sui cookies di terze parti, che sono i più problematici, ma anche i più interessanti, dal punto di vista della privacy. Si limiterà a fornire, tramite la Figura 3.2, le differenti tipologie.

Figura 3.2: Le diverse tipologie di cookies.

Un'importante ricerca [26] sottoposta a 150 utenti, con distribuzione dell'età casuale, evidenzia che le persone ritengono il *disclaimer del cookie* come una perdita di tempo e, quindi, accettano le informative senza capire, realmente, il contenuto.

Più nello specifico, si evidenzia che le persone classifichino i disclaimer come elementi di disturbo nella loro navigazione, in quanto trovano il messaggio *annoying*, cioè fastidioso. Al tempo stesso, lo studio rivela che gli utenti tengono molto alla loro privacy e trovano straziante non capire a cosa prestano il consenso.

La maggior parte di loro, però ugualmente, ignora il problema, reputandolo una perdita di tempo, oppure accetta senza preoccuparsi delle conseguenze.

È evidente, però, che, come evidenziato più volte in questa trattazione, ci sia un *bias comportamentale* intrinseco nel loro modo di pensare: dire qualcosa per poi effettuare l'opposto.

Si potrebbe pensare che il fenomeno riguardi solo i *cookie minori*, cioè quei cookie necessari per il corretto funzionamento del sito. In realtà, la distribuzione delle risposte, per ogni categoria di cookie, evidenzia che è un problema generale e che, in linea di massima, il problema dei cookies sia uniforme (Figura 3.3).

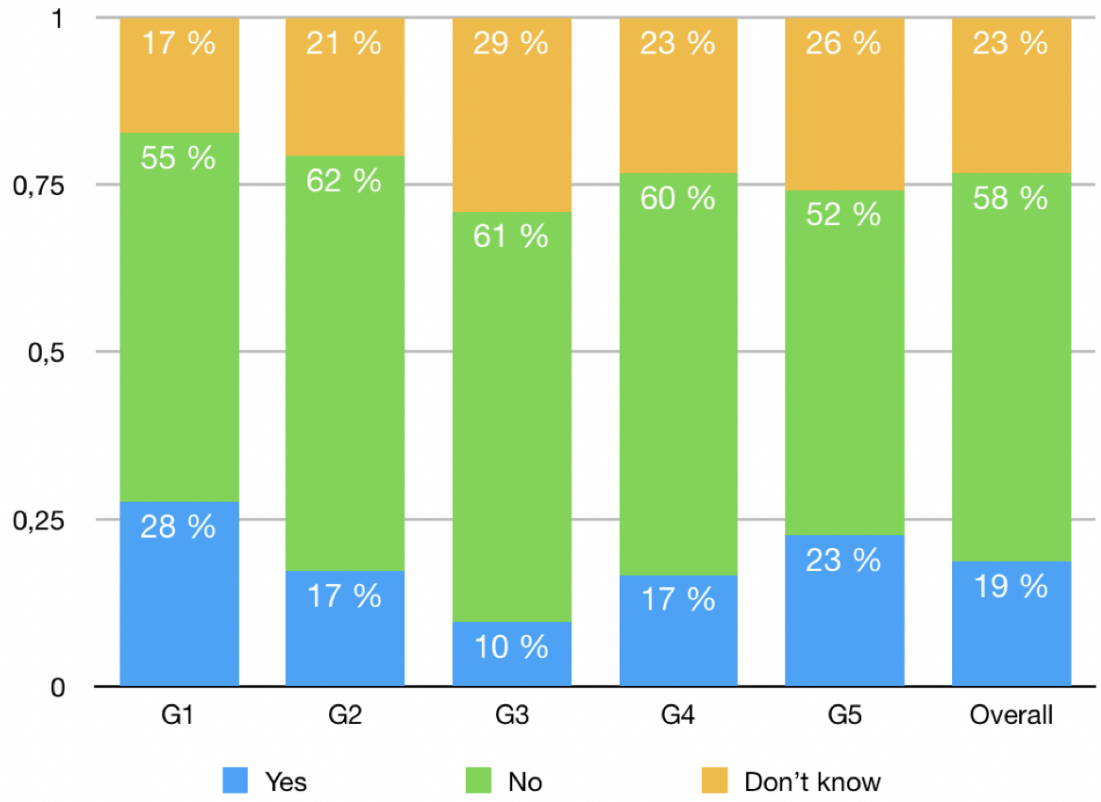

Figura 3.3: Utenti che abbandonano il sito, in seguito al *disclaimer*, divisi per tipologia di cookie.

3.3 Implicazioni future

La letteratura analizzata mette in evidenza il paradosso della privacy nella quotidianità. Inizialmente, la trattazione si è focalizzata su dei casi studio volti a definire la dimensione del fenomeno. Le ricerche effettuate, però, mostrano delle lacune che potrebbero condizionare la validità, generale, del paradosso.

Analizzando, infatti, il caso studio proposto da Carrascal et al. [2], riguardante la vendita dei propri dati in cambio di un panino, si evince che in nessun caso è menzionato il reddito dell'utente. La distribuzione del reddito è, invece per l'autore, una metrica fondamentale da considerare in un lavoro del genere e potrebbe essere estremamente significativa nel valutare il comportamento delle persone.

Idealmente, un consumatore potrebbe tenere fortemente ai suoi dati, ma, al tempo stesso, aver bisogno di sfamarsi. In tal modo, la cifra di 7 euro, equivalente al costo di un panino, potrebbe essere associata ad una bassa valutazione monetaria ma ad un'altissima *valutazione momentanea*. Proprio per tale motivo, le considerazioni seguenti sono orientate su servizi che, di base, sono gratutiti per tutti allo stesso modo. Le uniche differenze, in termini di utilizzatori, si fermeranno all'età dell'utente fruitore.

I social networks sono piattaforme facilmente accessibili che minimizzano il prezzo pagato dagli utenti (lo annullano del tutto nella maggior parte dei casi) in cambio dell'accettazione delle loro policies di utilizzo. Tali regole, che come evidenziato vengono accettate senza comprenderne le potenziali conseguenze, riguardano, tra le altre, la cessione dei dati personali. La preoccupazione, per la propria privacy, nel caso dei social networks nasce soltanto dopo eventi di data breachs. In questi casi, le persone tendono ad impostare il proprio profilo friends-only, in modo da renderlo accessibile unicamente agli amici. Tale misura, però, non è sufficiente e il caso Cambridge Analytica lo conferma. La maggior parte degli utenti non ricorda neanche quali informazioni abbia reso pubbliche.

Lo scandalo CA dimostra quanta attenzione si dovrebbe fare quando si accettano, al buio, le clausole dei SNs e pone dei dubbi, importanti, circa la *gratuità* di tali servizi.

Per ridurre il problema, gli Stati stanno cercando di creare degli standard per regolare il fenomeno. Stanno intervenendo in tema di intelligenza artificiale. Nonostante siano misure fondamentali, tali risultano inefficaci in quanto gli utenti, il più delle volte, non sono consapevoli dei rischi riguardanti la diffusione, incontrollata, dei loro dati e, quindi, non prestano troppa attenzione ai data breaches che si verificano.

L'applicazione del Cookie Law e del GDPR, regolamento generale per la protezione dei dati, non ha dato i risultati sperati. È stata, invece, evidenziata una tendenza dei consumatori a ridurre le intenzioni d'acquisto. Godlfarb & Tucker, infatti, hanno evidenziato che la regolamentazione limita l'efficienza del mercato ed

aumenta le frizioni poiché crea delle dispersioni. Lo studio [27], condotto attraverso l'applicazione di un modello di diff-in-diff, mette a confronto il comportamento degli utenti prima e dopo la sottoposizione allo shock di tipo esogeno (entrata in vigore del Cookie Law) e mette in risalto l'inefficienza dell'advertising in seguito all'entrata in vigore di direttive per la tutela della privacy (Figura 3.4).

Si riporta, di seguito, il modello econometrico.

$$Intent_{ijct} = \alpha Exposure_{ij} + \beta Exposure_{ij} \times Law_{ct} + \theta X_i + \gamma_{jct} + \epsilon_{ijct}$$

dove:

- *Intent* identifica quando la persona i era molto vicina all'acquisto;
- *Exposure* identifica le persone esposte all'ads nella ricerca j;
- *Law* è una dummy che identifica il periodo successivo all'implementazione della legge;
- X è un vettore dei dati demografici;
- γ colleziona ricerche, Paese ed effetti fissi di tempo.

	EU data only				All data
	(1) Ad exposure only	(2) No controls	(3) Demographic controls	(4) Campaign fixed effects	(5) Three-way difference
Exposed × AfterEULaw × EU		−0.0275***	−0.0254***	−0.0167**	−0.0171**
		(0.00474)	(0.00472)	(0.00694)	(0.00714)
Exposed	0.00746***	0.0300***	0.0292***	0.0256***	0.0263***
	(0.00187)	(0.00426)	(0.00424)	(0.00641)	(0.00635)
AfterEULaw × EU		−0.00221	0.0129***		
		(0.00340)	(0.00341)		
Female			0.0365***	0.0198***	0.0154***
			(0.00190)	(0.00381)	(0.00149)
Std. Internet hours			0.00274**	0.00936***	0.0122***
			(0.00116)	(0.00125)	(0.000341)
Std. income			−0.0169***	−0.0118***	−0.00288***
			(0.00143)	(0.00224)	(0.000480)
Std. age			−0.0378***	−0.0319***	−0.0185***
			(0.00101)	(0.00390)	(0.000683)
Constant	0.375***	0.377***	0.334***		
	(0.00136)	(0.00304)	(0.00320)		
Exposed × AfterEULaw					−0.00109
					(0.00194)
Exposed × NotEU					−0.00979
					(0.00658)
Campaign fixed effects	No	No	No	Yes	Yes
Observations	271,207	271,207	271,207	271,207	3,329,632
R-squared	0.379	0.379	0.385	0.160	0.172

Notes. Columns (1)–(4) use data from EU only. Column (5) uses data from the EU and rest of the world. Dependent variable is purchase intent. Robust standard errors are clustered at the website-campaign level. *AfterEULaw × EU* is collinear with the campaign fixed effects and is therefore excluded from column (4). *BeforeEULaw × NotEU, NotEU, and BeforeEULaw* are collinear with the campaign fixed effects and are therefore excluded from column (5).
*$p < 0.10$; **$p < 0.05$; ***$p < 0.01$.

Figura 3.4: Risultati del paper sull'applicazione di direttive per la regolazione della privacy [27].

Questa ricerca può essere intesa come la reale manifestazione del *paradosso della privacy*. Nonostante le persone considerino qualcosa come dannosa per la loro

privacy, non usano il loro tempo per informarsi e trovare delle soluzioni, che possano, in qualche modo, migliorare la situazione ma rimangono della loro idea, accettando delle policies al quanto discutibili. I SNs hanno reso il tutto più difficile. Gli utenti, ormai, scrollano continuamente il sito web e non prestano attenzione ai dettagli riguardanti le politiche sulla privacy. In tal senso, il cookie viene etichettato come una perdita di tempo e come *distruttivo* perché non permette una consultazione veloce dei dati.

Il focus di questo lavoro è incentrato sulla sanità. È preoccupante sapere che le considerazioni fatte fin'ora sono valide, anche, in campo sanitario. Il caso Immuni amplifica il problema. Immuni, come evidenziato in precedenza, è l'app scelta dal Ministero della Salute(MS) per tenere traccia dei contagi da Covid-19. Gli abitanti, però, hanno preferito non registrarsi per paura di come fossero usate le loro informazioni personali. Nonostante le ricerche stimino che sia una delle app più sicure, in termini di *contact tracing*, si è diffusa la tendenza a rifiutare il download per diffidenza nei confronti del MS. Lo stesso MS che, per definizione, protegge la privacy e gli interessi di tutti i cittadini.

Sicuramente, almeno per quanto riguarda il caso Immuni, l'importanza dei dei propri dati personali, da difendere a tutti i costi, è soltanto uno specchietto per le allodole. Dietro il rischio di ricevere una notifica di esposizione al Covid-19, con tutte le procedure di isolamento che ne conseguono, le persone preferiscono demonizzare l'impossibile e spostare l'attenzione su qualcosa a cui, realmente, non tengono.

Bisognerebbe indagare sul perché un SN, gestito da *big tech*, non spaventi gli utilizzatori e, invece, la condivisione delle informazioni a livello medico, per favorire il bene comune, possa scaturire un clamore mediatico senza precedenti. Capire la psiche delle persone è difficile ma poter indagare su questo paradosso, invece, è possibile a tutti. Si rischia, in tal modo, di contrastare inspiegabilmente il benessere collettivo ed assistere a fenomeni di *in-solidarietà digitale*.

È necessario, quindi, educare gli individui e promuovere azioni volte al bene comune. Bisogna introdurre delle dinamiche sociali che facciano capire i veri rischi derivanti dalla cessione, incondizionata, dei dati. Il caso Immuni deve essere un punto di partenza, che non dovrebbe più ripetersi, per implementare delle azioni che incentivino la protezione dei dati degli utenti utilizzatori. È poco confortevole sapere che un "giochino di moda" abbia più utilizzatori di un'applicazione in ambito medico e che, quindi, le persone siano maggiormente disponibili a cedere i loro dati per fini commerciali.

L'applicazione delle nuove tecnologie, blockchain su tutte, potrebbe permettere di stimolare l'accesso a tali tipi di servizi.

Parte II

La Blockchain e la tecnologia come abilitante

Capitolo 4

Dalla crisi finanziaria alla tecnologia trustless

La blockchain, letteralmente *catena di blocchi*, è una struttura decentralizzata, condivisa e crittograficamente immutabile.

In questo capitolo verrà mostrato come è nata la blockchain, spiegando le motivazioni che hanno indotto Satoshi Nakamoto ad investire su di essa. Inizialmente, verrà fatta una panoramica su questa tecnologia, soffermando in seguito l'attenzione sui punti di forza e debolezza e su come, questi ultimi, possano essere migliorati. Verrà presentata la blockchain come tecnologia che permette lo scambio di informazioni in maniera sicura, senza ricorrere ad una terza parte. Saranno indagati, anche, i punti di debolezza delle prime forme di blockchain e come questi sono stati risolti per garantire le applicazioni in diversi campi, tra cui quello medico.

Tale tecnologia nella sua forma semplificata, per quanto sofisticata ed utile, fu adoperata già a partire dal 1400 d.C. nell'isola di YAP. Sull'isola i pagamenti erano effettuati per mezzo della pietra Rai, che assolveva perfettamente al ruolo della moneta:

- facilitava gli scambi;
- poteva essere usata come unità di conto;
- poteva funzionare come riserva di valore.

Gli abitanti dell'isola sperimentarono un registro pubblico per gestire al meglio le pietre ed evitare che, queste, venissero custodite in maniera illecita. Uno dei grossi problemi, tangibili, era che le pietre erano rubate durante la notte e i proprietari ne perdevano il possesso. Il registro fu la soluzione, in quanto associava alla pietra, oltre al valore monetario, un valore informativo. Infatti, le transazioni giornaliere erano riportate sul registro e ogni abitante ne deteneva una copia.

In tal modo, anche se una pietra fosse stata rubata non sarebbe potuta essere spesa perché tutti si sarebbero accorti dell'incongruenza tra registro e transazione.

Nacque, così, il primo sistema decentralizzato per sopperire al problema della fiducia [28]. La blockchain attuale, infatti, rappresenta solo un'evoluzione del primo sistema, creato più di 600 anni fa, con l'applicazione di tecnologie al tempo sconosciute.

La necessità di avere un sistema decentralizzato, non controllato da un'entità terza è nata in seguito alla *grande recessione* del 2008. A partire dal 2006, le banche americane concessero prestiti molto rischiosi, senza curarsi della possibile insolvenza. La *bolla speculativa* portò, tra le varie conseguenze, ad un'esplosione dei prezzi degli immobili nel 2006, che non era sostenibile (Figura 4.1).

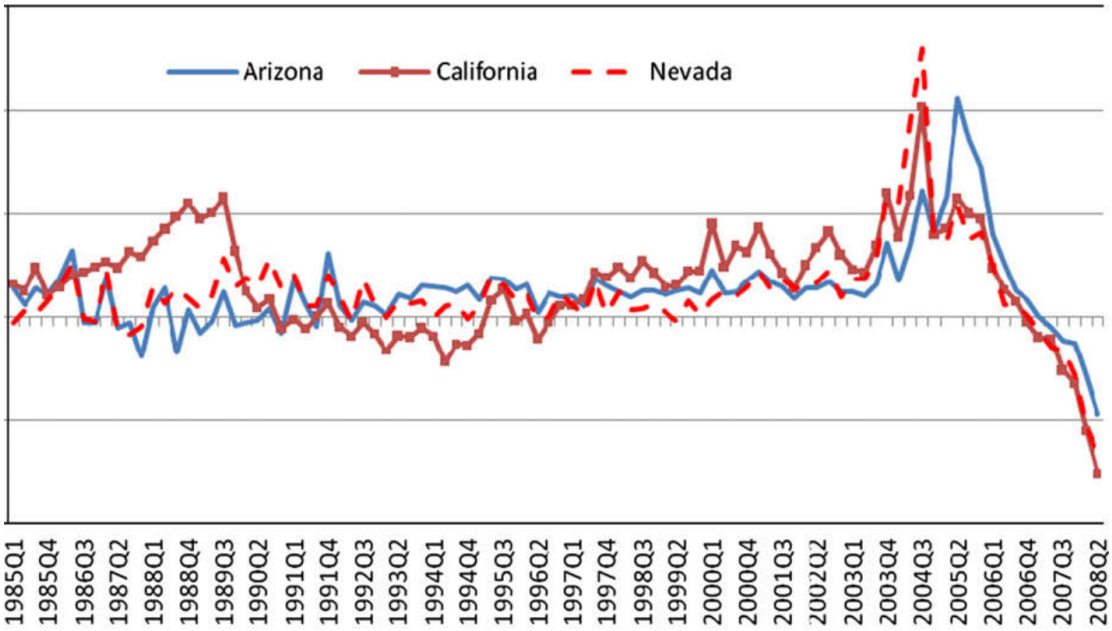

Figura 4.1: Crollo dei prezzi degli immobili in seguito alla crisi [29].

La crisi, derivante, portò al fallimento di Lehman Brothers con un debito residuo di circa 600 miliardi di dollari [30].

4.1 Una breve panoramica sulla blockchain

In questo paragrafo viene illustrato il funzionamento della crittografia dietro la blockchain e la generazione di funzioni hash. Inizialmente, verrà contestualizzato il periodo storico e la motivazione che ha portato allo sviluppo della tecnologia.

Bitcoin, la prima grande blockchain pubblica, nasce in seguito allo scandalo finanziario che coinvolse tutti i grandi istituti di credito. Il 3 gennaio 2009, riportando la frase "*chancellor on brink if second bailour for bank*", Satoshi Nakatomoto, fondatore di bitcoin, crea il primo blocco della catena. La stessa frase era stata riportata come titolo del *Times* e rappresentava, senza dubbio, una critica al sistema economico del periodo (Figura 4.2).

THE TIMES

Max 5C, min -5C Saturday January 3 2009 timesonline.co.uk No 69523 £1.50

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Start collecting tokens today Pullout inside

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37 billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets", The Times has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the boil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed guarantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

99p

Pub chain cuts the price of a pint from £1.69 to 1989 levels
Business, page 47

Salman Rushdie I won't marry again
Pages 22, 23

Giant killing? Guide to the FA Cup third round
Sport

Figura 4.2: Nascita di Bitcoin.

Ad oggi, Bitcoin rappresenta il primo grande sistema peer-to-peer, da persona a persona, per effettuare transazioni *trustless*, ovvero senza aver bisogno di fidarsi della controparte e senza intervento di autorità centrali. Il pensiero del fondatore "*adesso possiamo fare tutto senza che tutto crolli quando l'intermediario scompare*" rappresenta il punto di svolta portato da bitcoin e, più in generale, dalla blockchain. L'eliminazione, quasi totale, di un'autorità di cui fidarsi e a cui concedere i dati personali.

Il protocollo Bitcoin, idea fondante delle blockchain che si sono succedute nel corso degli anni, si basa su una struttura crittografica e pseudo-anonima, in grado di tutelare la privacy e l'identità degli utenti, facilitando gli scambi attraverso la piattaforma.

Nello specifico, si basa sulle seguenti proprietà:

- decentralizzazione: assenza di autorità centrale che vigila sui flussi di dati;
- sicurezza: impossibilità per terzi di prelevare il denaro;
- trasparenza: ogni transazione è memorizzata nella blockchain e non può essere modificata;
- velocità: l'elaborazione delle transazioni richiede pochi minuti e dipende dall'importo scambiato;
- anti-imbroglio: risolve il problema del *double spending*, ovvero la possibilità di spendere moneta elettronica due volte.

La vera innovazione portata da Bitcoin e da tutti i progetti Blockchain è utilizzare la *crittografia* come elemento fondamentale per assicurare la protezione del protocollo e dei dati inseriti all'interno. Essa si basa su due elementi:

- algoritmo: regola che permette di non far vedere chiaramente il messaggio trasmesso;
- chiave: mezzo per decriptare il messaggio originario.

La crittografia alla base delle più note blockchain, Bitcoin ed Ethereum su tutte, è di tipo *asimmetrico*, con due chiavi distinte: una chiave pubblica, utilizzata per criptare, ed una privata, utilizzata per decriptare. In tal modo, il mittente utilizza la chiave pubblica, del destinatario, per veicolare un messaggio che può essere decriptato, unicamente, dal destinatario autorizzato a leggerlo per mezzo della sua chiave privata (Figura 4.3).

Inoltre, per verificare che il messaggio sia integro, quindi non modificato da terze parti, utilizza le *funzioni hash* che producono, a partire da un testo di input, una stringa alfanumerica a 256 bit. Tale output prende il nome di *digest* e sfrutta l'algoritmo SHA, sviluppato dalla NSA (National Security Agency), per produrre stringhe,di 64 caratteri, uniche e irreversibili.

La funzione hash è fondamentale per garantire la sicurezza dei documenti, in modo da autenticarli in modo univoco e sicuro. Di seguito, si può notare il funzionamento del digest applicato a due frasi che variano, unicamente, per un segno di punteggiatura:

- *La tesi magistrale di Enrico Passaniti* produce il seguente output:
  f902f73446c1becb4305d96ee5c8e38f9e2195994b32aac9d622386825465247
- *La tesi magistrale di Enrico Passaniti.* produce, invece, il seguente output:
  ff3dd1d7874ae3d1f355fab3eee22e9553d9e50e685898f666b1f55cdddf22ee

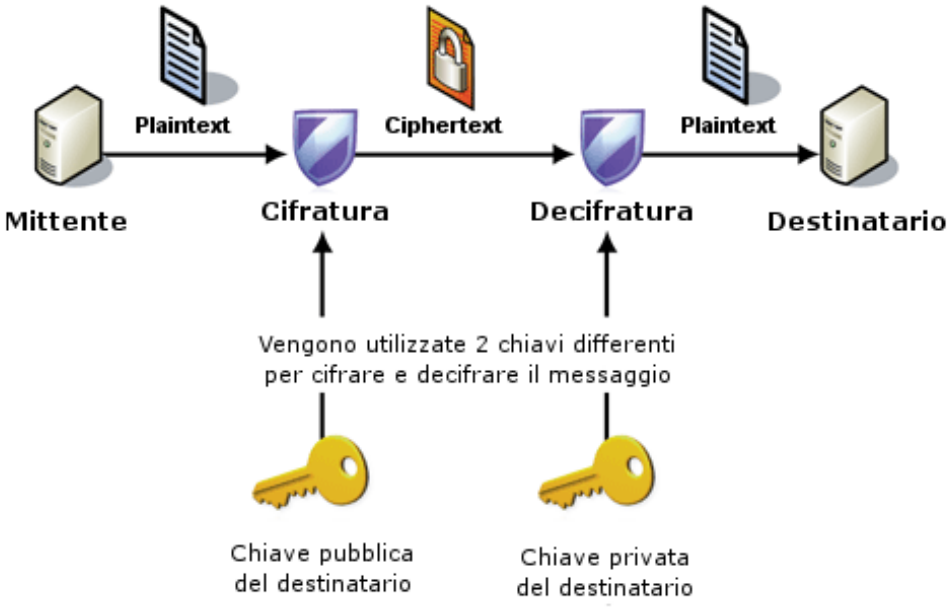

Figura 4.3: Funzionamento della crittografia asimmetrica [31].

È un tipo di funzione irreversibile in quanto dalla stringa prodotta non è possibile risalire al messaggio originario (messaggio di lunghezza arbitraria come nell'esempio sopra).

4.1.1 La blockchain da un punto di vista tecnico

Bitcoin, la blockchain associata alla valuta bitcoin, nasce dall'evidenza che la mediazione, che si ha nell'elaborazione di una transazione, aumenta il costo della transazione e, quindi, esclude il verificarsi di alcune di esse. Nel sistema tradizionale, la terza parte è necessaria per evitare che sia spesa valuta inesistente o che siano scambiate informazioni non veritiere.

In questo paragrafo viene rappresentata la soluzione della tecnologia blockchain al *double-spending*.

Il sistema ideato da Satoshi Nakamoto si basa sulla creazione di una valuta elettronica, intesa non come valore monetario ma come catena di firme digitali. Ogni soggetto può trasferire una valuta ad un altro attraverso la chiave pubblica del soggetto ricevente e firmando l'hash della transazione precedente.

Il ricevente non può verificare che i proprietari precedenti non abbiano effettuato più transazioni del dovuto e, quindi, speso due volte lo stesso denaro. La soluzione più facile per risolvere il problema sarebbe l'introduzione di un'autorità centrale

che sorvegli le transazioni. Il problema di questa soluzione è che il sistema monetario dipenderebbe, unicamente, da una società e si creerebbe un nuovo sistema centralizzato, equivalente a quello delle banche, che si vuole sostituire.

È necessario che ogni beneficiario sia sicuro che la transazione che lo riguarda sia autentica e non compromessa. Il miglior sistema, non avendo a disposizione un'autorità terza, per proteggere le informazioni, ma al tempo stesso vigilare sulla loro correttezza è renderle tutte pubbliche ed accessibili. In tal modo è facilmente verificabile se una transazione sia presente o meno.

Per attuare questa situazione, è necessario temporizzare tutte le transazioni ed essere in grado di ottenere un sistema di consenso, attraverso il quale ogni beneficiario possa essere al corrente che, almeno il 50 % + 1 dei nodi validatori abbiano approvato le transazioni. È stato, così, definito il *timestamp*, un pezzo di dato archiviato in ogni blocco, che agisce come identificatore e serve per determinare il momento esatto di estrazione e convalida del blocco nella rete blockchain (Figura 4.4). Ogni timestamp comprende il precedente nel suo hash, creando in tal modo una catena [32].

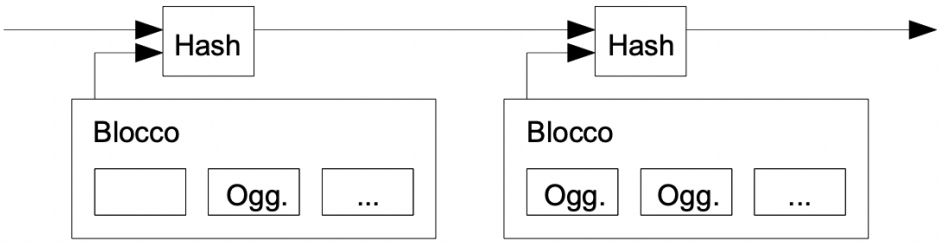

Figura 4.4: Timestamp [33].

Il server creato, basato su un contratto cliente-cliente, deve includere una soluzione che incentivi a non deviare dall'accordo. La soluzione adottata è una rivisitazione di Hashcash di Adam Back e prende il nome di *Proof-of-work* (POW). Alla base del funzionamento vi è la ricerca costante di un valore che, dopo essere stato sottoposto ad hash (SHA-256), restituisca un hash che ha come valore iniziale un numero di zero bit. Il lavoro richiesto, invece, non è costante ma esponenziale ed è proporzionale al numero di zero bit richiesti. La rete di hash, così creata, utilizza la POW aggiungendo un *nonce*, numero che può essere usato una sola volta,finché non è stato trovato un valore che conferisca gli zero bits necessari all'hash. La ricerca degli zero bits si basa su una competizione tra nodi validatori, attraverso lo sfruttamento di potenza computazionale delle CPUs dei loro computer. Una volta che il blocco è validato, esso non può più essere modificato e gli vengono aggiunti i nuovi blocchi della catena (Figura 4.5). Se si pensasse di voler cambiare il blocco

appena creato, bisognerebbe spendere molta più potenza computazionale in quanto sarebbe necessario cambiare, anche, i blocchi successivi.

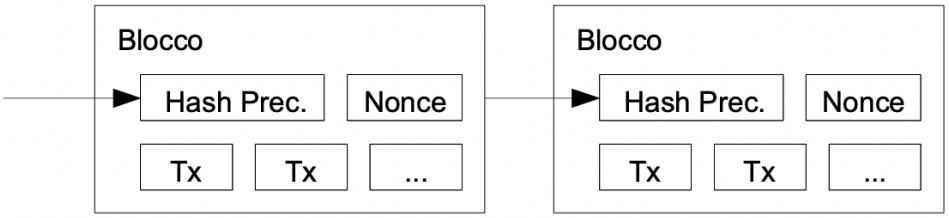

Figura 4.5: Catena di blocchi [33].

Il sistema decisionale della POW è basato sul principio *una CPU- un voto*. La catena più lunga rappresenta la maggioranza dell'intero network, in quanto su essa è stato speso il massimo sforzo, cioè è stata allocata al meglio la potenza computazionale. Questa soluzione risolve il principio *un indirizzo IP- un voto* che era inefficiente in quanto poteva essere eluso facilmente dagli utenti che fossero abili nel generare indirizzi IP multipli.

La difficoltà della POW è determinata da una media mobile, che tiene conto della variazione della velocità degli hardware e la variazione dei nodi che operano nel tempo. Il numero medio di blocchi creato ogni ora è costante ed è regolato attraverso la media mobile. All'aumentare della velocità di creazione dei blocchi, aumenta la complessità dell'algoritmo.

I nodi validatori sono degli utenti che sfruttano la potenza di calcolo dei loro computer per generare, e validare, dei nuovi nodi nella rete. Oltre alla POW, che permette di identificare la catena più lunga, è necessario un sistema di retribuzione che permetta la nascita di nuovi nodi, con informazioni corrette e non fraudolente. Il processo ideato, per compensare i nodi, è simile al processo di estrazione dell'oro, in quanto i minatori spendono risorse per incrementare la disponibilità di oro in circolazione. La risorsa, in questo caso, è la potenza della CPU e comporta una spesa di energia elettrica.

La prima transazione di un blocco della catena più lunga appartiene, metaforicamente, al *miner* (appellativo con cui si identifica il nodo validatore, per correlazione al processo di estrazione dell'oro) ed è valorizzato attraverso la coniazione di una nuova moneta. Essa rappresenta un incentivo a rimanere onesti. L'incentivo guadagnato deve essere superiore all'energia consumata ed è dato dalla somma del valore monetario della valuta ottenuta e dal costo delle transazione. In ogni caso, anche se poco probabile, non è esclusa la presenza di utenti malintenzionati che potrebbero voler generare una catena alternativa, più veloce di quella ufficiale. L'utente malintenzionato potrebbe solamente tentare di cambiare una delle sue transazioni

per recuperare denaro già speso, in quanto i nodi onesti non accetterebbero mai delle transazioni non valide.

Questa situazione è rappresentata da una *Binomial Random Walk*, passeggiata binomiale aleatoria. Si verifica l'evento successo quando la catena onesta è estesa di un blocco, aumentando il suo vantaggio di 1, invece si verifica l'evento insuccesso quando la catena del malintenzionato aumenta di 1 la propria dimensione, riducendo il divario di 1. L'utente malintenzionato parte da una situazione di svantaggio e la probabilità di recupero dal deficit può essere assimilata al teorema della Rovina del giocatore: in un gioco equo contro un banco illimitato ogni giocatore è destinato a perdere. La probabilità che l'utente malintenzionato possa raggiungere la catena onesta può essere calcolata come segue:

$$q_z = \begin{cases} 1, & \text{se p} \leq \text{q} \\ (\frac{q}{p})^z, & \text{se p>q} \end{cases}$$

dove

- p = probabilità che un nodo onesto generi il blocco successivo;
- q = probabilità che un utente malintenzionato generi il blocco successivo;
- q_z= probabilità che l'utente malintenzionato recuperi quando sono già stati generati z blocchi.

All'aumentare del numero di blocchi della catena diminuisce la probabilità che l'utente malintenzionato possa raggiungere la catena. Se il mittente di una transazione è il malintenzionato, il suo obiettivo sarà di recuperare il denaro speso senza che il destinatario si accorga in tempo dell'evento fraudolento.

Il mittente può preparare la catena di blocchi alternativa solo quando il destinatario gli da la propria chiave pubblica, come spiegato in precedenza. Questo permette di evitare che il mittente inizi a lavorare sulla catena alternativa da prima di ricevere l'indirizzo pubblico del destinatario, ma solo da quel momento in avanti.

Il tempo medio che il destinatario attende prima di vedersi approvata la transazione segue una distribuzione di Poisson, supponendo che il tempo medio sia lo stesso tempo medio atteso per un blocco onesto, con valore atteso:

$$\lambda = z \times \frac{q}{p}$$

Volendo ottenere la probabilità che l'utente malintenzionato possa recuperare in quel punto, si moltiplica la funzione di densità di probabilità di Poisson per ogni ammontare di progresso che può aver compiuto per la probabilità che possa recuperare da quel punto. In formule:

$$\sum_{k=0}^{\infty} \frac{\lambda^k \times e^{-\lambda}}{k!} \begin{cases} (\frac{q}{p})^{z-k}, & \text{if k} \leq \text{z} \\ 1, & \text{if k>z} \end{cases}$$

I risultati mostrano che la probabilità tende esponenzialmente a zero all'aumentare di z [33].

q=0.1	
z=0	p=1.0000000
z=1	p=0.2045873
z=2	p=0.0509779
z=3	p=0.0131722
z=4	p=0.0034552
z=5	p=0.0009137
z=6	p=0.0002428
z=7	p=0.0000647
z=8	p=0.0000173
z=9	p=0.0000046
z=10	p=0.0000012
q=0.3	
z=0	p=1.0000000
z=5	p=0.1773523
z=10	p=0.0416605
z=15	p=0.0101008
z=20	p=0.0024804
z=25	p=0.0006132
z=30	p=0.0001522
z=35	p=0.0000379
z=40	p=0.0000095
z=45	p=0.0000024
z=50	p=0.0000006

Nel modello decentralizzato appena descritto, oltre a preservare l'immutabilità della catena, è necessario garantire la privacy degli utenti. Il sistema tradizionale, centralizzato, limita l'accesso alle informazioni alle parti coinvolte e garantisce, in tal modo, la sicurezza delle informazioni. La blockchain, invece, suppone che la migliore protezione sia la pubblicazione di tutte le transazioni. Tutti vedono che qualcuno sta compiendo un'operazione ma non riescono a ricondurla ad un utente specifico in quanto le chiavi pubbliche sono anonime (Figura 4.6).

Questo sistema non è del tutto nuovo, ma in realtà segue il modello dei mercati azionari, i quali pubblicano la dimensione dei singoli scambi ma non rivelano

l'identità delle controparti. Inoltre, per evitare che all'aumentare delle transazioni aumenti la probabilità di risalire all'identità del soggetto, ad ogni nuova transazione deve essere utilizzata una nuova coppia di chiavi.

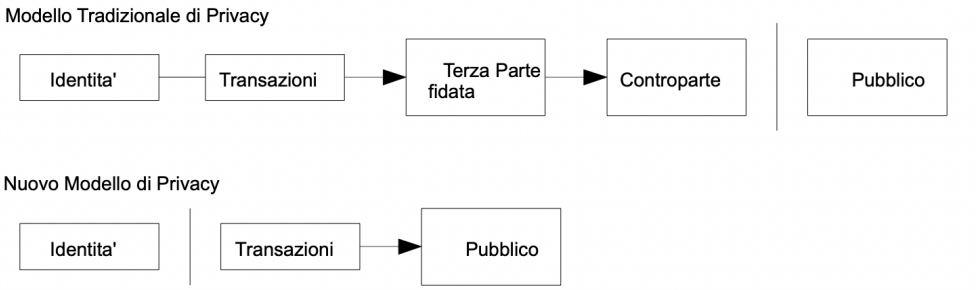

Figura 4.6: La privacy in blockchain [33].

Una volta introdotto il concetto di POW e crittografia asimmetrica, si può definire e far funzionare la rete come segue:

1. Trasmissione delle transazioni a tutti i nodi;
2. Le transazioni sono immagazzinate in un blocco dal nodo;
3. Ogni nodo lavora per trovare una POW difficile per il suo blocco;
4. Se un nodo trova la POW trasmette il blocco a tutta la rete di nodi;
5. Gli altri nodi accettano il blocco solo se tutte le transazioni sono valide, cioè se non si ha double-spending;
6. L'hash del blocco creato viene usato per convalidare il blocco successivo.

Alla base di questo sistema vi è il principio che la catena più lunga sia la catena non manomessa e, quindi, quella su cui lavorare. Se i nodi ricevessero contemporaneamente due versioni diverse del blocco, lavorerebbero inizialmente sul primo che hanno ricevuto, controllando il timestamp, ma salverebbero la seconda ramificazione nel caso diventasse più lunga. La rete di riserva viene scartata quando la proof of work successiva è trovata ed una delle due ramificazioni diventa più lunga.

4.1.2 Il problema dei generali bizantini

Le blockchain di Bitcoin ed Ethereum, oltre ad essere le più famose, risolvono il problema dei generali bizantini. In questo paragrafo verrà presentato cosa si intende per *il problema dei generali bizantini* (BFT), chiarendo come opera la blockchain. Esso viene presentato in una trattazione a parte, in quanto non tutte le blockchain

sono in grado di risolvere tale problema matematico. Il BFT è un termine coniato, nel 1982, da Leslie Lamport, Marshall Pease e Robert Shostak per descrivere un problema d'accordo che si verifica nelle reti decentralizzate.

Il dilemma, riconducibile alla teoria dei giochi, ipotizza che ci siano tre o più generali che stiano per attaccare una città nemica. Nello specifico:

- i generali si trovano in punti strategici diversi;
- i generali possono comunicare, solo, attraverso dei messaggeri per coordinare l'attacco [34].

I generali, dopo aver accerchiato la città, devono decidere se attaccare o ritirarsi. Tra i messaggeri, però, è probabile ci sia un traditore che potrebbe mandare messaggi contrari alla strategia, scelta dal comandante superiore, e portare l'intero esercito alla sconfitta.

Per poter vincere è necessario che tutti i generali eseguano la stessa azione, ovvero che si raggiunga il *consenso decentralizzato*. Senza consenso è, altamente, probabile che il messaggio di attacco non sarà coordinato e, contemporaneamente, alcuni generali attaccheranno ed altri si ritireranno (Figura 4.7).

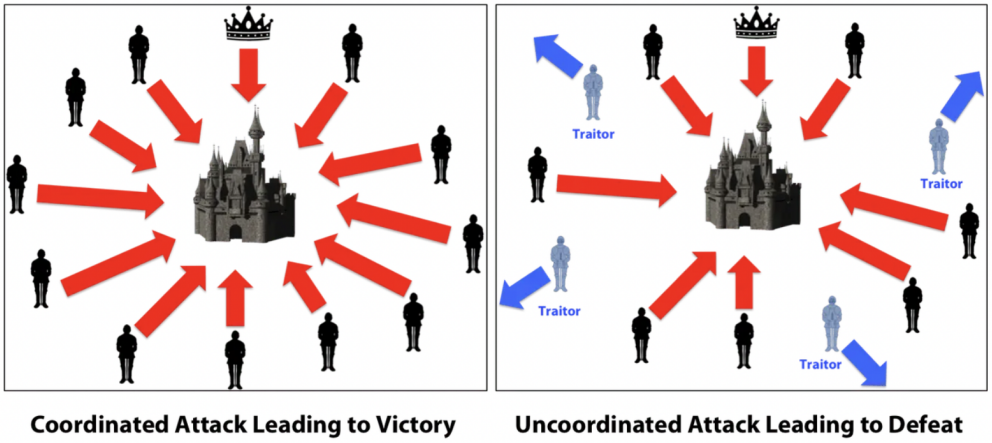

Figura 4.7: Il problema del consenso decentralizzato [34].

Il problema ha trovato una soluzione, solo, nel 2008 con Bitcoin. Satoshi Nakamoto, il suo fondatore, spiegò che bisognava focalizzarsi sulla comunicazione. Infatti, un generale poteva comunicare con un altro solo attraverso un messaggio recapitato da un messaggero. In tal modo, era lecito aspettarsi che il messaggio potesse subire delle manipolazioni.

Applicando la metafora alla blockchain, ogni generale rappresenta un nodo e i nodi devono ottenere il consenso sull'intera rete. La maggioranza del network deve concordare sull'azione da eseguire. Il messaggio, scambiato sull'intero network,

sarà criptato e decifrabile attraverso la soluzione di un problema matematico molto complesso (*funzionamento della proof of work*). Questo permette di evitare che il messaggio possa essere contraffatto e permette di stabilire con esattezza il momento d'attacco.

Il nodo che decripta il messaggio si pone come nodo validatore e si pone come nodo di partenza dell'intera catena. Più la catena, di nodi, è lunga più è facile che l'intera rete lavori in maniera sincrona ed efficiente.

Con la risoluzione del problema, ogni nodo assume la valenza di server associato al partecipante. In tal modo, i nodi si comportano da controllori e validatori, vigilando sulle transazioni e avendo accesso all'intera rete costruita.

4.2 Le modifiche alla prima blockchain

La blockchain ideata da Satoshi Nakamoto, la prima grande blockchain pubblica, presentava delle ridigità. In questo paragrafo verrà illustrato come queste possono essere superate e verrà introdotta una nuova tipologia di blockchain.

Le transazioni sulla rete Bitcoin sono lente e complesse, cinque transazioni al secondo, ed inoltre vi è un dispendio energetico molto elevato. Per questo motivo è stata introdotta la possibilità di fare degli *hard fork* della rete.

L'hard fork è la modifica del codice originario con l'obiettivo di correggere bug presenti o migliorare le performance della rete. In tal modo, con l'attuazione di nuove regole, si originano due blockchain distinte con regole e procedure diverse. Esso si origina quando parte della rete concorda sulla bassa efficacia di alcune regole che governano la blockchain, in modo da crearne una seconda competitiva con norme alternative. La nuova blockchain dispone, ugualmente, dei dati salvati sulla rete originaria fino a quel momento. Il fork descritto consente di introdurre la competizione tra reti diverse, ma generate dallo stesso nodo.

4.2.1 La Proof Of Work è dispendiosa

La blockchain, come descritto nei paragrafi precedenti, utilizza ingenti quantità energetiche per garantire la correttezza dei dati e, al tempo stesso, la decentralizzazione. L'utilizzo, incessante, di terminali CPU attaccati alla rete elettrica non permette l'efficienza da un punto di vista monetario. Proprio per questo è stato introdotto il termine *blockchain trilemma* che stabilisce che sia impossibile soddisfare contemporamentamente tre proprietà [35], come mostrato in Figura 4.8:

- correttezza;
- decentralizzazione;
- efficienza di costo;

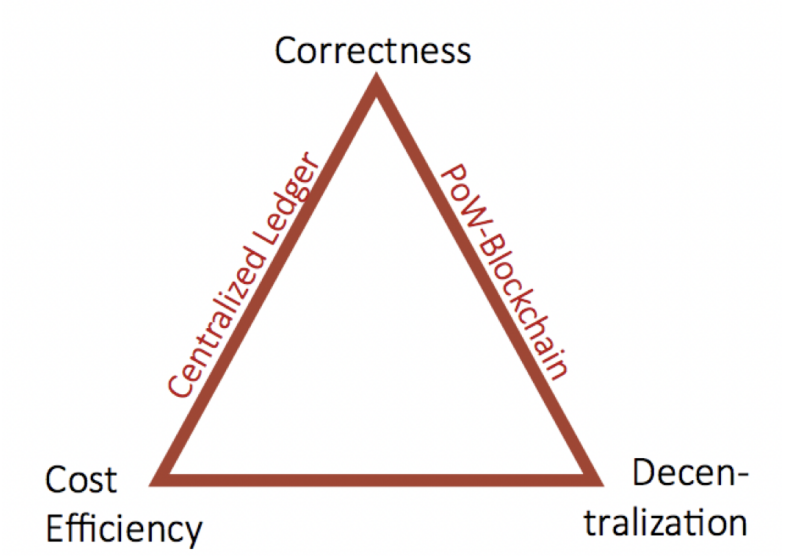

Figura 4.8: Il blockchain trilemma [35].

Infatti, la blockchain pubblica non è per nulla efficiente se si analizza l'utilizzo di risorse. Il protocollo, per garantire l'inviolabilità della rete, è basato infatti sulla duplicazione dei dati su ogni terminale connesso alla rete. I miners competono tra loro, sfruttando la potenza computazionale dei loro dispositivi, per risolvere l'enigma matematico e validare un nuovo blocco. In questo modo si determinano due risorse fisicamente scarse [36]:

- l'hardware richiesto per eseguire la computazione matematica;
- l'energia elettrica richiesta per alimentare gli hardware.

La potenza computazionale richiesta da un'intera rete blockchain è difficilmente misurabile, in quanto dipende dal numero di dispositivi connessi alla rete e dalla quantità di calcoli hash necessari per sbloccare i nuovi nodi. La letteratura attuale ha concentrato i suoi sforzi per determinare il consumo energetico della blockchain di Bitcoin, essenzialmente per due motivi:

- è la prima grande blockchain pubblica;

- è caratterizzata da un elevato numero di nodi validatori.

Si stima che il network Bitcoin abbia 10 mila nodi connessi ma ogni nodo non è rappresentato da un singolo hardware, quindi è difficile determinare con esattezza quanti siano gli hardware operanti nella rete [37].

Non è direttamente osservabile l'hashrate, potenza di elaborazione della rete Bitcoin, ma questo numero può essere ricavato dalla difficoltà e dal tempo richiesto per minare un nuovo blocco. Ogni secondo sono elaborate circa 26 milioni di miliardi di operazioni di hashing ininterrottamente (Figura 4.9). "Un hashrate di 14 terahash/sec può derivare da un singolo Antminer S9 in esecuzione su 1372 W" [37].

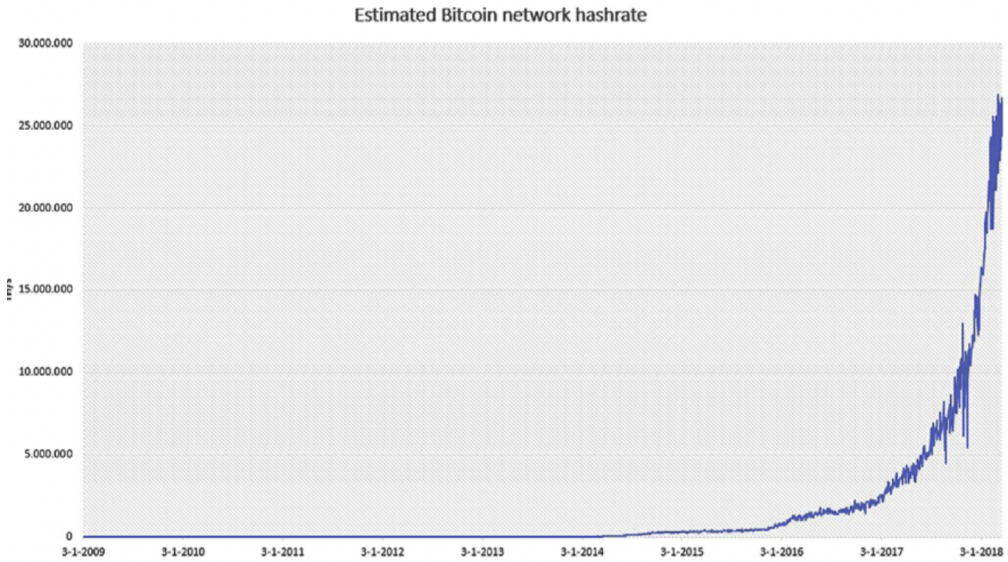

Figura 4.9: Operazioni di hashing eseguite dalla rete Bitcoin [37].

Ogni dispositivo, però, ha un'efficienza energetica differente (Tabella 4.1). Non si può determinare il consumo energetico preciso, ma soltanto un lower-bound e un upper-bound. Supponendo, quindi, che nella rete siano presenti unicamente dispositivi Antminer S9, con un'efficienza energetica di 0,098 Joule per gigahash, si trova un lower bound di 2,55 GW (26 milioni di milardi di operazioni di hashing per l'efficienza energetica).

Inoltre, l'ipotesi presentata non tiene conto della necessità di raffreddamento delle farm in cui sono contenuti i dispositivi, che fa aumentare il consumo energetico. Per calcolare il consumo di elettricità si può fare una stima dal punto di vista economico, considerando che gli hash siano prodotti finché il costo marginale per produrli non superi il prodotto marginale.

Hardware	Hashrate (TH/s)	Potenza usata (W)	Efficienza energetica (J/GH)
Antminer S9	14	1,372	0,098
Antminer T9	12,5	1,576	0,126
Antminer T9+	10,5	1,332	0,127
Antminer V9	4	1,027	0.257
Antminer S7	4.73	1,293	0.273
AvalonMiner 821	11	1,200	0.109
AvalonMiner 761	8.8	1,320	0.150
AvalonMiner 741	7.3	1,150	0.160
Bitfury B8 Black	55	5,600	0.11
Bitfury B8	47	6,400	0.13

Tabella 4.1: Hardware utilizzati nella rete Bitcoin ed efficienza energetica [37].

Il prodotto marginale, ricompensa del miner per aver inserito un nuovo blocco, è pari a 24 milioni di $, dato dal valor medio osservato di bitcoin (27 mila $) per il numero di bitcoin prodotti ogni 10 minuti (6,25) per il numero di minuti di una giornata.

I costi marginali sono caratterizzati dal costo dell'energia elettrica e dal costo dei macchinari. Un Antminer S9 ha un costo di produzione di 500 $ ed una durata media attesa di 2 anni. Supponendo un costo dell'energia di 0,05 $ per KWh, si trova che il costo dell'energia elettrica costituisce circa il 70 % del costo totale di un Antminer S9 (Figura 4.10).

Machine	Expected Lifetime (Years)	Estimated Production Costs (US$)	Lifetime Electricity Use (kWh)	Lifetime Electricity Costs (US$)	Total Lifetime Costs (US$)	Electricity Costs/Total Costs (%)
Antminer S9	2	500	24,037	1,202	1,702	70.6
Antminer S9	1.5	500	18,028	901	1,401	64.3
Antminer S9	1	500	12,019	601	1,101	54.6

Figura 4.10: Costo stimato di un dispositivo Antminer S9 [37].

In questo modo si riesce a calcolare l'impatto energetico della rete, considerando il 70 % del costo totale in equilibrio, pari ad un consumo di 25,2 GW.

Questo approccio, data la sua semplicità, è usato per calcolare il *Bitcoin Energy Consumption Index*, che stima l'energia attuale consumata dal network Bitcoin

[38]. Attualmente, stima un consumo di circa 150 TWh per anno, paragonabile al consumo energetico della Malesia e con un'impronta ecologia di 72 milioni di tonnellate di CO_2 all'anno, paragonabile al carbon footprint della Grecia (Figura 4.11).

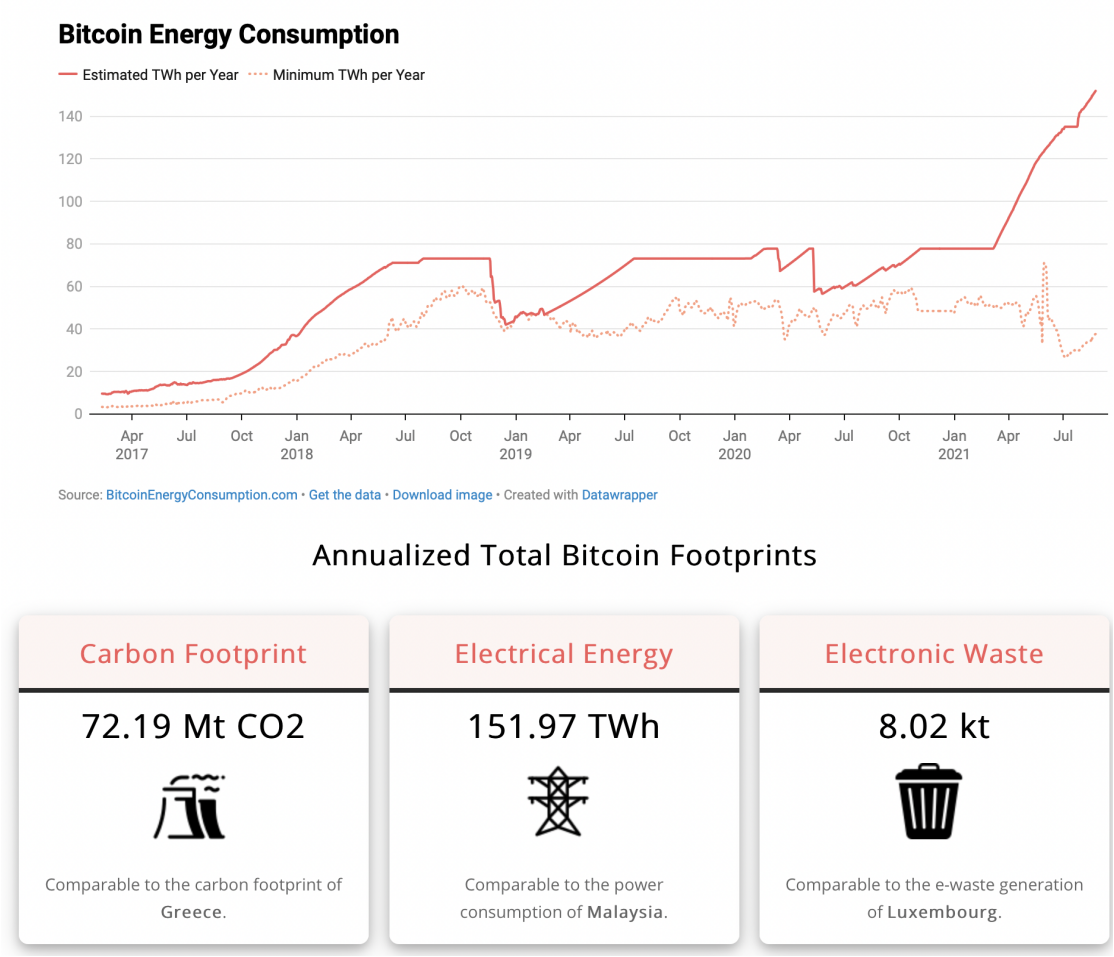

Figura 4.11: Bitcoin Energy Consumption Index [38].

Analizzando, invece, una singola transazione e rapportandola alle normali transazioni VISA, si percepisce la mole di energia consumata. Una singola transazione in Bitcoin consuma 10 volte l'equivalente energetico per 100 mila transazioni Visa (Figura 4.12).

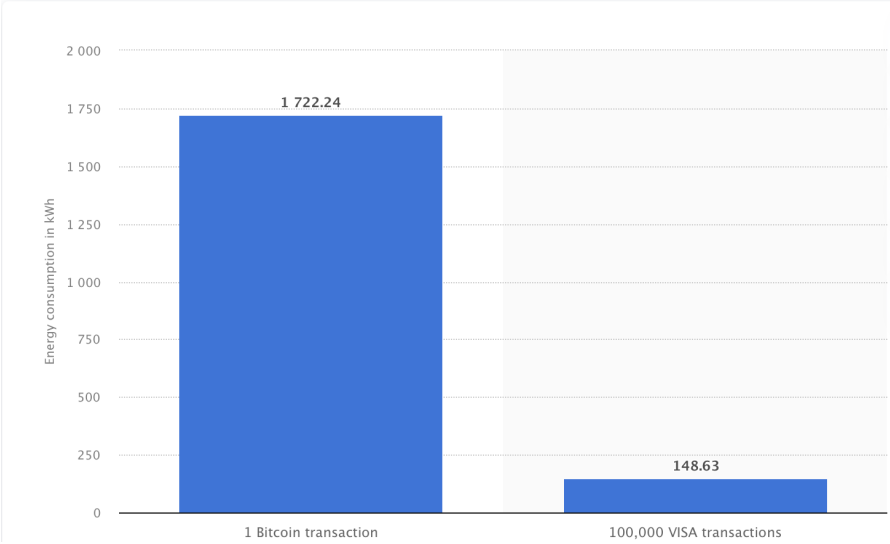

Figura 4.12: Consumo energetico del network Bitcoin per transazione confrontato con quello del circuito VISA [39].

Per ovviare a questo problema, sono state proposte ed inventate delle blockchain di tipo privato. In questo tipo di blockchain, solo l'autorità centrale ha il potere di scrivere e modificare il registro. Gli utenti e le altre entità, invece, hanno il potere di lettura dei dati condivisi. Poiché l'informazione certificata passa da un unico nodo, la POW non è più necessaria e si elimina, quindi, l'utilizzo massivo delle risorse. D'altro canto, però, la blockchain in esame somiglia più al sistema tradizionale, costituita da un unico controllore, che a reti decentralizzate. La differenza, concreta, con il modello centralizzato è che gli utenti vigilano, attivamente, sul rispetto delle regole, da parte del nodo centrale, e possono promuovere un suo allontanamento se si verificano attività fraudolente (ad esempio, dati non usati correttamente).

In ogni caso, è confermata la veridicità del trilemma. È impossibile, fino ad ora, trovare una soluzione efficiente che soddisfi le tre proprietà descritte in precedenza.

4.3 Ethereum e gli smart contract

In questo paragrafo verrà presentata la rete decentralizzata Ethereum, che si contraddistingue per la possibilità di creazione degli smart contract. Inoltre, si proverà a comprendere come Ethereum stia provando a risolvere il problema dell'eccessivo consumo energetico.

Ethereum è la principale blockchain alternativa a Bitcoin. La sua valuta di riferimento, *ether (ETH)*, è definita *altcoin* per rimarcare il concetto di alternative coin al bitcoin. Il progetto Ethereum, nato nel 2013, a differenza di Bitcoin mira a

creare un sistema decentralizzato per la memorizzazione di dati non, strettamente, per fini monetari.

Ethereum è la prima, grande, blockchain programmabile:

- permette di eseguire transazioni predefinite;
- permette di creare delle applicazioni blockchain decentralizzate *(dApp)*.

La blockchain di Ethereum è la prima blockchain che immagina un'applicazione non di tipo strettamente economico. Introduce la possibilità di creare contratti intelligenti per gestire, al meglio, ogni tipo di transazione.

Gli smart contract non nascono con la blockchain ma trovano la loro utilità con le reti decentralizzate perché rafforzano, a vicenda, l'idea di trust e sicurezza.

Nel 1994 Nick Szabo ha, per la prima volta, introdotto il concetto di contratto intelligente definendolo come un "*protocollo transazionale computerizzato che esegue i termini di un contratto*". Un contratto intelligente, semplicemente, traspone il contenuto di un contratto tradizionale e si attiva quando si verificano determinate situazioni [40]. Tutte le informazioni necessarie per eseguire la transazione sono salvate nel contratto e non è necessaria la presenza di una terza parte.

Gli smart contract, indipendentemente dal linguaggio di programmazione utilizzato per crearli, dispongono di proprietà comuni:

- sono autonomi, una volta creati non hanno bisogno di essere monitorati;
- sono distribuiti;
- sono parte integrante di un applicativo.

I primi smart contract trovano applicazione nel mondo retail. Essi permettono, definendo *ex-ante* le condizioni di vendita, di agevolare le vendite e di ridurre i tempi medi delle transazioni.

Gli sviluppatori sono in grado di personalizzare lo smart contract in modo da soddisfare differenti interessi. Ad esempio, il contratto potrebbe attivarsi e permettere il salvataggio di dati in una transazione.

Gli smart contract, utilizzati in un sistema blockchain, sono aggiunti ad ogni nodo per evitare la manomissione di un solo blocco (*contract tampering*).

Attualmente, si sta sperimentando l'uso di smart contract, inseriti in reti blockchain, come metodo di rilascio di certificati digitali sicuri. Essi possono essere usati come metodo per rilasciare certificati di laurea, non manomissibili. La prima sperimentazione ha avuto luogo in Taiwan, per combattere il fenomeno, sempre più crescente, della contraffazione dei certificati di laurea [41].

Il sistema, basato su blockchain di Ethereum, prevede in una prima fase la creazione di una copia digitale del certificato, cartaceo, di laurea, collegandogli

un hash: esso, in un secondo momento, verrà inserito nella blockchain e rilascerà, in automatico, un codice QR. In questa fase agisce lo smart contract: se i dati dell'utente, precedentemente inseriti nella blockchain, e i dati del certificato corrispondono, allora verrà rilasciato in automatico il QR-code.

In questo modo migliora la credibilità delle certificazioni, evitando una possibile manomissione. È bene specificare che gli smart contract svolgono la loro funzione se associati ad una blockchain. Valutando il caso descritto sopra, senza l'utilizzo della rete blockchain lo smart contract non sarebbe riuscito a garantire la validità dei dati. Avrebbe, in ogni caso, potuto generare un codice QR, ma non avrebbe potuto assicurare l'unicità dello stesso. Nel sistema tradizionale, infatti, è possibile certificare delle informazioni e riportarle in forma elettronica, come ad esempio con il *green pass* anti-Covid, ma non è possibile essere sicuri che il pass generato sia utilizzato dagli aventi diritto (falsificazione del dato).

In questo lavoro il focus sarà incentrato sulle applicazioni in ambito *healthcare*.

La blockchain, attraverso la funzione chiave della protezione dei dati, può rappresentare il nuovo paradigma da usare nella sanità, per garantire sicurezza all'utente e, al tempo stesso, sfruttare economie di rete per ottenere un sistema più efficiente.

4.3.1 La Proof of stake come soluzione al consumo energetico

La rete Ethereum sta provando, attraverso un fork che entrerà in vigore entro fine 2021, ad attuare un sistema basato su *proof of stake* (POS). La POS è un meccanismo di consenso basato sul concetto di interesse attraverso la disponibilità di una quota (stake). A differenza della POW, in un sistema POS gli utenti non competono per la validazione di un nuovo blocco ma sono scelti in maniera pseudo-casuale dall'algoritmo. La probabilità di selezione di un nodo dipende dal periodo di staking, dai fondi posseduti dal nodo e da un processo randomico.

Per poter essere selezionati, gli utenti devono mettere in staking una somma fissa (moneta nel caso di Ethereum) all'interno del network. Per non favorire, unicamente, gli utenti con elevata disponibilità vi sono dei processi randomici che si aggiungono alla maggiore probabilità di selezione per staking elevato. Ad esempio, il metodo *Coin Age* sceglie i nodi in base a quanto tempo hanno lasciato i propri token congelati sulla rete [42].

Per far avvenire il passaggio da POW a POS, è stata creata una rete Ethereum parallela (*Beacon Chain*) che è necessaria per compiere la migrazione completa.

Carl Beekbuizen, sviluppatore ETH 2.0, termine che identica la nuova catena ETH, ha stilato un rapporto sull'efficienza energetica del nuovo protocollo. Per svolgere le proprie analisi, ha utilizzato 87897 nodi validati da 16405 indirizzi univoci. Ha osservato che POS risulta, circa, 2000 volte più efficiente a livello

energetico (Figura 4.13) e porta ad una riduzione del 99,95 % del consumo di energia [43].

Si rimanda all'analisi completa per considerazioni di tipo tecnico.

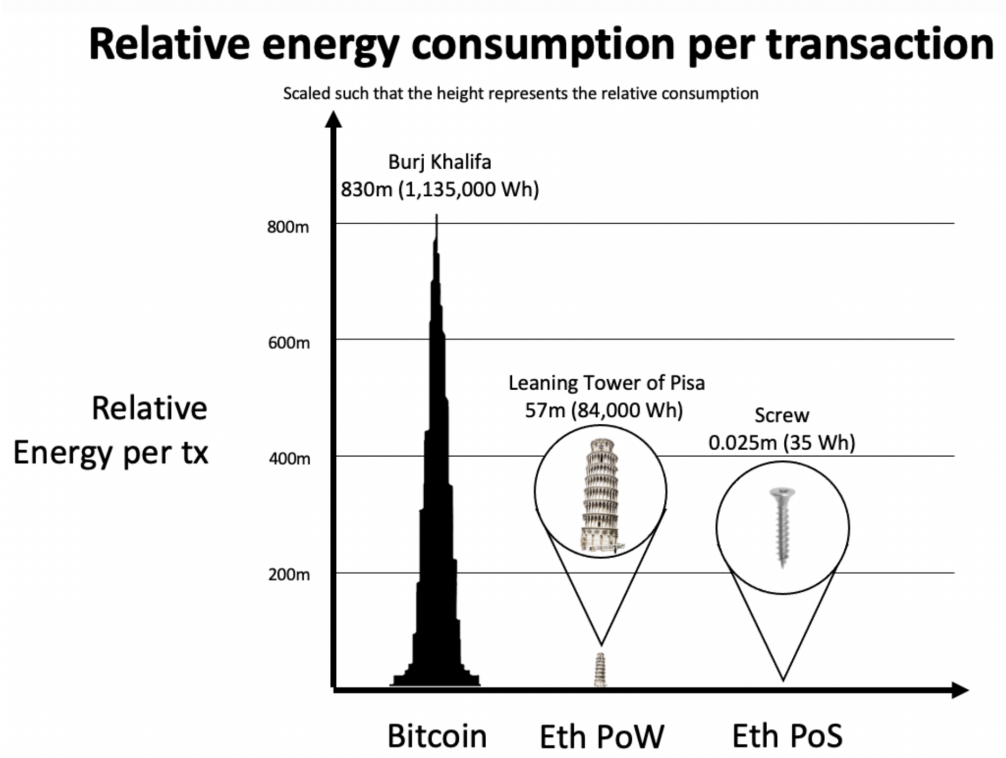

Figura 4.13: Il consumo energetico con POS [43].

La soluzione proposta da ETH sembrerebbe risolvere il trilemma, in quanto è più efficiente in termini di risorse consumate, assicura la decentralizzazione e la correttezza dei dati. A differenza della POW, però, si potrebbe verificare il fenomeno *nothing at stake* (NAS), per il quale la posta in gioco è talmente bassa da rendere conveniente il rischio di perderla per provare un'azione fraudolenta [44]. In tal modo, la correttezza dei dati verrebbe meno. Sebbene il verificarsi dell'evento NAS sia poco probabile, se ciò accadesse porterebbe ad una validazione di nodi fraudolenti.

Ancora una volta, nonostante le migliorie apportate da POS in ambito energetico, è confermata la difficoltà di soluzione al trilemma della blockchain.

Capitolo 5

La blockchain applicata al settore medico

L'interesse per la tecnologia blockchain è aumentato esponenzialmente negli ultimi anni. Dal 2008, anno in cui è stata introdotta, ad ora ha subito diversi aggiornamenti e migliorie. In poco più di 10 anni la percezione della blockchain è variata, non essendo unicamente associata alle criptovalute.

La letteratura recente la descrive come una possibile general purpose technology (GPT), in quanto non è più identificabile, solamente, con il settore delle criptovalute ma è potenzialmente adottabile da tutti ed, inoltre, incoraggia la creazione di innovazioni [45]. Tra i nuovi campi d'applicazione vi è il settore medico.

Nel 2017 è stata condotta una ricerca, per verificare l'interesse per la blockchain, somministrata a degli studenti dell'ultimo anno della scuola di Medicina di Zagabria (Croazia). Il 75,4 % degli studenti ha affermato di non aver mai sentito parlare di blockchain e, solo, il 3,4 % ha dichiarato di monitorarla costantemente [46]. Dal 2017 ad oggi, però, la tecnologia blockchain si è evoluta e il suo interesse in campo medico è aumentato. Sono state sviluppate soluzioni *private* che attribuiscono il potere di scrittura, solamente, ad alcuni membri (ad esempio le case farmaceutiche) ma la lettura a tutti i partecipanti al network. In tal modo si argina, completamente, il rischio di un attacco da parte della totalità del network, il cosiddetto *attacco del 51 %*, e si instaura il principio secondo cui i dati sono condivisi in maniera sicura. Una rete del genere, di tipo privato, permetterebbe comunque ai pazienti di vigilare sull'uso corretto dei loro dati, senza la necessità, per il sistema sanitario, di attuare una soluzione energeticamente dispendiosa come la POW.

In questo capitolo verrà mostrata, inizialmente, un'evidenza dell'esistenza del paradosso della privacy anche in campo medico e, successivamente, verrà presentata la blockchain ideata da IBM per la distribuzione dei vaccini in America. L'obiettivo è di limitare attacchi informatici a strutture pubbliche, che possano compromettere

i dati di migliaia di persone e possano causare difficoltà logistiche. Ad esempio, l'attacco informatico alle reti della Regione Lazio, con conseguente blocco nella somministrazione dei vaccini, evidenzia l'importanza di una struttura difficilmente accessibile.

In ambito sanitario la blockchain non ha trovato, ancora, un paradigma definitivo. Per questo motivo, si è scelto di rappresentare le proprietà della blockchain attraverso la descrizione del caso studio IBM.

Una prima applicazione, portata avanti dalla startup americana Patientory, punta a creare un sistema di economia chiusa, attraverso il quale i pazienti siano remunerati per i dati forniti ed i medici valutati, e pagati di conseguenza, per le prestazioni fornite [47].

5.1 La blockchain per contrastare il paradosso della privacy in campo medico

Negli ultimi anni sono stati creati ed immessi nel mercato numerosi dispositivi per monitorare la salute dei cittadini. Queste apparecchiature, definite in America come mobile health(m-health), permettono di controllare parametri vitali, come ad esempio il battito cardiaco, e segnalano eventuali anomalie. Svolgono una funzione essenziale di controllo delle condizioni di salute. Inolte, permettono di associare il contatto del medico e di inoltrare in tempo reale il risultato delle anomalie riscontrate (Apple watch con la funzione ECG).

Questi dispositivi, però, memorizzano dati e li condividono, anche, con terze parti. Oltre ai potenziali benefici citati, è necessario porre attenzione ai rischi per la privacy degli utenti. Sarebbe dannoso e controproducente se i dati ceduti a terzi creassero delle discriminazioni [48].

Anche a livello sanitario si verifica il fenomeno del paradosso della privacy, con risultati pressoché simili a quelli mostrati nei capitoli precedenti. Dal punto di vista del paziente emerge un livello di fiducia elevato verso i dispositivi di monitoraggio, nonostante il 79 % delle applicazioni ceda i dati personali a terze parti [49].

In campo medico la definizione di privacy non si discosta troppo dalla definizione canonica e può essere definita come "il desiderio di una persona di avere un maggior controllo sulla raccolta e la diffusione dei propri dati personali da parte delle organizzazioni sanitarie e dei produttori di tecnologie ad esse connesse" [50].

Si registra una correlazione negativa tra la volontà di un paziente di aderire ad un sistema informatizzato e le maggior restrizioni messe in pratica per salvaguardare la sua privacy [51]. Un fenomeno simile, descritto nel capitolo 3 di questa trattazione, si è verificato con l'introduzione del GDPR che ha portato una diminuzione delle intenzioni d'acquisto dei consumatori.

La letteratura disponibile ha analizzato le credenze sulla privacy attraverso un modello PCT, secondo il quale gli individui sono disposti a cedere i propri dati personali finché i benefici attesi superano i rischi percepiti [52]. Si valutano i benefici attesi dai pazienti congiuntamente ai lori timori riguardanti la privacy per formulare una correlazione con l'adozione di dispositivi medici portatili (Figura 5.1). Si ipotizza che i timori per la privacy influenzino negativamente l'adozione di nuove tecnologie, invece i benefici attesi abbiano una correlazione positiva. È necessario includere, anche in questo caso così come analizzato nei capitoli precedenti, eventuali bias comportamentali degli utenti che causano una valutazione sbagliata dei rischi e benefici.

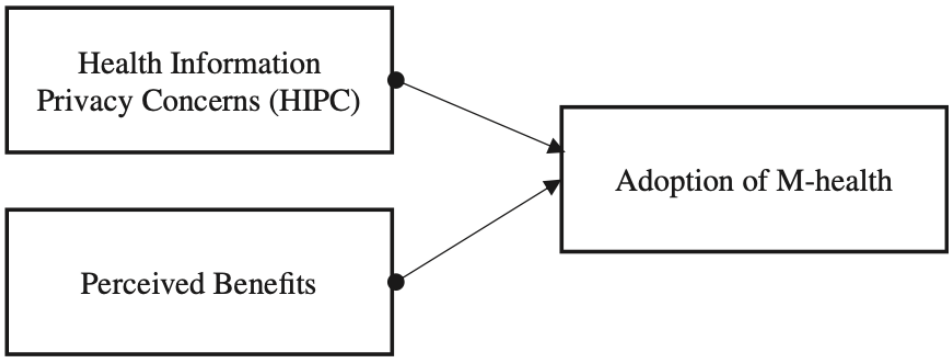

Figura 5.1: Modello PCT [52].

I risultati ottenuti confermano l'esistenza di un paradosso della privacy anche in campo medico. La maggior parte delle persone, sottoposte ad un sondaggio, dichiara di tenere fortemente alle proprie informazioni mediche e di non volere che i propri dati finiscano nelle mani sbagliate. Inoltre, affermano di non essere disposti in alcun caso a condividere i propri dati con i produttori di tecnologie in campo medico perché preoccupati di, eventuali, rivendicazioni economiche.

Emerge che la decisione di adottare le nuove tecnologie sia influenzata dal bias dell'immediata gratificazione, che porta l'utente a sovrastimare i benefici e valutare ex-post i problemi legati alla privacy. La maggior parte di loro, infatti, afferma di tenere molto alla privacy e che disinstallano un'applicazione se questa richiede molte informazioni. Il tutto, però, dopo averla usata per mesi [52].

Il paradosso della privacy in campo medico, più che in altri campi, è un fenomeno che deve essere limitato. Le nuove tecnologie permettono di raccogliere i dati molto facilmente, permettendo di aggregarli e portare avanti la ricerca. È necessario, però, che i dati siano raccolti con scrupolo, secondo delle regole precise e con scopi ben delineati. La raccolta di dati con un fine non specifico comporta uno spreco di risorse non indifferente.

La blockchain, come tecnologia abilitante, può essere necessaria per ridurre il fenomeno del paradosso della privacy. Gli utenti avrebbero una maggiore consapevolezza dei dati che stanno condividendo e, sopratutto, saprebbero con chi li condividono e con quale scopo finale.

I recenti modelli di sanità digitale, già adottati in America e parzialmente in Irlanda, potrebbero beneficiare di un'integrazione con la rete blockchain. Infatti, emerge che i pazienti americani siano disposti a cedere i loro dati a patto che le loro informazioni siano usate solo per finalità mediche. Inoltre, emerge da studi effettuati su un campione di pazienti americani ed irlandesi, che le preoccupazioni per la privacy quando ci si confronta con lo specialista sono minime e i pazienti sono disponibili a cedere i loro dati con finalità di ricerca.

La blockchain, in questo campo, permetterebbe di dare più sicurezza al paziente e, al tempo stesso, poter utilizzare al meglio i dati, evitando la raccolta generica degli stessi.

5.2 La blockchain per la distribuzione dei vaccini

La pandemia da Covid-19 ha creato instabilità nella popolazione. Le continue modifiche al piano vaccinale, dovute a fenomeni avversi che si sono verificati su una fascia della popolazione, hanno aumentato la diffidenza verso le istituzioni e verso il vaccino stesso. La scarsa sperimentazione e i bassi tempi di sviluppo non hanno favorito l'adesione di massa attesa. È necessario, però, che gli Stati intervengano per portare a conclusione il piano vaccinale delineato ed arginare, al meglio possibile, la diffusione del virus.

IBM, con la collaborazione di KPMG, Merck e Walmart, per testare le funzionalità e l'applicazione della blockchain in campo medico, ha lanciato un progetto pilota volto a migliorare la *supply chain* del settore farmaceutico [53]. Una legge degli Stati Uniti, la "*Drug Supply Chain Security Act* " (DSCSA), stabilisce che le case farmaceutiche debbano collaborare per garantire, come fine ultimo, la sicurezza del paziente. L'obiettivo è di monitorare e tracciare tutte le prescrizioni per farmaci che necessitano di ricetta medica (*prescription drugs*). Tale sistema ha permesso di migliorare l'intera rete farmaceutica americana (Figura 5.2). Nello specifico, la blockchain:

- ha permesso di mettere in contatto enti diversi, creando un'unica interfaccia accessibile sia ai distributori che alle case farmaceutiche;

- ha aumentato la sicurezza dei clienti, sostituendo il richiamo, manuale, dei prodotti difettosi con degli alert inseriti nello smart contract.

L'utilizzo della blockchain ha permesso di migliorare i processi di gestione della supply chain e implementare un sistema automatico di richiamo dei prodotti non conformi.

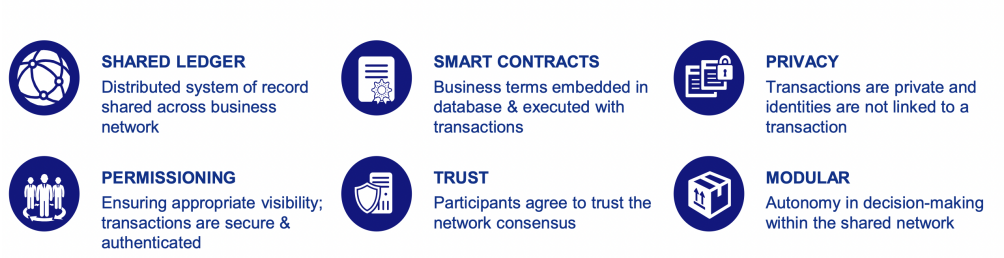

Figura 5.2: Benefici derivanti dall'implementazione della rete blockchain [53].

Sulla base dei risultati positivi ottenuti, IBM e Moderna stanno lavorando per applicare la blockchain alla distribuzione dei vaccini anti Covid-19. La crescente paura ed incertezza relativa alla sperimentazione crea, nella popolazione, una mancanza di fiducia e, di conseguenza, un tasso di rifiuto molto elevato [54].

La blockchain rappresenta la soluzione concreta per ridurre le incertezze e aumentare, sensibilmente, il tasso di adesione. L'obiettivo è coinvolgere la Pubblica Amministrazione per rendere il processo di distribuzione *trasparente* e, sopratutto, diffondere l'idea di attendibilità.

Alla base del funzionamento di tale tecnologia vi è un sistema *open-source*, cioè liberamente accessibile agli utenti, di tipo farmaceutico. In tal modo ci si attende di ottenere i seguenti vantaggi:

- tracciabilità end-to-end;
- riduzione dei rischi;
- garanzia di sicurezza ed efficacia.

I vaccini ad mRNA devono essere mantenuti ad una temperatura di, circa, 70°C sotto zero, per evitare reazioni chimiche e non intaccare la validità del vaccino. Questo richiede, quindi, una catena del freddo efficiente e priva di ritardi logistici. La rete logistica, però, è costituita da numerosi intermediari che potrebbero essere soggetti a malfunzionamenti dei macchinari e compromettere il corretto mantenimento del vaccino.

La prima grande innovazione risiede nella creazione di una *catena di approvvigionamento intelligente*, in modo da assicurare e rispettare l'obiettivo di tracciabilità end-to-end. In tal modo si assicura visibilità della distribuzione e dei punti di custodia in tempo reale [55]. Inoltre, sarebbe possibile gestire al meglio l'ultimo miglio, che è anche il più importante. Si eviterebbero problemi di pianificazione

della domanda, riuscendo in tempo reale a verificare la presenza delle dosi in un particolare centro di smistamento.

La pandemia, però, ha incrementato l'attenzione degli hacker verso le infrastrutture pubbliche e, quindi, diventa di vitale importanza salvaguardare le informazioni all'interno dei database governativi. Inoltre, come suggerito dalla National Security Agency (NSA) [56], è indispensabile implementare soluzioni informatiche che prevengano ogni possibilità di attacco esterno. Senza una protezione adeguata si rischierebbe di vanificare tutti gli investimenti fatti per la somministrazione del vaccino. La blockchain proposta da IBM riduce al minimo tale rischio, sfruttando la soluzione al problema dei generali bizantini, e permette di accedere, unicamente, ad informazioni verificate e veritiere.

L'obiettivo ricercato da IBM, con la blockchain, è di ottenere un'infrastruttura di rete alla quale possano interagire diversi attori della filiera, in modo da diffondere *sicurezza* e *fiducia*. Il rischio concreto è, infatti, che si diffonda l'idea che il vaccino sia poco efficace e poco sicuro. Il settore pubblico e privato cooperano per trasmettere informazione trasparente ed accessibile in ogni momento.

Infine, oltre ai grandi investimenti per rinforzare la logistica, è necessario creare un modo per collezionare i dati degli utenti e detenerli senza il rischio di, possibili, data breach. IBM ha introdotto *IBM Digital Health Pass*, un sistema, basato su blockchain, che permette di salvare i propri dati sanitari ed interfacciarsi con le aziende, in modo sicuro e senza correre rischi (Figura 5.3).

Figura 5.3: Interfaccia dell'app IBM [57].

Attraverso lo standard W3C, che garantisce l'attendibilità delle informazioni,

gli utenti possono condividere con le aziende le loro credenziali senza diffondere le informazioni personali. Il sistema è progettato per tre categorie di utilizzatori [58]:

- farmacie che possono rilasciare credenziali verificate, come ad esempio i risultati di un tampone, e trasmetterle all'applicazione;
- individui che utilizzano l'applicazione per certificare il proprio stato di salute;
- controllori che verificano la salute degli individui interfacciandosi alle singole applicazioni.

La rete creata è integrabile nei software delle diverse aziende e permette una migliore gestione dello stato pandemico. È progettata per garantire la sicurezza di tutti e diffondere l'idea di *assenza di rischio* nei posti visitati.

5.3 Implicazioni future

La letteratura analizzata suggerisce che la blockchain può essere considerata come una grande innovazione degli anni recenti. Sono stati effettuati degli investimenti, inizialmente in campo economico, da entità minori che, però, hanno rivoluzionato il modo di relazionarsi con il mondo. Il bitcoin, ad esempio, è un bene facilmente accessibile a chiunque voglia acquistarlo e racchiude le caratteristiche tipiche di un prodotto innovativo, basato su ricerca e sviluppo: gode dell'effetto rimpiazzo.

Nonostante sia difficile pensare che il bitcoin, così come qualsiasi altra criptovaluta, possa sostituire il sistema bancario tradizionale è utile pensare che questa moneta ha rivoluzionato il modo di concepire il sistema di transazioni tradizionale.

Alcuni cittadini, sopratutto dei Paesi dove l'inflazione è molto elevata (*iperinflazione*), utilizzano bitcoin come bene rifugio, per tutelare il proprio patrimonio. La Repubblica di El Salvador ha reso bitcoin una valuta a corso legale.

Dal punto di vista finanziario, con bitcoin e altre criptovalute, la blockchain sembra funzionare bene. L'obiettivo, attuale, delle aziende è applicarla, il più possibile, nelle loro organizzazioni perché ridurrebbe la necessità di burocrazia. Il vantaggio principale è da ricercarsi nella possibilità di accesso da ogni computer collegato alla rete:

- ogni membro potrebbe connettersi in sicurezza, senza rischio di essere intercettato;
- l'intera rete è criptata e le informazioni non sono accessibili dall'esterno;
- la blockchain può essere immaginata come un grande database che raccoglie informazioni che sono sempre accessibili in ogni momento.

Il libro "*Blockchain, Blueprint for a New Economy*" [59] suddivide la blockchain in tre fasi operative:

- Blockchain 1.0
- Blockchain 2.0
- Blockchain 3.0

Attualmente ci troviamo in una fase 2.0, nella quale solo poche persone hanno apprezzato la bontà dell'innovazione e la maggior parte la classifica, unicamente, con applicazioni di tipo finanziario. In tale fase, però, si inizia ad apprezzare la validità degli smart contracts e la loro applicazione al di fuori del contesto economico.

Rifacendosi al modello di Rogers, attualmente ci troviamo in una fase in cui solo alcune persone, identificabili con l'appellativo di *early adopters*, stanno usando la tecnologia e ne apprezzano l'utilità (Figura 5.4).

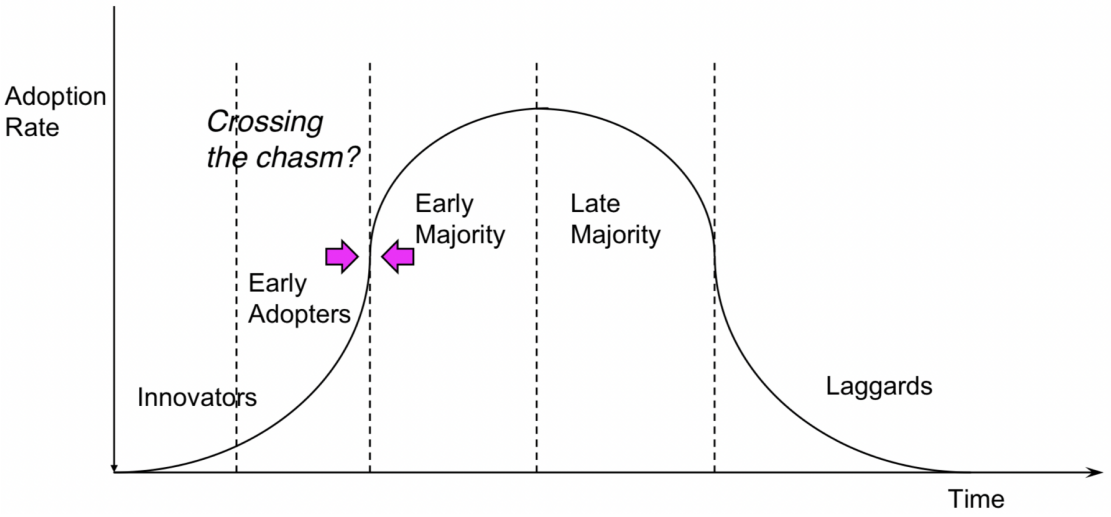

Figura 5.4: Modello di Rogers.

Tale modello suggerisce che è stata superata la fase caratterizzata dal "*bandwagon effect*", effetto dovuto alla contagiosità dell'innovazione, e ci si appresta all'utilizzo perché, realmente, pratica e funzionale. Nonostante ciò, però, ancora non si può parlare di paradigma dominante e il tutto è reso più evidente dalla diverse tipologie di blockchain disponibili sul mercato.

È necessario che gli investimenti, crescenti negli ultimi anni, siano effettuati da enti il cui scopo è il benessere dei cittadini. Il caso IBM, ad esempio, suggerisce che la blockchain in ambito sanitario può introdurre importanti novità e può ringiovanire

un sistema, ormai, obsoleto. L'ultima grande novità del settore sanitario risiede nella, mancata, implementazione del registro elettronico (Electronic Health Records). I sistemi sanitari mondiali, attraverso l'uso di un modello centralizzato, volevano digitalizzare i dati dei pazienti in modo da rendere più agevole, per il medico, la loro consultazione. Gli specialisti, però, hanno ritenuto il sistema poco funzionale e hanno preferito l'uso del sistema tradizionale.

Nel campo della sanità pubblica l'uso della blockchain è necessario e dovrebbe essere incentivato dagli Stati. Non solo perché donerebbe al paziente la centralità di cui ha bisogno ma, anche, perché ridurrebbe i costi derivanti dalla gestione degli ospedali e dei dati dei pazienti. Una ricerca condotta, nel 2016, da Credit Suisse [60] evidenzia che ospedali, compagnie di assicurazione e l'intera industria farmaceutica possano beneficiare di una riduzione dei costi implementando la blockchain (Figura 5.5). L'utilizzo di dati a livello anonimo, senza il rischio di ledere la privacy dei pazienti, potrebbe migliorare i processi interni degli ospedali e rivelare aree critiche, che rappresentano i colli di bottiglia dell'intero processo.

La pandemia ha accentuato il bisogno di avere una struttura decentralizzata, che permetta lo scambio di informazioni tra più organizzazioni in modo da gestire, contemporaneamente, un flusso di dati elevato. Questa necessità era stata ipotizzata, riferendosi ad una crisi pandemica, nel paper "Opportunities for Use of Blockchain Technology in Medicine" [46], evidenziando come le strutture pubbliche, nel 2018, fossero inadeguate a gestire un eventuale evento avverso.

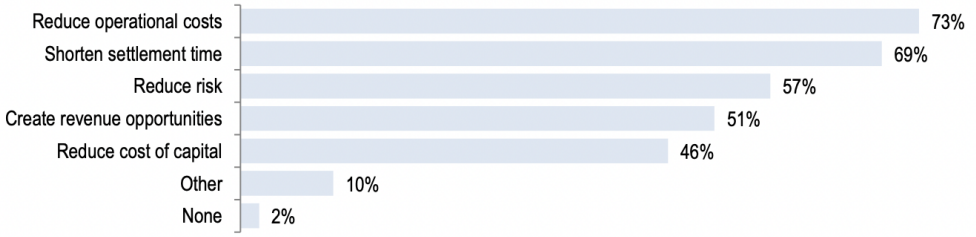

Figura 5.5: Maggiori benefici derivanti dall'implementazione blockchain [60].

Ciò che risulta evidente è che, sopratutto in ambito medico, è necessaria un'innovazione di tipo tecnologico. La blockchain rappresenta un nuovo punto di partenza su cui basare la restaurazione. I pazienti hanno bisogno di un sistema moderno, che garantisca loro efficenza e, sopratutto, protezione dei dati. È necessario che tali dati siano raccolti in maniera anonima per migliorare i processi e creare degli standard minimi di qualità a cui possano accedere tutti, indistintamente dal luogo o Paese di utilizzo. Qualora, invece, fosse necessario divulgare i dati dei pazienti, si potrebbe pensare ad un tipo di *economia chiusa*, come suggerito nel libro "*Radical*

Markets: Uprooting Capitalism and Democracy for a Just Society", nella quale i pazienti fissano il prezzo per la consultazione dei propri dati.

La blockchain, sicuramente, rappresenta uno dei mezzi più innovativi e alla portata per affrontare le sfide tecnologiche del presente e del futuro. È importante, però, evidenziare che non è l'unico mezzo che si potrebbe utilizzare e che, anche essa, ha dei punti di debolezza. Non è sempre applicabile e, in alcuni casi, non conviene neanche (Figura 5.6) . L'obiettivo della trattazione è evidenziare che il Sistema Sanitario Nazionale, e tutta la rete ad esso connessa, abbia bisogno di definire degli standard minimi di sicurezza nel trattamento dei dati dei pazienti. Standard che potrebbero essere necessari per trattare al meglio eventuali *patologie rare*.

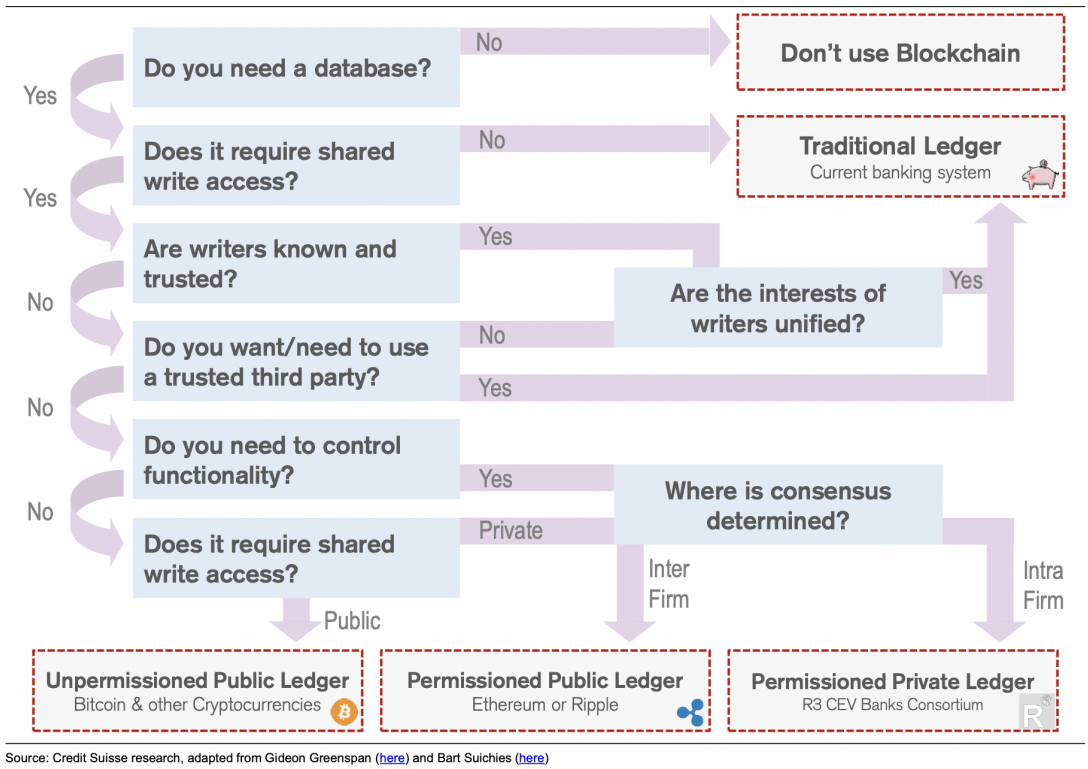

Figura 5.6: Quando conviene implementare blockchain [60].

Parte III

La blockchain applicata alla gestione delle malattie rare

Capitolo 6

I problemi comuni nelle malattie rare

Le malattie rare rappresentano delle condizioni che affliggono una bassa percentuale della popolazione mondiale. In questo capitolo si darà una definizione di malattia rara e si presenteranno i problemi caratteristici della diagnosi e gestione di una patologia rara.

Definire formalmente una malattia rara non è semplice. Ogni Stato classifica le patologie rare in modo diverso, creando delle eterogeneità di trattamento. Attualmente esistono 296 definizioni diverse in tutto il mondo. La differenza di trattamento tra Paesi diversi porta un paziente ad essere definito *raro* in una determinata località e *comune* in un'altra. In Europa, l'EMA (European Medicines Agency) considera rara una malattia che affligge meno di 1 persona su 2000. In America, invece, una patologia è considerata rara quando affligge meno di 200.000 persone nell'intero Paese.

Collettivamente, le malattie rare affliggono, circa, il 7 % dell'intera popolazione mondiale [61]. Gli USA sono stati i primi ad interessarsi al trattamento delle malattie rare, promulgando nel 1983 l'Orphan Drug Act (ODA) per promuovere lo sviluppo di terapie efficaci per il trattamento di queste patologie. Nello specifico, con questo atto, gli Stati Uniti incentivavano l'industria farmaceutica ad investire in farmaci sperimentali, garantendo un periodo di esclusività di 7 anni ed il tax credit. La stessa legge è stata replicata, in maniera simile, dall'Europa e dal Giappone e può essere considerata un successo: il numero di sperimentazioni è raddoppiato, passando da una media di 63 negli anni 90 ad una media di 126 per anno nel 2010-2011 (Figura 6.1).

In questa trattazione, data l'assenza di una definizione omogenea, verranno considerate rare le patologie con una prevalenza inferiore a 1 su 2000 persone (definizione Europea). Nonostante siano classificate come rare, in quanto lo sono se

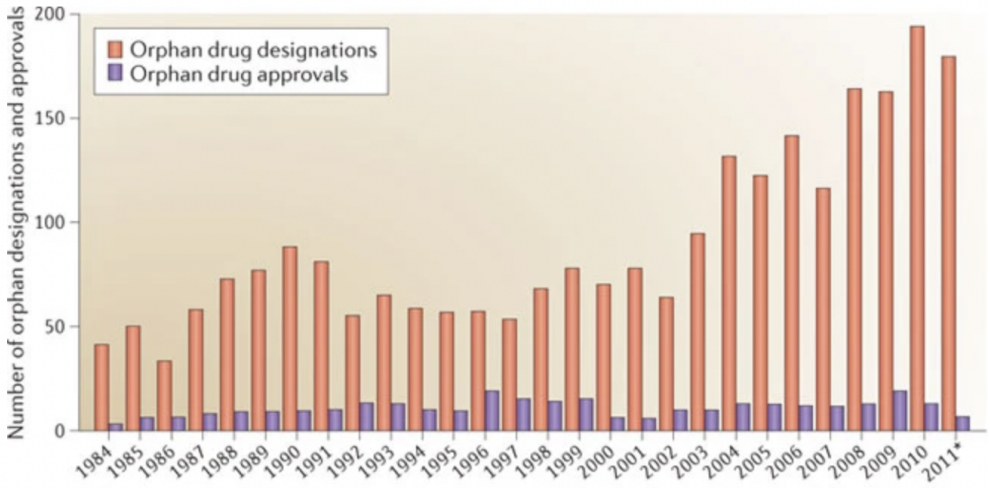

Figura 6.1: Numero di sperimentazioni tra gli anni 90 e il 2011 [61].

si considera la singola patologia, globalmente circa 450 milioni di persone sono affette da malattie rare nel mondo. Con il passare degli anni, è sempre più comune scovare nuove malattie rare ed attualmente l'Orphanet, sito web europeo che contiene informazioni su malattie e trattamenti, ne riconosce più di 6000. La tendenza a crescere di una popolazione di un Paese comporta una maggiore diffusione delle malattie rare, almeno teoricamente. Inoltre, se si valuta un singolo disordine è lecito pensare che questo nel tempo diventi sempre più comune, in termini di prevalenza, per due motivi:

- la diagnosi, con l'aiuto di nuove tecnologie, diventa più semplice;
- la scoperta di farmaci adatti permette di migliorare le aspettative di vita, aumentando il numero di persone affette che contemporaneamente vive in un Paese.

Uno studio tawainese stima che la prevalenza delle malattie rare aumenta di circa il 20 % ogni anno [62].

Un ostacolo comune, a tutte le malattie rare, è rappresentato dagli alti costi di ricerca e sviluppo di trattamenti efficaci. Solo negli Stati Uniti, in circa 10 anni, sono stati spesi più di 1 miliardo di dollari per produrre e promuovere trattamenti in grado di contrastare gli effetti portati dalle patologie rare. Inoltre, la scoperta di nuove patologie rare non aiuta a definire delle linee guida omogenee. Delle 6000 malattie rare identificate da Orphanet, solo 355 hanno delle terapie efficienti [63].

Per ridurre i costi di ricerca è stata proposta la creazione di centri nazionali che possano gestire al meglio le risorse e identificare meglio le patologie. Più in generale, la creazione di board nazionali per lo sviluppo di trattamenti terapeutici

potrebbe migliorare la produttività e creare beneficio per tutte le patologie. In tal modo, sarebbe più facile identificare malattie, classificate diversamente, simili tra loro.

I registri attuali, in Italia ad esempio, sono a carico dei centri specializzati o di associazioni e le strutture mediche non sono tenute a collaborare tra di loro. Lo stesso vale a livello internazionale. Nel 2013 è stata proposta una collaborazione internazionale tra i vari centri per migliorare la comunicazione e la diagnosi relativa alle malattie rare. L'obiettivo, da ricercare, è la creazione di un database condiviso che permetta di evitare la duplicazione di item e la ricerca di standard minimi definiti. Infatti, attualmente le malattie rare sono definite diversamente tra vari Paesi e, sopratutto, la differente prevalenza porta a diversificare gli investimenti in ricerca e sviluppo. Inoltre, visto che il trattamento dei dati dipende dal singolo centro, anche a livello nazionale il livello di dettaglio varia e, il più delle volte, non è possibile fare un confronto tra i vari dati.

In Italia, come detto in precedenza, i registri delle malattie rare non sono statali ma appartengono ai singoli centri o associazioni. Attualmente se ne contano 89, di cui 21 privati e, quindi, non facilmente consultabili. L'assenza di un'unica rete, per la singola malattia, porta a sovradimensionare il numero di affetti da una determinata patologia, rendendo, inoltre, difficile l'associazione di un paziente ad un centro specifico. Infatti, i centri registrano presso la propria struttura il paziente in ingresso e lo classificano come *malato raro* ma non registrano i suoi movimenti. Lo stesso paziente potrebbe recarsi presso un altro centro ed essere, nuovamente, registrato come in cura presso la struttura. In tal modo, un unico paziente è registrato in due centri diversi, creando una duplicazione, inutile e dispendiosa, del dato.

6.1 Il problema degli standard

L'assenza di standard rappresenta, sicuramente, il più grande problema nella gestione di una malattia rara. È difficile parlare di standard se non esiste neanche una definizione univoca tra gli Stati.

Per quanto riguarda le malattie rare, l'assenza di standard è da ricercarsi nell'assenza di cooperazione a livello internazionale. Bisognerebbe puntare ad una standardizzazione della nomenclatura, che è possibile, e non ad una standardizzazione dell'intero processo.

Per attuare un sistema di questa portata, gli Stati dovrebbero dedicare delle risorse, monetarie e non, per permettere uno scambio facile di informazioni tra i vari centri. Attualmente, infatti, non esiste un canale ufficiale di scambio di informazioni tra i singoli centri e i singoli Stati, ma sono i medici, volontariamente, che collaborano tra loro nella ricerca di soluzioni efficaci. Un'iniziativa del genere

permetterebbe l'eliminazione di voci duplicate e una maggiore facilità ad interfacciarsi con malattie, dal nome diverso, non troppo diverse. Solo a titolo d'esempio, l'uveite e l'artrite reumatoide, nei loro casi più gravi, sono curate entrambe con il farmaco biologico Adalimumab, pur essendo due patologie totalmente diverse.

Inoltre, l'utilizzo di un sistema contenente dati aggiornati di una stessa malattia darebbe valore al singolo dato. Un dato, da solo, ha poco valore, ma in combinazione con altri dati simili acquisisce un potenziale elevato. Poter disporre di una struttura, di cui tutti verificano il contenuto, potrebbe permettere di fare associazioni complesse e non banali. Ad esempio, si potrebbero associare le cure di malattie totalmente diverse, come nel caso di uveite ed artrite reumatoide, con più facilità e destinare la ricerca verso nuove sperimentazioni. La condivisione dei dati rappresenterebbe, in tal senso, il metodo migliore per generare valore sia per i pazienti che per i medici.

La condivisione dei dati, inoltre, permetterebbe di evitare duplicazione di dati e permetterebbe di creare un processo diagnostico più veloce. Un approccio di questo tipo, basato sull'associazione dei sintomi, darebbe valore non solo al trattamento di una patologia rara, ma permetterebbe di ridurre il costo della ricerca per le patologie definite *ultra rare*. È necessario, però, capire cosa vogliono i pazienti per assicurare che condividano le informazioni e permettere il fluire della ricerca [64]. Inoltre, bisogna assicurare che i dati siano trattati in maniera sicura per ottenere la fiducia del paziente. Il rispetto e il trattamento dei dati, di un paziente raro, è ancora più importante in quanto è più probabile risalire all'identità del paziente nel caso in cui condividesse le informazioni, data la bassa numerosità della popolazione di riferimento.

Un problema fondamentale è l'assenza di *cultura* nella condivisione dei dati: raccogliere i dati, senza aver delineato uno scopo preciso, è dispendioso e non sarebbe utile alla causa. Inoltre, la condivisione dei dati richiede compatibilità tra i vari sistemi. Le reti dei vari centri dovrebbero concordare sul modello di riferimento [65].

Includere i pazienti nella creazione di un modello, basato sulla condivisione dei dati, permetterebbe di avere una rete flessibile ed, al tempo stesso, di alto valore. Ottenere il consenso del paziente è il modo migliore per creare un sistema condiviso, in quanto non si avrebbero problemi di fiducia ed inoltre ci sarebbe l'interesse reciproco, di medici e pazienti, di migliorare l'intera rete.

L'investimento in nuovi macchinari e tecnologie è necessario per migliorare il processo diagnostico. Uno studio condotto presso l'Arcispedale Santa Maria Nuova (RE), ad esempio, mostra come la disponibilità di nuovi test e l'approccio interdisciplinare tra più medici renda la diagnosi di uveite più semplice. Nel caso di alcune malattie rare non è sempre possibile diagnosticare con precisione la malattia, quindi diventa necessario investire in tecnologie di precisione e promuovere la cooperazione tra branche mediche diverse. Nella malattia di Behçet (BD), ad

esempio come sarà discusso in seguito, la diagnosi non può essere confermata ma può, al massimo, essere altamente probabile. In questi casi è necessario assicurare al paziente che possa entrare in contatto con una rete di medici, con approccio interdisciplinare, e, al tempo stesso, il paziente deve contribuire alla ricerca condividendo i suoi dati.

6.2 Il rispetto della privacy e il problema della qualità

Le malattie rare, come detto, sono patologie che affliggono poche persone. Nella totalità, però, riguardano il 7 % della popolazione mondiale. I dati a disposizione non sono molti ed è necessario sfruttarli al meglio per determinare nuovi trattamenti ed aspetti comuni tra diversi disordini rari. È fondamentale che si lavori, a livello europeo, nella creazione di standard comuni per la raccolta e l'elaborazione dei dati, in modo da determinare aspetti statisticamente significativi. Le ricerche attuali puntano a studiare il genotipo delle malattie, per determinare risposte comuni a disordini diversi. Esse, però, il più delle volte non conducono a risultati soddisfacenti, principalmente, perché il campione di riferimento è limitato [66].

Nel contesto delle malattie rare il problema della protezione della privacy risulta molto complesso. La bassa incidenza, che comporta una più facile identificazione del paziente, obbliga gli specialisti a trattare i dati con estrema cautela. Proprio per questo è stato lanciato un progetto pilota che punta a creare un registro globale (GRDR) del tutto anonimizzato, in modo da aggregare i dati da più Paesi ed effettuare ricerche su un campione di dati maggiore. Tale progetto nasce dall'evidenza che nel modello attuale c'è il rischio concreto di identificazione dell'identità del paziente, definita "re-identification", nello scambio di dati tra istituti diversi [66]. Per attuare un modello del genere è necessario che i dati in materia di privacy siano trattati ugualmente dai centri aderenti e, sopratutto, che sia garantita l'anonimizzazione del dato.

In questo modo, oltre ad ottenere la fiducia del paziente che è necessaria vista la bassa incidenza, si riuscirebbe a gestire meglio le risorse sia economiche che materiali. Nello specifico, i medici lavorerebbero su un campione di dati più grande e sarebbe possibile ottenere, più facilmente, delle evidenze statistiche derivanti dalle ricerche. Inoltre, le ricerche congiunte, effettuate per mezzo di team dedicati, eviterebbero i lavori di singoli centri basati su pochi dati. Infine, sarebbero da valutare anche i cross-side effect che si genererebbero con un registro unico. L'associazione, attraverso il genotipo, di malattie diverse sarebbe più facile e potrebbe portare ad identificare dei marcatori comuni.

I pazienti rari mostrano una grande propensione a condividere i loro dati personali, sopratutto se questi possano favorire la ricerca e determinare nuove

terapie. Al tempo stesso, richiedono che i loro dati siano trattati in modo anonimo, senza che si possano verificare episodi di discriminazione e re-identification.

Attualmente, la privacy è descritta dai ricercatori come "il problema", la barriera più grande nella ricerca e nella scoperta di nuovi trattamenti [67]. Più in generale, è difficile determinare se è meglio avere "libertà di ricerca", con risultati possibilmente migliori, o puntare alla protezione dei dati dei partecipanti. Questo è un dilemma che affrontano i medici, in quanto la privacy è un diritto del paziente ma essa non è assoluta e deve essere valutata a seconda dei casi.

La convenzione di Oviedo, firmata il 4 aprile 1997, stabilisce che ogni persona ha il diritto di essere a conoscenza di tutte le informazioni mediche, riguardanti se stesso, che sono stare raccolte. Inoltre, stabilisce all'articolo 5 che "gli interventi medici possono essere effettuati solo con il consenso informato del soggetto, che può essere revocato in qualunque momento" [68]. Per alcuni specialisti questa restrizione va contro i principi di qualità e, se applicata rigorosamente, rappresenterebbe un ostacolo alla fornitura di servizi di qualità. Risulta difficile bilanciare il diritto alla privacy con il dovere a fornire prestazioni di qualità, essendo questa una condizione necessaria per prevenire danni fisici alla persona. Inoltre, i medici rivendicano la *libertà di ricerca*, così come espressa all'articolo 12 del trattato, come necessaria per portare avanti la ricerca, garantire equità di trattamento e con il "dovere di alleviare la sofferenza e migliorare la salute del paziente".

Per ottenere conclusioni significative è necessario che i dati siano aggregati tra di loro e che siano aggiornati. L'approccio odierno, basato sulla comunicazione di registri diversi, ha la grave problematica di non essere esente dalla re-identification, alla quale si preferisce la fornitura di prestazioni di alta qualità. L'utilizzo dei dati risulta necessario, anche se si presenta il problema della qualità in contrapposizione alla privacy. Più in generale, i dati aggregati comportano innumerevoli benefici, tra cui la possibilità di predire cambiamenti nella malattia e la capacità di determinare l'efficacia dei trattamenti, in modo da indirizzare correttamente gli investimenti verso terapie specifiche [66]. Un esempio che evidenzia la presenza del conflitto tra l'alta qualità del trattamento e il rispetto della privacy del dato è rappresentato dalla sviluppo del vaccino contro l'infezione da papilloma virus umano (HPV). Lo sviluppo del vaccino è stato possibile grazie alla presenza di dati accumulati nel tempo, in quanto il virus attacca diversi decenni dopo l'infezione. Di contro, nonostante la grande scoperta permetta di salvare migliaia di vite ogni anno, non è stata garantita l'anonimizzazione dei dati e l'assenza di re-identification [69].

Il paradosso portato avanti dalla letteratura attuale riguarda la divisione tra qualità e privacy. I maggiori specialisti dichiarano che è necessario offrire trattamenti di qualità, che possano creare delle condizioni di vita migliori, come espresso nell'articolo 3 della Convenzione, anche a danno della privacy. Infatti, se si giudicasse alla lettera la normativa molti database dovrebbero essere eliminati, con conseguenti danni per la ricerca futura. È necessario, d'ora in avanti, interrogarsi e

determinare quanto sia profonda la divisione tra la giusta qualità e la privacy e se possa esistere un modello che le abiliti entrambe.

6.3 Il caso studio Behçet

In questo paragrafo si presenta la malattia rara Behçet, evidenziando i problemi, tipici, nella diagnosi della patologia. Questa trattazione è necessaria per introdurre nel paragrafo successivo il tema dell'importanza dei dati, della loro protezione e di politiche d'intervento nella gestione di una malattia rara.

La malattia di Behçet è una vasculite multisistemica di origine eziologica sconosciuta, caratterizzata prevalentemente da afte orali e genitali, manifestazioni oculari e lesioni della pelle [70].

BD è più comune nei Paesi della via della seta, con prevalenza maggiore nel sud dell'Europa, in Turchia e in Giappone. La correlazione con il territorio in cui si abita non è ancora confermata, ma si pensa sia dovuta ad una maggiore distribuzione del gene HLA-B51 nei territori sopra citati. In Tabella 6.1 vengono schematizzati i risultati derivanti da uno studio condotto su pazienti affetti da BD. Le persone positive al gene HLA-B51 hanno una probabilità 6 volte maggiore di avere la malattia rispetto a chi risulta negativo al gene (odds ratio). Al tempo stesso, la presenza del gene non può essere considerata altamente significativa, in quanto circa il 20 % della popolazione italiana è positiva.

	Healthy Controls	BD	P	Odds Ratio
HLA-B51	19,2 %	57,4 %	0,0001	5,7

Tabella 6.1: Incidenza della presenza del gene HLA-B51 derivante da un test del chi-quadrato condotto tra soggetti sani (Healthy controls) e malati (BD), con intervallo di confidenza del 95 % e p-value=0,0001 [71].

Nonostante non si siano trovate delle correlazioni tra il luogo in cui si vive e la probabilità di sviluppare la malattia, uno studio ha dimostrato che la prevalenza della malattia per un turco che vive in Germania è nettamente più alta di un nativo tedesco, ma più bassa di un turco che abita in Turchia.

La malattia si verifica con una frequenza simile in uomini e donne [72] e presenta le maggiori complicanze, se non diagnosticate per tempo, intorno al 30-esimo anno d'età. La diagnosi precoce diventa, quindi, necessaria per evitare le complicanze della malattia. I criteri internazionali per l'identificazione della malattia, che per non appesantire la trattazione verranno riportati in Tabella 6.2, presentano dei problemi di sensibilità, in quanto identificano nelle afte orali il primo fenomeno della malattia, senza il quale non è possibile effettuare una diagnosi. Numerosi studi, al contrario, evidenziano che le afte orali non sono il primo sintomo della malattia

ma vengono sviluppate solamente in seguito e, di conseguenza, non è possibile effettuare una diagnosi precoce. Si riporta un'immagine, derivante dallo studio condotto dall'Arcispedale Santa Maria Nuova di Reggio Emilia, che testimonia che all'inizio della malattia, il 23 % dei pazienti non soddisfa i criteri minimi necessari, secondo la definizione attuale, per avere una diagnosi di BD (Figura 6.2).

afte orali ricorrenti	almeno 3 volte all'anno
più due dei seguenti	
ulcere genitali	ricorrenti
lesioni oculari	uveiti anteriori o posteriori, panuveiti
lesioni della pelle	eritema nodoso, follicolite o vasculite retinica
pathergy test	positivo

Tabella 6.2: Criteri internazionali BD.

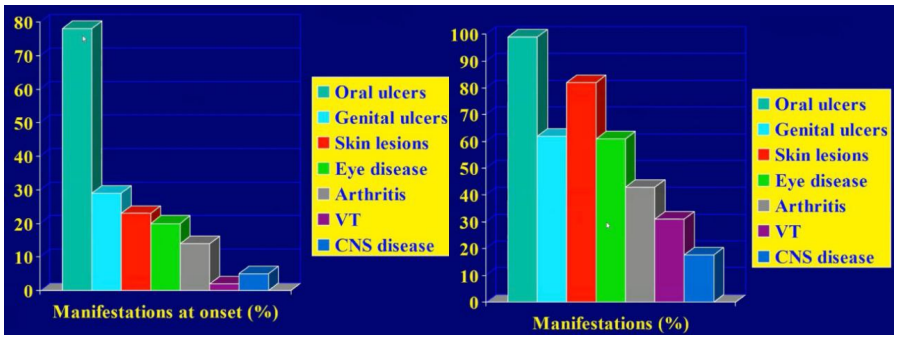

Figura 6.2: Evidenze contro la definizione generale per la diagnosi di BD [73].

Per migliorare la sensibilità, sono stati introdotti dal 2013 nuovi criteri che permettono di fare una diagnosi precoce della malattia, in modo da evitare i picchi sintomatologici riscontrati intorno al 30-esimo anno d'età. I criteri suggeriti utilizzano un sistema a punti, permettendo una diagnosi precoce se il paziente raggiunge un punteggio di almeno 4 (Tabella 6.3).

La nuova definizione permette di intercettare i pazienti con sintomi iniziali e poter definire, al meglio, un processo di cura e gestione. Risulta evidente che lo standard internazionale, utilizzato per una diagnosi precisa, è poco efficace ed è necessario, per evitare complicanze future, intervenire in anticipo.

È necessario, inoltre, che i pazienti si rendano disponibili nella condivisione dei loro dati, in modo da trovare evidenze che permettano dei miglioramenti della terapia o nuove scoperte. È, altresì, importante includere il paziente nei processi di cambiamento, in modo da assicurarsi la sua fiducia e la disponibilità, costante, di nuove informazioni, come ad esempio nuovi sintomi.

afte orali	2 punti
afte genitali	2 punti
lesioni oculari	2 punti
lesioni della pelle	1 punto
coinvolgimento neurologico	1 punto
lesioni vasculari	1 punto
pathergy test	1 punto (opzionale)

Tabella 6.3: Formulazione a punti per la diagnosi di BD.

6.3.1 Metodologia

Il presente lavoro, condotto dall'autore, è stato sottoposto a pazienti affetti da Behçet nel periodo da Luglio ad Agosto 2021. Il lavoro si pone l'obiettivo di capire quali siano le opinioni e i pensieri dei pazienti, affetti da BD, riguardo la condivisione dei loro dati e la privacy delle loro informazioni, in modo da trovare delle evidenze che suggeriscano l'implementazione di una rete blockchain per la gestione delle malattie rare.

Il questionario è stato sottoposto attraverso il sito web dell'associazione italiana sindrome, malattia di Behçet e Behçet Like (SIMBA) in lingua italiana. Essendo in Italia alcuni dei centri che hanno proposto il cambio di standard per la diagnosi della patologia, non è stata fatta alcuna discriminazione d'età permettendo a tutti coloro che entrassero in contatto con il sito di poter compilare l'indagine.

Il questionario è stato sottoposto, idealmente, a tutta la popolazione Behçet italiana ed ha ottenuto un numero di risposte pari a 101, con un tasso di completamento del 56 %. L'incidenza in Italia è di 2,4 casi ogni milione di abitante.

Il questionario è stato condotto, prevalentemente, utilizzando scale del differenziale semantico a 5 punti, a cui estremi sono indicati due aggettivi bipolari riferiti all'attributo valutato. È stata scelta una scala con categorie dispari in modo da consentire una *via di fuga* nel caso in cui il compilatore non avesse una chiara idea sull'attributo da valutare. Il questionario si compone di 7 sezioni, volte a comprendere:

- La distribuzione della malattia in Italia;
- La decisione di condividere le informazioni personali;
- L'importanza di ogni informazione personale condivisa;
- Quando il paziente è disposto a condividere le informazioni personali;
- Quali siano le caratteristiche più importanti nella gestione di una malattia rara per un paziente;

- Quanto il paziente si senta sicuro nel condividere le proprie informazioni con diversi enti;
- Lo stato di fiducia rispetto a reti informatiche.

Unicamente nella prima sezione è stato effettuato un lavoro di pulizia, in quanto alcune risposte alla domanda "in quale regione sei attualmente in cura" riportavano il nome della struttura ospedaliera o il nome di una città. Nessuna risposta è stata esclusa.

6.3.2 Risultati

La quasi totalità dei rispondenti (86 %) ha più di 30 anni d'età (Figura 6.3). Questo valore è in linea con la letteratura attuale che stima che, in accordo alla definizione standard, i maggiori sintomi si riscontrano intorno ai 30 anni d'età.

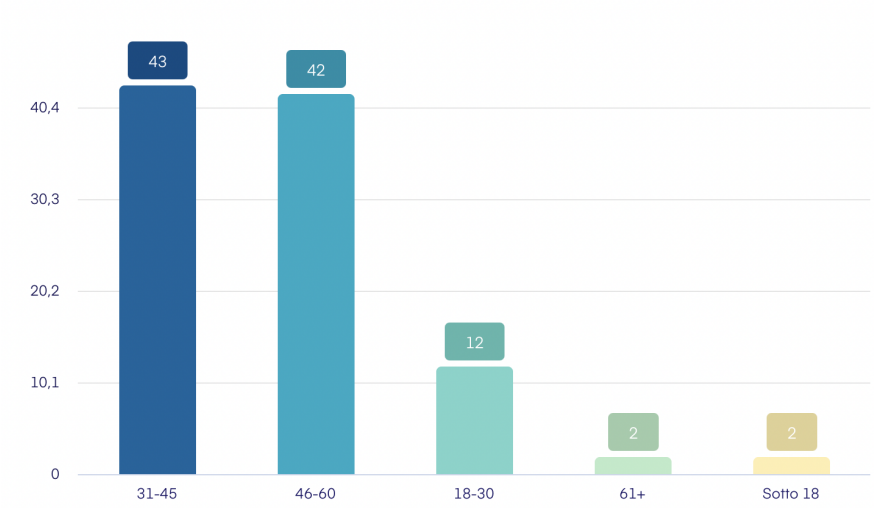

Figura 6.3: Distribuzione dell'età dei rispondenti.

Il 49 % dei rispondenti è in cura presso un centro specializzato delle regioni Emilia Romagna, Lombardia o Toscana, nonostante la distribuzione delle residenze sia più o meno omogenea. Infatti, il 38,6 % ha residenza al Nord Italia, il 30,7 % al centro Italia e il 30,7 % al Sud. Nella categoria "altro", accorpata successivamente al Sud Italia, alcuni rispondenti hanno indicato la loro città di residenza nel Sud Italia (Figura 6.4).

Il 97 % dei soggetti afferma di avere una diagnosi di BD, contro il 3 % che sospetta di averla ma non ha una diagnosi ufficiale (Tabella 6.4). Pochi centri, in Italia, utilizzano la nuova definizione per diagnosticare BD, quindi l'incertezza dei pazienti potrebbe essere dovuta all'assenza di contatto con specialista che utilizza

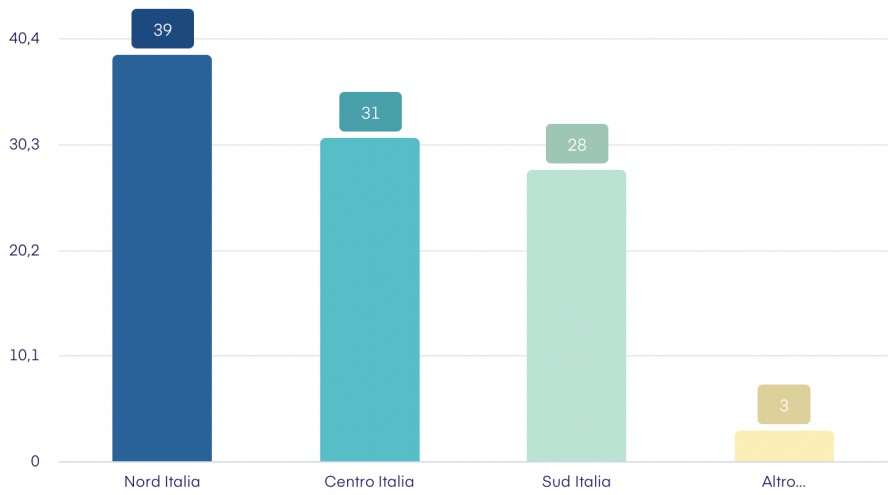

Figura 6.4: Distribuzione del luogo di residenza dei rispondenti.

il metodo a punti. Si ricorda che la definizione standard riconosce come primo sintomo la presenza di afte orali e questa è una condizione necessaria per la diagnosi.

(n=101)	Risposte	% di risposte
si	98	97 %
no	3	3 %

Tabella 6.4: Sei affetto dalla sindrome di Behçet?

Ai rispondenti è stato chiesto quando sarebbero stati disponibili a condividere i loro dati personali (Figura 6.5). Emerge una forte propensione a condividere i propri dati personali, sopratutto se la condivisione incrementa il benessere sociale in campo medico. Nello specifico, i pazienti sono fortemente disponibili a condividere le loro informazioni personali se queste possono migliorare le cure per la BD (96 %) e migliorare la ricerca in generale (98 %). Gli uomini mostrano, rispetto a queste domande, una propensione maggiore delle donne a condividere i loro dati personali. Infatti, il 95 % degli uomini è fortemente d'accordo a condividere i dati personali per migliorare la ricerca, contro l'80 % delle donne. I soggetti con età compresa tra i 46 e i 60 anni sono i più disponibili a condividere i dati per migliorare la cura della patologia, con un grado di accordo complessivo del 100 %. Per quanto riguarda la ricerca, invece, si registra che la fascia di soggetti tra i 31 e i 45 anni è altamente propensa a condividere i propri dati, con un tasso d'accordo del 98 %. Tale dato va contro la letteratura analizzata, che indica che i giovani, sopratutto universitari, siano i più propensi a condividere i propri dati ai fini della ricerca. È

utile, però, ricordare che i maggiori sintomi della malattia compaiano dai 30 anni in su, quindi la differenza riscontrata potrebbe essere dovuta a questo fattore.

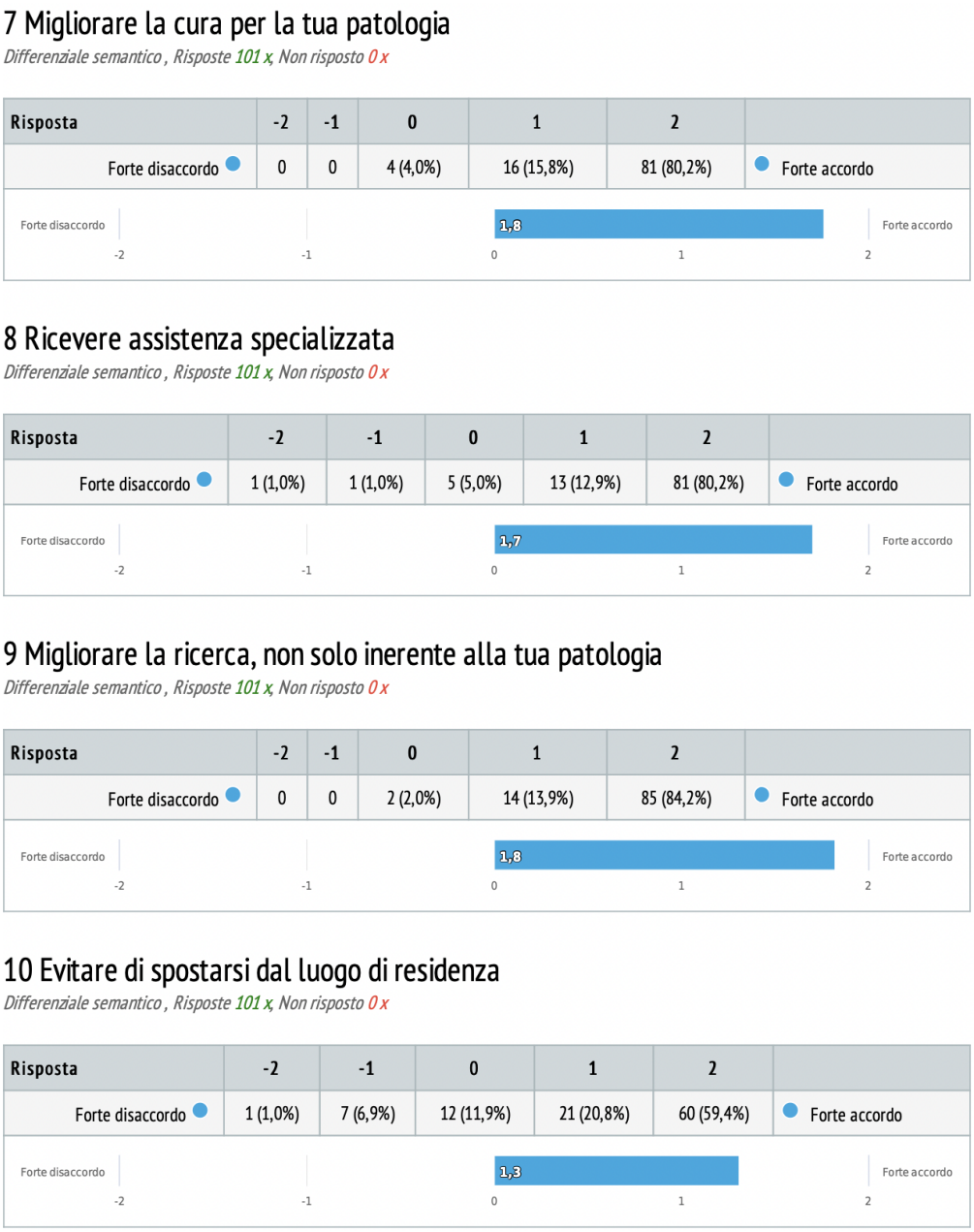

Figura 6.5: Ti chiedo di decidere in quali occasioni saresti disposto a condividere le tue informazioni personali?

Emerge che i pazienti affetti da BD sono disponibili a condividere le proprie

informazioni personali, se queste possano essere utili a comprendere meglio la malattia (94 %) (Figura 6.6) , ricevere assistenza specializzata (93 %) o evitare di spostarsi dal luogo di residenza (80 %). Come evidenziato in precedenza, infatti, 3 regioni in Italia registrano la maggior affluenza di pazienti nonostante, in totale, ci siano 86 centri abilitati. Riguardo quest'ultimo punto, risulta essere più rilevante per gli uomini che lo considerano essenziale (85 %) rispetto alle donne, che esprimono una propensione a condividere i loro dati per evitare di spostarsi dal luogo di residenza di poco superiore al 50 %. I soggetti tra i 31 e i 45 anni sono gli unici che nella loro totalità, con un tasso del 100 %, sono disponibili a condividere le loro informazioni per comprendere meglio la malattia. La comparsa dei sintomi più gravi al 30-esimo anno d'età potrebbe giustificare la necessità della fascia 31-45 di ottenere maggiori informazioni sul proprio stato di salute e, quindi, sulla malattia.

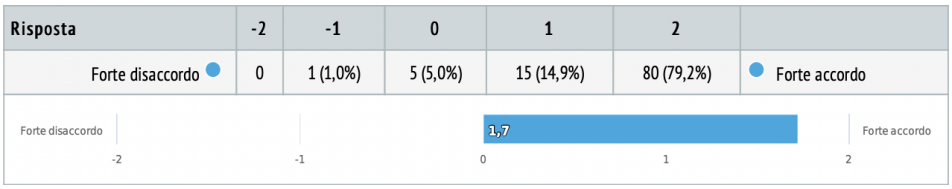

Figura 6.6: Condivisione delle proprie informazioni personali per comprendere meglio la malattia.

Una grande maggioranza dei votanti (80 %) è favorevole a condividere i propri dati per migliorare la ricerca non a scopo medico (Figura 6.7). Gli uomini sono più disponibili (75 %) a condividere le loro informazioni per migliorare la ricerca non a scopo medico, rispetto alle donne (50 %). La fascia di utenti tra i 18 e i 30 anni rappresenta la categoria più propensa a condividere i propri dati personali per migliorare la ricerca con finalità non medica. Questo dato è in linea con la letteratura analizzata nei capitoli precedenti, nei quali si dava evidenza che i ragazzi sono più disponibili a fornire i propri dati personali, anche se non direttamente correlati con il campo d'interesse indagato.

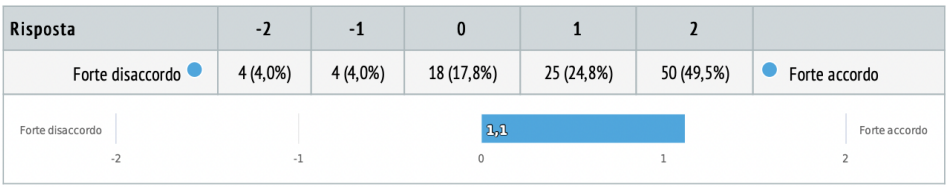

Figura 6.7: Condivisione delle proprie informazioni personali per migliorare la ricerca, non con finalità medica.

Successivamente, è stato chiesto ai rispondenti quanto pensassero che le informazioni condivise fossero sensibili. Condividere di essere affetto da una malattia rara

ed indicare il suo nome da molti non è considerata un'informazione sensibile (44 %), mentre altri (10 %) preferiscono non esprimere una posizione netta (Figura 6.8). Non risultano differenze nelle risposte di uomini e donne: entrambi, con le stesse percentuali, condividono l'idea che il nome della malattia sia un'informazione poco sensibile. I rispondenti con età compresa tra i 46 e i 60 anni, a differenza delle altre categorie, ritengono anche la condivisione del nome della malattia un'informazione sensibile (60 %).

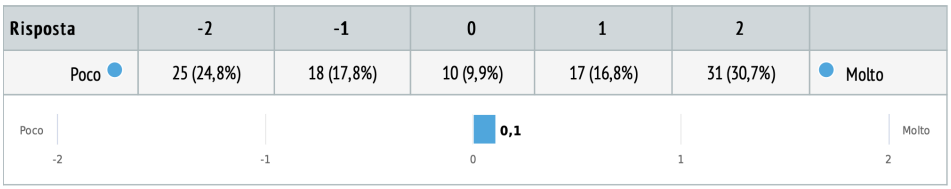

Figura 6.8: Quanto la condivisione del nome della malattia è considerata sensibile.

A differenza della precedente domanda, quando si richiede al paziente di condividere informazioni sulla sua patologia la sensibilità del dato varia (Figura 6.9). Infatti, anche se nella totalità dei voti non è considerata molto sensibile, i rispondenti considerano più sensibile tale tipo di dato rispetto al precedente. Come analizzato in precedenza, anche in questo caso non emergono differenze tra le risposte di uomini e donne. La fascia di rispondenti con età compresa tra i 46 e i 60 anni considera la condivisione dei sintomi come un'informazione altamente sensibile (70 %), a differenza delle altre fasce d'età che la considerano un'informazione sensibile ma non troppo.

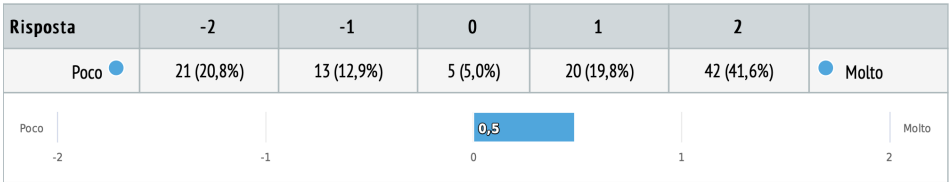

Figura 6.9: Quanto la condivisione dei sintomi della malattia è considerata sensibile.

Il centro di riferimento in cui si è seguiti non è considerata un'informazione troppo sensibile (49 %) ed è quella che ha totalizzato il punteggio minore, insieme al nome della malattia, nella scala del differenziale semantico (0,1).

Le informazioni circa il proprio stato di salute, come analisi del sangue (56 %), caratteristiche fisiche (51 %) e disabilità (56 %), risultano sensibili (Figura 6.10). Nello specifico, differenziando tra molto sensibile e sensibile nella scala semantica, la condivisione dei sintomi della patologia risulta essere l'informazione più sensibile per

i pazienti (42 %). Questo è, in parte, dovuto alla mole di informazioni da condividere quando si parla dei sintomi, riconducendosi alle informazioni genetiche del paziente. Emergono, inoltre, delle differenze tra le risposte di uomini e donne. Gli uomini, nella quasi totalità delle risposte (85 %) non considerano le caratteristiche fisiche come un'informazione sensibile da condividere, a differenza delle donne che la considerano sensibile (60 %). Analizzando le diverse fasce d'età non emergono differenze nelle risposte.

Figura 6.10: Se ti fosse chiesto di condividere le tue informazioni personali, quanto pensi che ognuna di queste sia sensibile?

Ai rispondenti è stato chiesto quando sarebbero disponibili a condividere le loro informazioni personali, scegliendo 3 opzioni tra una lista di 9 alternative (Figura 6.11).

18 Dovendo scegliere, tra le seguenti, solo tre alternative, per quali saresti disposto a condividere le tue informazioni sanitarie?

Scelta multipla , Risposte 101 x, Non risposto 0 x

Risposta	Risposte	Rapporto
Essere sicuro che siano condivise in modo sicuro	36	35,6%
Comprendere meglio la malattia	47	46,5%
Possibilità di confrontarsi con i medici	38	37,6%
Possibilità di essere a contatto con una rete di specialisti, anche da remoto	54	53,5%
Essere avvisato se le tue informazioni sono usate	12	11,9%
Essere informato sui miglioramenti della terapia	36	35,6%
Essere informato sul progresso della ricerca, in generale	28	27,7%
Non sei disposto, in ogni caso, a cedere i tuoi dati	3	3,0%
Non so	4	4,0%

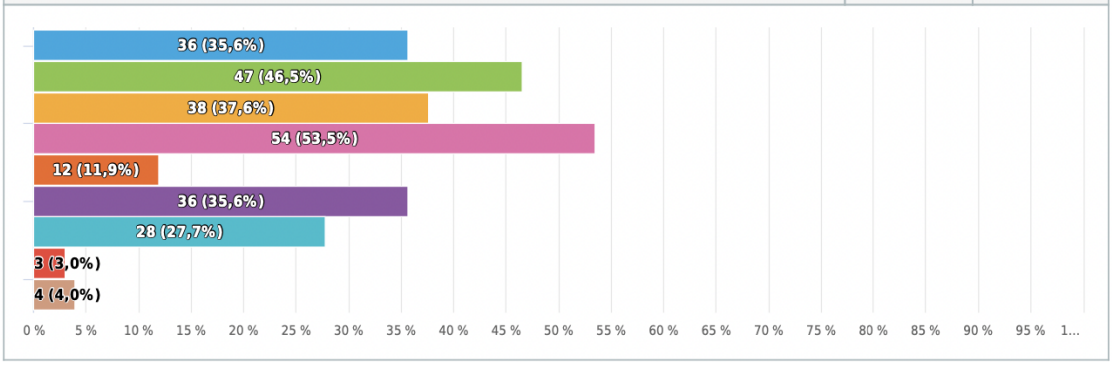

Figura 6.11: Dovendo scegliere, tra le seguenti, solo tre alternative, per quali saresti disposto a condividere le tue informazioni sanitarie?

Le alternative che permettono di comprendere meglio la malattia o di essere in contatto e confrontarsi con i medici sono quelle che hanno ottenuto più voti. Il 54 % condividerebbe le proprie informazioni se potesse essere in contatto, anche da remoto, con una rete di specialisti, il 47 % per comprendere meglio la malattia e il 38 % per potersi confrontare, liberamente, con i medici. Le considerazioni di uomini e donne sono uguali sulle prime due alternative, ma differiscono sull'ultima. Gli uomini sarebbero più disponibili a condividere le loro informazioni personali

per favorire il progresso della ricerca. I soggetti appartenenti alla fascia d'età 18-30, a differenza degli altri gruppi, non ritengono la comprensione della malattia una caratteristica fondamentale ma preferiscono essere informati sui miglioramenti della terapia.

Al contrario, anche se il Sistema sanitario italiano non lo permette, il 3 % non condividerebbe mai i propri dati personali. Inoltre, il 36 % sarebbe disponibile a condividere le proprie informazioni personali a condizione che queste siano trattate in modo sicuro e in rispetto delle normative vigenti in tema di privacy e protezione dei dati (GDPR). La categoria più interessata al tema della condivisione dei dati in modo sicuro è quella che comprende i soggetti tra i 31 e i 45 anni d'età. Inoltre, è l'unica categoria che inserisce questa opzione nelle prime tre alternative.

Una minoranza, il 12 % dei rispondenti, condividerebbe le proprie informazioni con il vincolo di essere avvisato se esse fossero usate in qualche progetto di ricerca. In pochi, il 4 %, non ha una chiara idea di quando condividerebbe le proprie informazioni sanitarie.

Successivamente, sulla base della domanda precedente, è stato chiesto ai rispondenti di classificare 5 opzioni riguardanti la cessione dei propri dati personali, con il punteggio 5 che rappresenta il massimo valore e il punteggio 1 il minimo (Figura 6.12).

Emerge che, quasi, la totalità dei pazienti condividerebbe i propri dati personali per entrare facilmente in contatto con i migliori specialisti (importanza di 4,3) e questo è in linea con la domanda precedente nella quale si chiedeva di scegliere, unicamente, 3 alternative. La possibilità di comunicare facilmente con gli specialisti ha ottenuto un'importanza più elevata di un possibile miglioramento della terapia (importanza di 3,6). Essere in contatto costante con una rete di medici è, dunque, una necessità di cui hanno bisogno i pazienti. Al contrario, l'opzione meno convincente sembra essere lo snellimento delle pratiche burocratiche (importanza di 1,6). Riguardo l'ultimo punto, nonostante in precedenza gli uomini avessero valutato come essenziale la possibilità di non spostarsi dal luogo di residenza, con un tasso d'accordo dell'85 %, tutti hanno assegnato l'importanza più bassa allo snellimento delle pratiche burocratiche. Le due valutazioni risultano in contrasto, in quanto, attualmente, è necessario portare i risultati delle visite precedenti ad ogni visita di tipo specialistico. Non risultano differenze di valutazione tra le diverse fasce d'età.

È stato chiesto ai pazienti quanto, in base alla loro esperienza, si sentissero sicuri della condivisione dei loro informazioni personali con diversi enti. Nello specifico, la stragrande maggioranza dei pazienti si sente molto sicura a condividere le proprie informazioni con lo specialista (74 %). La, quasi, totalità dei partecipanti condividerebbe le informazioni con lo specialista senza timore (91 %). Risulta essere il valore più alto totalizzato nell'intero questionario, con un valore di 1,6 nella scala del differenziale semantico (Figura 6.13). Le donne esprimono una diffidenza maggiore degli uomini. Infatti, il 10 % delle donne ha espresso un voto d'incertezza

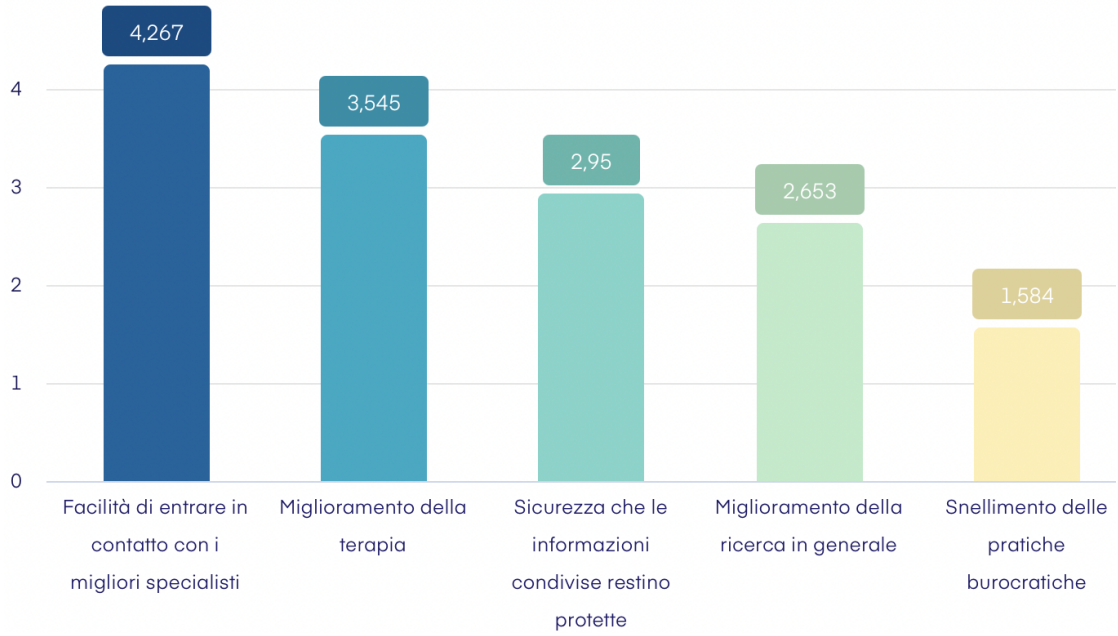

Figura 6.12: Quando saresti disposto a condividere i tuoi dati personali? Ti chiedo di classificare le seguenti 5 voci.

o negativo, a differenza della totalità degli uomini che non hanno alcun timore nel condividere i dati con lo specialista. I rispondenti appartenenti alla fascia 18-30 si sentono molto sicuri nella condivisione dei dati con lo specialista, con un tasso di sicurezza del 100 %. Nelle altre fasce, invece, almeno un partecipante si è mostrato incerto.

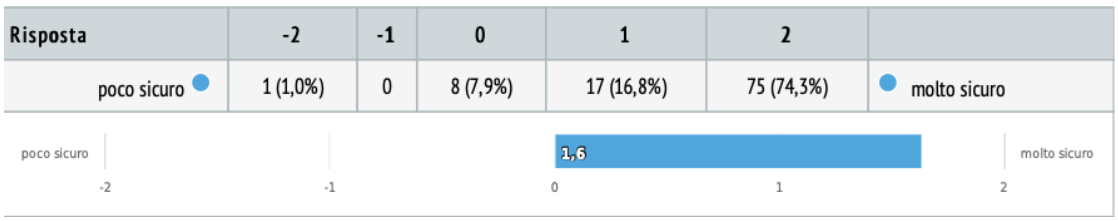

Figura 6.13: Rispetto alla tua esperienza, ti chiedo quanto ti senti sicuro rispetto alla condivisione delle tue informazioni personali con lo specialista.

In generale, la condivisione dei propri dati con i medici o associazioni dei pazienti non preoccupa i rispondenti (Figura 6.14). Infatti, entrambe raggiungono una definizione di sicurezza simile (71 % il primo e 67 % il secondo). Le associazioni dei pazienti, SIMBA nel caso dei malati Behçet, svolgono il ruolo di intermediazione

tra gli specialisti e il paziente ed intervengono, dopo aver intercettato i bisogni del paziente, per assicurare il miglior specialista per il paziente. Anche in questo caso emergono delle differenze nelle valutazioni di uomini e donne: gli uomini, rispetto alle loro esperienze, non si sentono mai poco sicuri, a differenza delle donne che esprimono la totalità dell'incertezza del campione (6 %). Analizzando le singole fasce d'età, quella dai 31 ai 45 anni d'età esprime la massima insicurezza rispetto alla condivisione dei dati con il medico di base (39 %). Questo dato potrebbe essere dovuto alla difficoltà di diagnosi di BD, che porta il paziente a doversi confrontare con diversi medici prima di trovare la causa scatenante. Secondo la letteratura, infatti, è la prima fascia di popolazione interessata dai sintomi più gravi della malattia.

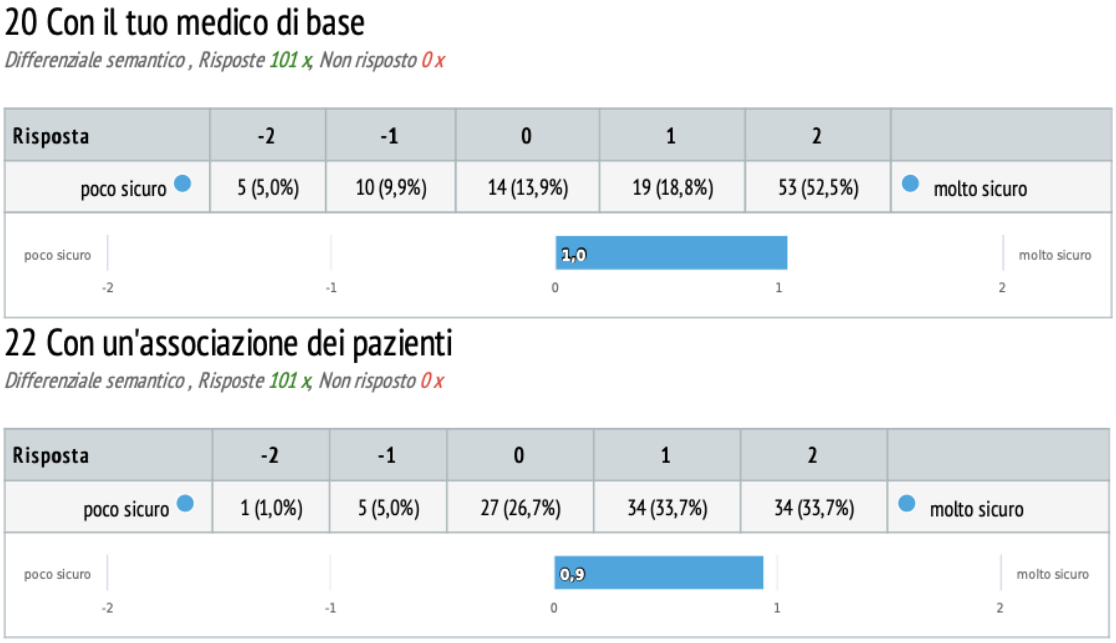

Figura 6.14: Rispetto alla tua esperienza, ti chiedo quanto ti senti sicuro rispetto alla condivisione delle tue informazioni personali.

La sicurezza diminuisce quando il paziente non si deve confrontare con enti che non si occupano, direttamente, della malattia (Figura 6.15). Le altre associazioni mediche, come farmacie e centri vaccinali, registrano una percentuale elevata (31 %) di soggetti che preferisce non esprimere una chiara preferenza. La stessa situazione si verifica quando il paziente si confronta con lo Stato (40 %) e con il datore di lavoro (34 %). Le preferenze espresse da uomini e donne sono simili, differiscono unicamente nella fiducia riposta verso lo Stato: gli uomini mostrano un tasso di sicurezza più alto (45 %) rispetto alle donne (20 %). I rispondenti appartenenti alla fascia 46-60 esprimono un elevato tasso d'insicurezza quando si confrontano con

questi enti: varia dal 35 % per le altre organizzazioni mediche al 45 % per lo Stato. Se, invece, vengono considerate anche le posizioni non nette, cioè coloro che hanno votato 0 nella scala del differenziale semantico, emerge un tasso di insicurezza verso le organizzazioni mediche del 60 % e verso lo Stato del 75 %.

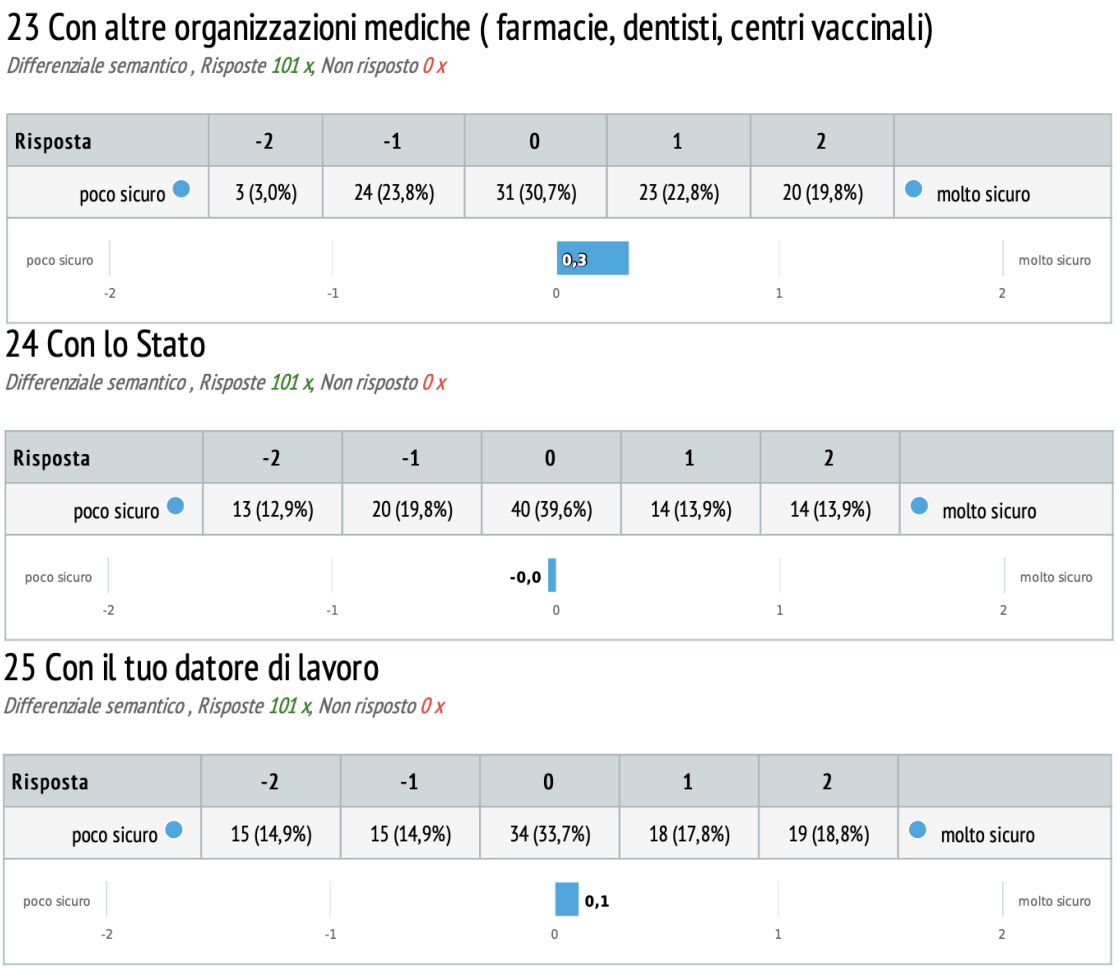

Figura 6.15: Rispetto alla tua esperienza, ti chiedo quanto ti senti sicuro rispetto alla condivisione delle tue informazioni personali con i seguenti enti.

La fiducia si riduce al minimo quando il paziente si confronta con la compagnia di assicurazione. Questa categoria risulta l'unica, dell'intero questionario, con un valore totale negativo (-0,5) nella scala del differenziale semantico. Il 43 % dei soggetti preferisce non esprimere una chiara posizione e il 42 %, invece, conferma di essere poco sicuro quando deve condividere i propri dati con la compagnia di assicurazione. Questo dato è in linea con la letteratura in campo medico, che riporta dei tassi di confidenza, nel condividere le informazioni con una compagnia

di assicurazione, a livelli minimi.

Risposta	-2	-1	0	1	2	
poco sicuro	24 (23,8%)	19 (18,8%)	43 (42,6%)	11 (10,9%)	4 (4,0%)	molto sicuro

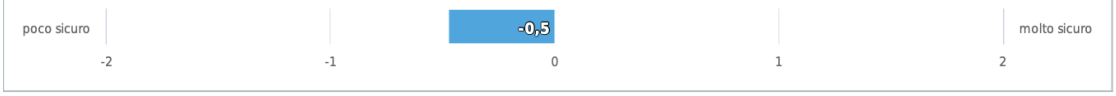

Figura 6.16: Rispetto alla tua esperienza, ti chiedo quanto ti senti sicuro rispetto alla condivisione delle tue informazioni personali con la compagnia d'assicurazione.

Infine, è stato chiesto ai pazienti se l'utilizzo di una rete informatizzata totalmente sicura, in cui salvare i dati personali, potesse farli sentire più sicuri e più a loro agio nella condivisione delle loro informazioni (Figura 6.17). Il 65 % dei partecipanti si mostra favorevole, con solo il 7 % che non è convinto del miglioramento apportato dalla tecnologia. La restante parte di rispondenti (29 %) non ha una chiara idea sull'implementazione della tecnologia in campo medico. La fascia dai 18 ai 30 anni è quella che riporta un grado di apprezzamento più alto (75 %).

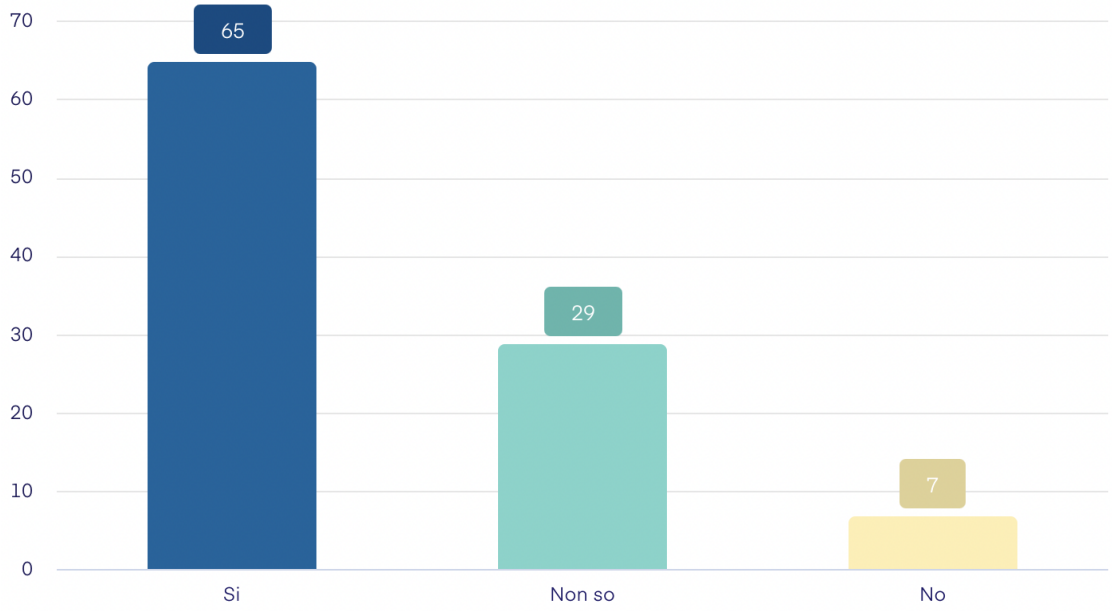

Figura 6.17: Pensi che l'introduzione di una rete informatica totalmente sicura, in cui salvare i dati, possa farti sentire più a tuo agio sulla condivisione delle tue informazioni mediche?

Ai soggetti che hanno indicato di essere disponibili a condividere le loro informazioni personali con la condizione che fossero condivise in modo sicuro sono state poste altre 3 domande, per comprendere meglio le loro credenze riguardo la privacy. Inizialmente è stato chiesto perché ritenessero che fosse importante che i dati fossero condivisi in maniera sicura (Figura 6.18). Emergono risposte differenti, ma dallo stesso significato. I pazienti vorrebbero che fosse assicurata una condivisione sicura, in quanto i dati rappresentano loro stessi e dovrebbero essere usati solo per le giuste finalità, da chi ne ha diritto.

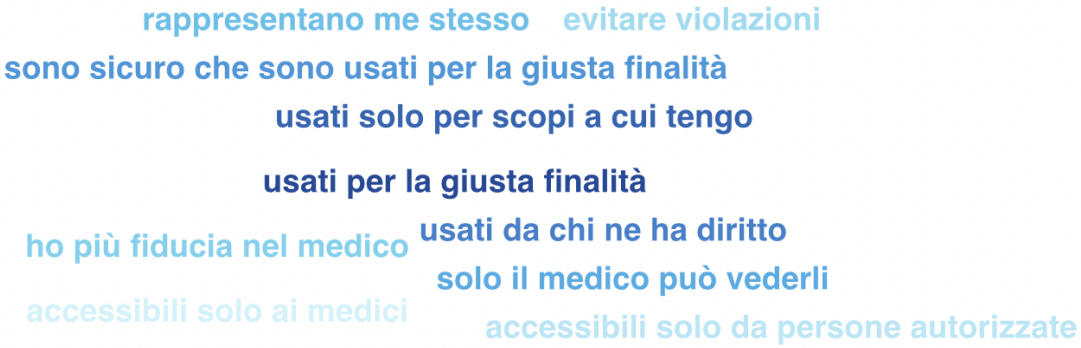

Figura 6.18: Perché ritieni importante che i tuoi dati siano condivisi in modo sicuro?

Successivamente, è stato chiesto loro quali fossero i rischi percepiti nella condivisione dei dati personali (Figura 6.19).

Emerge, dalla maggior parte delle risposte, che i votanti temano che i loro dati siano usati in maniera impropria e che possano creare delle condizioni di svantaggio rispetto ai soggetti sani. Inoltre, temono che i dati possano provocare dei furti d'identità, con conseguenti azioni non autorizzate.

Infine, è stato chiesto se ci fossero soluzioni che potessero farli sentire più sicuri (Figura 6.20).

Emerge che i votanti vorrebbero sempre sapere chi utilizza i loro dati e, al tempo stesso, vorrebbero utilizzare i servizi in modo anonimo. Inoltre, risulta necessario per il paziente che i dati siano consultati unicamente dallo specialista o che il paziente sia contattato per autorizzare il trattamento dei dati.

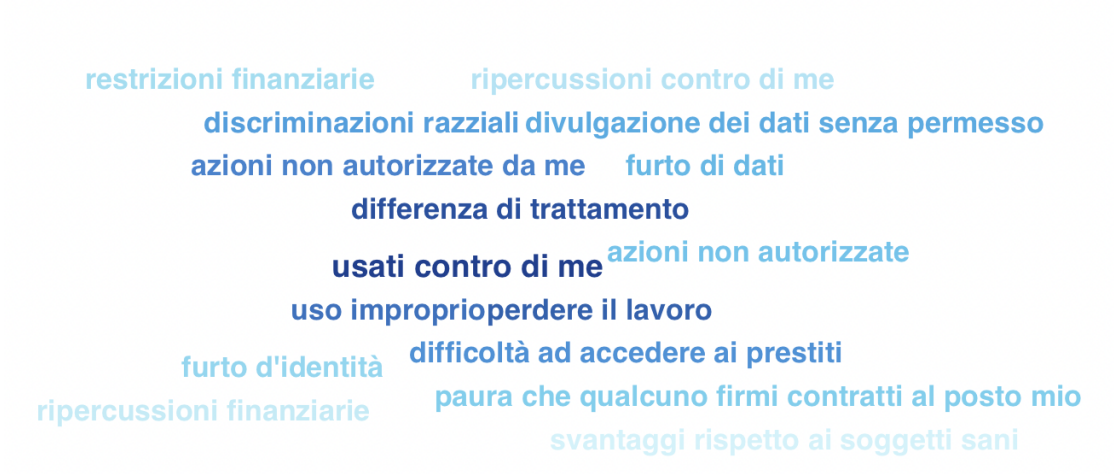

Figura 6.19: Quali sono i rischi che percepisci nella condivisione dei tuoi dati personali?

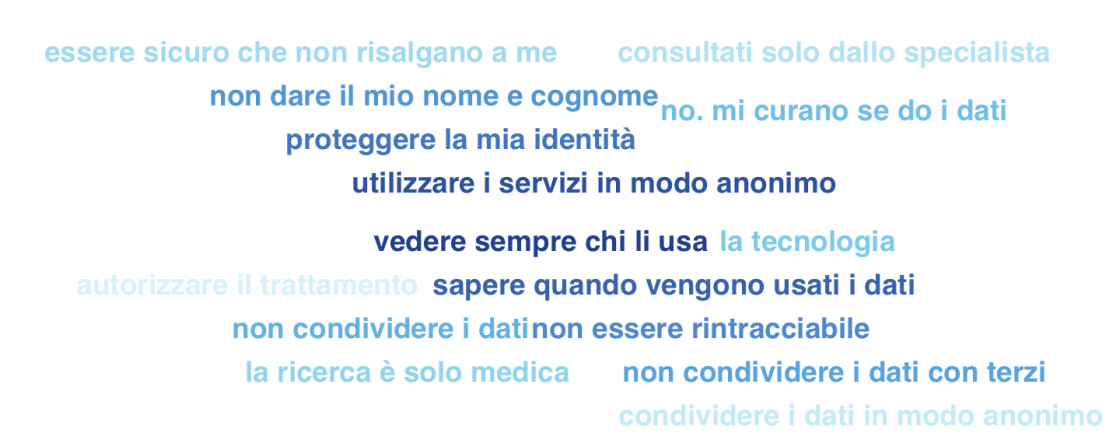

Figura 6.20: Pensi che esistano soluzioni che possano farti sentire più sicur*?

Capitolo 7

Conclusioni e Prospettive future

7.1 Conclusioni

Il lavoro svolto dimostra la propensione dei pazienti affetti da Behçet alla condivisione delle proprie informazioni personali. La quasi totalità dei partecipanti si sente sicuro quando condivide le informazioni con gli specialisti e le condividerebbe, sicuramente, per entrare in contatto con una rete di specialisti. Il contatto da remoto rappresenta un punto di svolta per il paziente e lo fa propendere a cedere i propri dati personali.

In tal senso, l'utilizzo della tecnologia rappresenta un punto di svolta nella cura di una malattia rara. La possibilità di avere un contatto immediato con i medici rassicura il paziente e questo aspetto è più importante della sicurezza del dato. Inoltre, non mostrano diffidenza nel condividere i loro dati personali per favorire la ricerca e lo sviluppo di nuove soluzioni.

In generale, i rispondenti si mostrano disponibili a condividere le loro informazioni con enti direttamente correlati con la loro patologia. Al contrario, mostrano diffidenza verso le istituzioni di natura non medica. Questo risultato è in linea con il modello di Hofstede applicato all'Italia, che mostra una bassa fiducia nelle istituzioni da parte degli Italiani.

Emergono delle differenze tra le valutazioni di uomini e donne. Gli uomini sono più interessati a condividere le loro informazioni per migliorare la ricerca e la cura della patologia. Le diverse propensioni sono dovute, probabilmente, alla diversa incidenza e alla diversa gravità. La letteratura attualmente disponibile conferma che gli uomini sono più colpiti delle donne, con forme più gravi della malattia. Questo comporta degli interessi diversi e una propensione maggiore degli uomini a trovare delle cure che possano alleviare i sintomi.

Si notano differenze anche a livello di gruppi d'età. I rispondenti appartenenti alla fascia tra i 46 e i 60 anni sono i più disponibili a fornire i propri dati per migliorare la cura della malattia. La letteratura attuale suggerisce che negli ultimi 15 anni sono stati fatti passi in avanti per la cura della patologia, introducendo nuove tipologie di farmaco altamente performanti. È plausibile che i soggetti tra i 46 e i 60 anni abbiano beneficiato dei nuovi farmaci, che permettono di migliorare le condizioni di vita e superare i sintomi più gravi. Infatti, i farmaci biologici, che sono stati approvati per il trattamento dei disordini più gravi nel 2003 [74], favoriscono una condizione di remissione della malattia.

In linea con la letteratura precedentemente analizzata, il flusso di informazioni condivise diminuisce all'aumentare della sensibilità del dato. I pazienti Behçet mostrano più diffidenza nella condivisione dei dati quando questi sono estremamente sensibili (nome della malattia vs informazioni sulla tua disabilità).

A differenza della letteratura analizzata, i pazienti sono propensi a condividere le loro informazioni e sembrano non essere parte integrante del paradosso della privacy discusso in precedenza.

Analizzando le risposte individuali, però, emerge una contraddizione nelle risposte degli uomini. Loro vorrebbero condividere i propri dati personali per evitare di spostarsi dal luogo di residenza, ma al tempo stesso danno la più bassa valutazione possibile allo snellimento delle pratiche burocratiche. Attualmente, almeno per quanto riguarda la gestione delle malattie rare, spostandosi da un centro ad un altro è necessario portarsi dietro la cartella medica con tutti gli esami diagnostici effettuati. Inoltre, vista l'assenza di standard comuni tra i vari centri, è necessario ripetere gli esami, anche se sostenuti a distanza di pochi giorni. Non esiste un database condiviso che permetta di registrare i dati dei paziente e che eviti, sopratutto, spese non necessarie per il Sistema Sanitario Nazionale (SSN). Almeno tra i centri di riferimento, che risultano accreditati per il trattamento di una malattia rara, dovrebbe esistere un collegamento che permetta al paziente di non ripetere analisi già fatte e allo specialista di accettare gli esami, se effettuati a breve distanza, effettuati da altri laboratori. In definitiva, emerge un paradosso nelle risposte individuali che non era emerso a livello globale. Il paradosso, però, mette in evidenza una carenza del SSN che dovrebbe essere risolta, per garantire al paziente un processo meno invasivo e, sopratutto, evitare uno spreco monetario non giustificabile.

Solo una minoranza dichiara di non essere mai disposto a cedere i propri dati personali, in nessun caso. Questa situazione, almeno in Italia, non è plausibile in quanto per confrontarsi con un medico è necessario fornire il proprio nome, cognome e codice fiscale. Tali dati, anche se ritenuti non troppo sensibili, fanno ugualmente parte dei dati sanitari di una persona.

La fascia di rispondenti tra i 31 ed i 45 anni è l'unica a porre come tema fondamentale la sicurezza dei dati. Questo interesse potrebbe essere dovuto alla

formulazione delle prime direttive in tema di protezione dei dati online nei primi anni 2000. Infatti, la prima direttiva per il trattamento dei dati personali risale al 2002. I votanti potrebbero essersi interessati al fenomeno da più giovani, avendo ora consapevolezza dei rischi derivanti dalla condivisione dei dati. Dalle risposte emerge che i pazienti sono disponibili a condividere i loro dati a condizione che questi siano trattati in modo anonimo e che abbiano finalità unicamente mediche. Inoltre, percepiscono come rischio principale la possibilità che il dato condiviso possa essere usato contro di loro: ad esempio, identificano nelle penalizzazioni finanziarie un rischio concreto.

La blokchain, nonostante non sia mai stata nominata, assolve perfettamente ai problemi identificati dai pazienti. Permette di trattare i dati in modo anonimo, di trasformare le informazioni in stringhe tramite la crittografia e di approvare l'utilizzo dei dati, per mezzo degli smart contract. Emerge dai pazienti una disponibilità ad usare la tecnologia per la gestione dei loro dati personali. In tal modo, si potrebbe evitare il rischio di detenere registri non correttamente trattati in materia di gestione dei dati personali, permettendo al medico di non dover scegliere tra qualità e privacy.

7.2 Prospettive future

Il paradosso della privacy è un fenomeno presente in tutti i settori. In alcuni di essi, però, produce dei problemi che bisogna arginare prontamente, creando delle soluzioni durature nel tempo.

Nel settore medico, ad esempio, il paradosso della privacy rappresenta una problematica che comporta delle decisioni importanti. Il medico è costretto a scegliere tra il diritto alla privacy del paziente e il dovere a fornire cure di qualità. La letteratura suggerisce che, alcuni, medici bypassano la normativa, in quanto è loro dovere fornire cure di qualità e questo dovere è più forte del diritto alla privacy. Questo comporta che molti registri, secondo la normativa attuale, siano non conformi e rischino di essere eliminati, con danni enormi sia per la ricerca che per il paziente.

Non è sempre detto che normative stringenti creino condizioni migliori, anzi il più delle volte si verifica il viceversa. La normativa stringente verso la protezione dei dati dei cittadini, che è corretta vista l'importanza della tutela dei dati personali, rischia di creare dei limiti importanti per la ricerca, con conseguenze catastrofiche nel lungo periodo. Nel settore delle malattie rare questo rappresenta un chiaro problema e bisogna intervenire il prima possibile per trovare una soluzione equa che garantisca sia il diritto alla privacy che il dovere a fornire cure di qualità.

È fondamentale chiedersi, però, se in un Paese come il nostro un cittadino possa rifiutarsi di condividere i suoi dati personali se questi sono necessari per

garantire una qualità della vita migliore a centinaia, se non migliaia, di persone affette dalla sua stessa patologia. Si pone la questione sul nostro Sistema Sanitario Nazionale perché, nonostante negli ultimi anni sia stato più volte etichettato come di scarsa qualità, fornisce gratuitamente a tutti i malati rari farmaci dal costo elevato. L'adalimumab, più volte citato in questa trattazione, ha un costo di 1410,84 €, nella sua formulazione fornita dalla casa farmaceutica Amgen. La durata del trattamento dipende dalla gravità dei sintomi, ma il farmaco viene somministrato almeno per un anno per un costo complessivo di 16930,08 €.

La risposta alla domanda non è banale. Bisognerebbe porre il paziente nelle condizioni in cui non possa rifiutare la condivisione dei dati. Questo è possibile, unicamente, se si garantisce trasparenza nell'uso dei dati e si trasmette una condizione di fiducia. Come evidenziato nel caso studio, il paziente affetto da Behçet, o più in generale da una malattia rara, identifica nello specialista un soggetto di cui fidarsi, senza porsi dei problemi nella condivisione dei dati. Tale situazione si origina perché si identifica nello specialista una persona che possa offrire cure di qualità eccelsa, permettendo di migliorare le condizioni di vita. Si dovrebbe puntare ad un modello nel quale il paziente sia libero di condividere informazioni, di tipo certificato, come se stesse interagendo sempre con lo specialista.

La blockchain potrebbe rappresentare un punto di svolta nella gestione delle malattie rare, puntando contemporaneamente al rispetto dei dati e alla qualità delle cure. Una singola blockchain non sarebbe sufficiente, perché si dovrebbe obbligare il medico a svolgere funzioni non attenenti al suo lavoro. In via del tutto teorica, sarebbe sufficiente creare due tipi di blockchain:

- una di tipo pubblico, utilizzata dai pazienti;
- una di tipo privato, utilizzata dai medici.

Per la tipologia utilizzata dai pazienti si propone una blockchain di tipo pubblico, attraverso la quale possano certificare le informazioni. L'accesso sarebbe garantito attraverso il codice di esenzione che identifica la malattia e i dati dei pazienti, quali ad esempio i sintomi, sarebbero gestiti attraverso la crittografia, garantendo l'anonimizzazione richiesta. Le blockchain pubbliche, però, funzionano se ad esse è associata una valuta. Si potrebbe creare un token, di tipo inflattivo, da spendere unicamente nel SSN, ad esempio per interagire in sessioni di Q&A con gli specialisti. Si creerebbe una forma di economia chiusa, a lungo dibattuta nella letteratura attuale.

Un sistema del genere non avrebbe bisogno di un sistema di protezione altamente performante come la POW, ma sarebbe sufficiente un sistema di tipo POS. Infatti, l'assenza di valore della moneta renderebbe nullo il rischio di nothing at stake presentato nel capitolo 4.

Per la tipologia utilizzata dai medici, invece, si propone una blockchain di tipo privato. Essa si dovrebbe interfacciare con la blockchain dei pazienti, permettendo

di monitorare i dati inseriti. In tal modo i medici possono utilizzare i dati in aggregato per finalità di ricerca. L'utilizzo è uguale a quello di un normale database, quindi non ci sarebbero differenze tangibili nel loro lavoro. L'unica differenza è da individuarsi nella possibilità del paziente di poter monitorare se il medico utilizza i dati per lo scopo indicato.

Prima di attuare un sistema del genere, che è proposto soltanto in forma teorica, bisognerebbe indagare i costi per realizzarlo e, sopratutto, per mantenerlo. Indubbiamente, però, permetterebbe di eliminare il costo che il SSN paga per le strutture accreditate al trattamento di una determinata patologia rara. Emerge infatti che molti centri abbiano un tasso di frequenza molto basso se non nullo. Dal caso Behçet, ad esempio, emerge che i pazienti siano in cura prevalentemente in 3 regioni d'Italia. Se si sfruttasse la tecnologia, il costo dell'accreditamento, almeno per i centri non utilizzati, potrebbe essere riconvertito. I medici, non per forza specialisti della malattia, potrebbero accedere alla blokchain privata ed informarsi sui sintomi che riportano i pazienti, in modo da individuare precocemente la malattia. In questo modo, sarebbe più facile per il paziente intraprendere il giusto percorso terapeutico.

La blockchain potrebbe essere la soluzione per migliorare il processo di gestione di una malattia rara, garantendo al paziente la centralità di cui ha bisogno. Non è detto che sia l'unico sistema disponibile. Attualmente, però, è uno di quelli che risponde meglio e potrebbe risolvere numerosi problemi citati in questa trattazione. È necessario che nell'immediato futuro siano adottate soluzioni che non permettano l'esistenza del paradosso. Un medico non si deve trovare nella condizione di violare le normative vigenti sulla privacy per offrire cure di qualità al paziente. Ugualmente, al paziente dovrà essere garantito un trattamento qualitativo e la protezione totale dei dati. Non è un cambiamento semplice da attuare, ma è doveroso e necessario e la tecnologia emergente è determinante per renderlo concreto.

Bibliografia

[1] "https://www.treccani.it/enciclopedia" (cit. a p. 7).

[2] Juan Pablo Carrascal, Christopher Riederer, Vijay Erramilli, Mauro Cherubini e Rodrigo de Oliveira. «Your Browsing Behavior for a Big Mac: Economics of Personal Information Online». In: *Proceedings of the 22nd International Conference on World Wide Web*. WWW '13. Rio de Janeiro, Brazil: Association for Computing Machinery, 2013, pp. 189–200. ISBN: 9781450320351. DOI: 10.1145/2488388.2488406. URL: https://doi.org/10.1145/2488388.2488406 (cit. alle pp. 7, 18).

[3] Alessandro Acquisti. «Privacy in Electronic Commerce and the Economics of Immediate Gratification». In: *Proceedings of the 5th ACM Conference on Electronic Commerce*. EC '04. New York, NY, USA: Association for Computing Machinery, 2004, pp. 21–29. ISBN: 1581137710. DOI: 10.1145/988772.988777. URL: https://doi.org/10.1145/988772.988777 (cit. a p. 7).

[4] B. A. Huberman, E. Adar e L. R. Fine. «Valuating privacy». In: *IEEE Security Privacy* 3.5 (2005), pp. 22–25. DOI: 10.1109/MSP.2005.137 (cit. a p. 7).

[5] Alastair R. Beresford, Dorothea Kübler e Sören Preibusch. «Unwillingness to pay for privacy: A field experiment». In: *Economics Letters* 117.1 (2012), pp. 25–27. ISSN: 0165-1765. DOI: https://doi.org/10.1016/j.econlet.2012.04.077. URL: https://www.sciencedirect.com/science/article/pii/S0165176512002182 (cit. a p. 8).

[6] Tamara Dinev e Paul Hart. «An Extended Privacy Calculus Model for E-Commerce Transactions». In: *Information Systems Research* 17.1 (2006), pp. 61–80. DOI: 10.1287/isre.1060.0080. eprint: https://pubsonline.informs.org/doi/pdf/10.1287/isre.1060.0080. URL: https://pubsonline.informs.org/doi/abs/10.1287/isre.1060.0080 (cit. a p. 8).

[7] Spyros Kokolakis. «Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon». In: *Computers Security* 64 (2017). URL: https://www.sciencedirect.com/science/article/pii/S0167404815001017 (cit. a p. 8).

[8] Vaibhav Garg, Kevin Benton e L. Jean Camp. «The Privacy Paradox: A Facebook Case Study». In: *TPRC Conference Paper* (2014). URL: http://dx.doi.org/10.2139/ssrn.2411672 (cit. a p. 9).

[9] "https://investor.fb.com/financials/default.aspx" (cit. a p. 10).

[10] Alyson Leigh Young e Anabel Quan-Haase. «PRIVACY PROTECTION STRATEGIES ON FACEBOOK». In: *Information, Communication & Society* 16.4 (2013), pp. 479–500. DOI: 10.1080/1369118X.2013.777757. eprint: https://doi.org/10.1080/1369118X.2013.777757. URL: https://doi.org/10.1080/1369118X.2013.777757 (cit. a p. 11).

[11] " urly.it/3cba4" (cit. a p. 11).

[12] Mary Madden e Aaron Smith. «Reputation Management and Social Media». In: (2010). URL: http://www.pewinternet.org/2010/05/26/reputation-management-and-social-media/ (cit. a p. 11).

[13] " https://www.ilpost.it/2018/03/19/facebook-cambridge-analytica/" (cit. a p. 12).

[14] "https://www.vice.com/en/article/mg9vvn/how-our-likes-helped-trump-win" (cit. a p. 12).

[15] "https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/?sh=2ee478b4bd54" (cit. a p. 13).

[16] "urly.it/3cba0" (cit. a p. 13).

[17] Eric P.S. Baumer, Phil Adams, Vera D. Khovanskaya, Tony C. Liao, Madeline E. Smith, Victoria Schwanda Sosik e Kaiton Williams. «Limiting, Leaving, and (Re)Lapsing: An Exploration of Facebook Non-Use Practices and Experiences». In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '13. Paris, France: Association for Computing Machinery, 2013, pp. 3257–3266. ISBN: 9781450318990. DOI: 10.1145/2470654.2466446. URL: https://doi.org/10.1145/2470654.2466446 (cit. a p. 13).

[18] "https://www.theguardian.com/technology/2018/apr/16/cambridge -analytica-scandal-highlights-need-for-ai-regulation" (cit. a p. 13).

[19] Alice E Marwick e danah boyd. «Networked privacy: How teenagers negotiate context in social media». In: *New Media & Society* 16.7 (2014), pp. 1051–1067. DOI: 10.1177/1461444814543995. eprint: https://doi.org/10.1177/1461444814543995. URL: https://doi.org/10.1177/1461444814543995 (cit. a p. 14).

[20] Joanne Hinds, Emma J. Williams e Adam N. Joinson. «"It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal». In: *International Journal of Human-Computer Studies* 143 (2020), p. 102498. ISSN: 1071-5819. DOI: https://doi.org/10.1016/j.ijhcs.2020.102498. URL: https://www.sciencedirect.com/science/article/pii/S1071581920301002 (cit. a p. 14).

[21] " http://hdl.handle.net/10077/30878" (cit. a p. 14).

[22] " https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7812813/" (cit. a p. 14).

[23] " https://www.statista.com/statistics/1190062/covid-19-app-downloads-uk/" (cit. a p. 15).

[24] "https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:32009L0136" (cit. a p. 15).

[25] "https://gdpr.eu/cookies/" (cit. a p. 15).

[26] "urly.it/3cba6 " (cit. a p. 16).

[27] Avi Goldfarb e Catherine E. Tucker. «Privacy Regulation and Online Advertising». In: *Management Science* 57.1 (2011), pp. 57–71. DOI: 10.1287/mnsc.1100.1246. eprint: https://doi.org/10.1287/mnsc.1100.1246. URL: https://doi.org/10.1287/mnsc.1100.1246 (cit. a p. 19).

[28] Gian Luca Comandini. *Da Zero alla Luna*. Dario Flaccovio Editore, 2020 (cit. a p. 23).

[29] Anthony Sanders. «The subprime crisis and its role in the financial crisis». In: *Journal of Housing Economics* 17.4 (2008). Special issue on subprime mortgage lending, pp. 254–261. ISSN: 1051-1377. DOI: https://doi.org/10.1016/j.jhe.2008.10.001. URL: https://www.sciencedirect.com/science/article/pii/S1051137708000363 (cit. a p. 23).

[30] Lawrence J. Christiano, Martin S. Eichenbaum e Mathias Trabandt. «Understanding the Great Recession». In: *American Economic Journal: Macroeconomics* 7.1 (gen. 2015), pp. 110–67. DOI: 10.1257/mac.20140104. URL: https://www.aeaweb.org/articles?id=10.1257/mac.20140104 (cit. a p. 23).

[31] " http://cryptosystem.altervista.org/chiave-privata/" (cit. a p. 26).

[32] "https://bitcoin.org/bitcoin.pdf" (cit. a p. 27).

[33] "https://bitcoin.org/files/bitcoin-paper/bitcoin$_i$*t.pdf*" (cit. alle pp. 27, 28, 30, 31).

[34] " https://cryptonomist.ch/2019/08/04/problema-generali-bizantini-soluzione-bitcoin/" (cit. a p. 32).

[35] Joseph Abadi e Markus Brunnermeier. *Blockchain Economics*. Working Paper 25407. National Bureau of Economic Research, dic. 2018. DOI: 10.3386/w25407. URL: http://www.nber.org/papers/w25407 (cit. alle pp. 33, 34).

[36] Vincenzo Morabito. *Business Innovation Through Blockchain*. Gen. 2017. ISBN: 978-3-319-48477-8. DOI: 10.1007/978-3-319-48478-5 (cit. a p. 34).

[37] Alex de Vries. «Bitcoin's Growing Energy Problem». In: *Joule* 2.5 (2018), pp. 801–805. ISSN: 2542-4351. DOI: https://doi.org/10.1016/j.joule.2018.04.016. URL: https://www.sciencedirect.com/science/article/pii/S2542435118301776 (cit. alle pp. 35, 36).

[38] "https://digiconomist.net/bitcoin-energy-consumption" (cit. a p. 37).

[39] "https://www.statista.com/statistics/881541/bitcoin-energy-consumption-transaction-comparison-visa/" (cit. a p. 38).

[40] " https://www.blockchain4innovation.it/mercati/legal/smart-contract/blockchain-smart-contracts-cosa-funzionano-quali-gli-ambiti-applicativi/" (cit. a p. 39).

[41] Jiin-Chiou Cheng, Narn-Yih Lee, Chien Chi e Yi-Hua Chen. «Blockchain and smart contract for digital certificate». In: *2018 IEEE International Conference on Applied System Invention (ICASI)*. 2018, pp. 1046–1051. DOI: 10.1109/ICASI.2018.8394455 (cit. a p. 39).

[42] "https://www.binance.com/en/defi-staking" (cit. a p. 40).

[43] "https://blog.ethereum.org/2021/05/18/country-power-no-more/" (cit. a p. 41).

[44] "https://www.hwupgrade.it/news/web/ethereum-con-il-proof-of-stake-consumera-davvero-il-99-95-in-meno-si-secondo-i-calcoli-di-uno-sviluppatore$_9$7857.*html*" (cit. a p. 41).

[45] Ethan. Kane. «Is Blockchain a General Purpose Technology?» In: (March 11, 2017). eprint: http://dx.doi.org/10.2139/ssrn.2932585. URL: https://ssrn.com/abstract=2932585 (cit. a p. 42).

[46] Likić R. Radanović I. «Opportunities for Use of Blockchain Technology in Medicine.» In: *Appl Health Econ Health Policy 16, 583–590 (2018)*. (). URL: https://doi-org.ezproxy.biblio.polito.it/10.1007/s40258-018-0412-8 (cit. alle pp. 42, 50).

[47] " https://patientoryassociation.org/wp-content/uploads/2018/11/italian.pdf" (cit. a p. 43).

[48] Xing Zhang, Shan Liu, Xing Chen, Lin Wang, Baojun Gao e Qing Zhu. «Health information privacy concerns, antecedents, and information disclosure intention in online health communities». In: *Information Management* 55.4 (2018), pp. 482–493. ISSN: 0378-7206. DOI: https://doi.org/10.1016/j.im.2017.11.003. URL: https://www.sciencedirect.com/science/article/pii/S0378720617300174 (cit. a p. 43).

[49] A. Phaneuf. «How mHealth apps are providing solutions to the healthcare market's problems». In: (2019). URL: https://www.businessinsider.com/mhealth-apps-definition-examples?r=US&IR=T (cit. a p. 43).

[50] Grace Fox e Regina Connolly. «Mobile health technology adoption across generations: Narrowing the digital divide». In: *Information Systems Journal* 28.6 (2018), pp. 995–1019. DOI: https://doi.org/10.1111/isj.12179. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/isj.12179. URL: https://onlinelibrary.wiley.com/doi/abs/10.1111/isj.12179 (cit. a p. 43).

[51] Corey Angst e Ritu Agarwal. «Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion». In: *MIS Quarterly* 33 (giu. 2009), pp. 339–370. DOI: 10.2307/20650295 (cit. a p. 43).

[52] Grace Fox. «"To protect my health or to protect my health privacy?" A mixed-methods investigation of the privacy paradox». In: *Journal of the Association for Information Science and Technology* 71.9 (2020), pp. 1015–1029. DOI: https://doi.org/10.1002/asi.24369. eprint: https://asistdl.onlinelibrary.wiley.com/doi/pdf/10.1002/asi.24369. URL: https://asistdl.onlinelibrary.wiley.com/doi/abs/10.1002/asi.24369 (cit. a p. 44).

[53] "https://www.ibm.com/downloads/cas/9V2LRYG5?utm$_medium$ = $OSocialutm_source = Blogutm_content = 000020YKutm_term = 10005803$ $utm_id = How - the - FDA - is - piloting - blockchain - for - the - pharmaceutical - supply - chain - CTA - Button - 1cm_mmc =$ $OSocial_Blog -_ Blockchain + and + Strategic + Alliances_Blockchain -_ WW_WW -_ How - the - FDA - is - piloting - blockchain - for - the - pharmaceutical - supply - chain - CTA - Button - 1cm_mmca1 =$ $000020YKcm_mmca2 = 10005803$" (cit. alle pp. 45, 46).

[54] " https://www.ibm.com/it-it/blockchain/solutions/vaccine-distribution" (cit. a p. 46).

[55] " https://newsroom.ibm.com/A-Groundbreaking-Vaccine-Will-Need -a-Groundbreaking-Supply-Chain" (cit. a p. 46).

[56] " https://media.defense.gov/2020/Jul/23/2002462846/-1/-1/1/ $\mathrm{OT}_A DVISORY - DUAL - OFFICIAL - 20200722.PDF$" (cit. a p. 47).

[57] "https://www.ibm.com/downloads/cas/QRP1EP1V" (cit. a p. 47).

[58] " https://www.ibm.com/it-it/products/digital-health-pass" (cit. a p. 48).

[59] Melanie Swan. *Blockchain: blueprint for a new economy*. Sebastopol: O'Reilly Media, 2015 (cit. a p. 49).

[60] "https://www.finextra.com/finextra-downloads/newsdocs/document -1063851711.pdf" (cit. alle pp. 50, 51).

[61] I. Melnikova. «Rare diseases and orphan drugs.» In: *Nat Rev Drug Discov* 11 (2012), pp. 267–268. DOI: https://doi.org/10.1038/nrd3654 (cit. alle pp. 53, 54).

[62] Carlos R. Ferreira. «The burden of rare diseases». In: *American Journal of Medical Genetics Part A* 179.6 (2019), pp. 885–892. DOI: https://doi.org/10.1002/ajmg.a.61124. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/ajmg.a.61124. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/ajmg.a.61124 (cit. a p. 54).

[63] Shi T. Jia J. «Towards efficiency in rare disease research: what is distinctive and important?.» In: *Sci. China Life Sci.* 60 (2017), pp. 686–691. DOI: https://doi.org/10.1007/s11427-017-9099-3 (cit. a p. 54).

[64] Dimond R. Bros-Facer V. Courbier S. «Share and protect our health data: an evidence based approach to rare disease patients' perspectives on data sharing and data protection - quantitative survey and recommendations.» In: *Orphanet J Rare Dis.* 14 (2019), p. 175. DOI: https://doi.org/10.1186/s13023-019-1123-4 (cit. a p. 56).

[65] Jorge L. Contreras e Jerome H. Reichman. «Sharing by design: Data and decentralized commons». In: *Science* 350.6266 (2015), pp. 1312–1314. ISSN: 0036-8075. DOI: 10.1126/science.aaa7485. eprint: https://science.sciencemag.org/content/350/6266/1312.full.pdf. URL: https://science.sciencemag.org/content/350/6266/1312 (cit. a p. 56).

[66] Deborah Mascalzoni, Angelo Paradiso e Matts Hansson. «Rare disease research: Breaking the privacy barrier». In: *Applied Translational Genomics* 3.2 (2014). From Biobanks to the Clinic, pp. 23–29. ISSN: 2212-0661. DOI: https://doi.org/10.1016/j.atg.2014.04.003. URL: https://www.sciencedirect.com/science/article/pii/S2212066114000052 (cit. alle pp. 57, 58).

[67] Aymé S. et al. Mascalzoni D. Knoppers B. «Rare diseases and now rare data?.» In: *Nat Rev Genet* 14 (2013), p. 372. DOI: https://doi.org/10.1038/nrg3494 (cit. a p. 58).

[68] «The Convention for the Protection of Human Right and Dignity of the Human Being With Regard to the Application of Biology and Medicine: Con- vention on Human Rights and Biomedicine (Oviedo Convention)». In: (). URL: http://www.tissuebank.it/publicazioni/docUfficiale/DocumentiInternazionali/ConvenzioneOviedo.pdf (cit. a p. 58).

[69] M. Hansson. «Where should we draw the line between quality of care and other ethical concerns related to medical registries and biobanks?» In: *Theor Med Bioeth* 33 (2012), pp. 313–323. DOI: https://doi.org/10.1007/s11017-012-9229-x (cit. a p. 58).

[70] Carlo Salvarani, Nicolò Pipitone, Maria Grazia Catanoso, Luca Cimino, Bruno Tumiati, Pierluigi Macchioni, Gianluigi Bajocchi, Ignazio Olivieri e Luigi Boiardi. «Epidemiology and clinical course of Behçet's disease in the Reggio Emilia area of Northern Italy: A seventeen-year population-based study». In: *Arthritis Care & Research* 57.1 (2007), pp. 171–178. DOI: https://doi.org/10.1002/art.22500. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/art.22500. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/art.22500 (cit. a p. 59).

[71] C Salvarani et al. «Association of MICA alleles and HLA-B51 in Italian patients with Behçet's disease.» In: *The Journal of Rheumatology* 28.8 (2001), pp. 1867–1870. ISSN: 0315-162X. eprint: https://www.jrheum.org/content/28/8/1867.full.pdf. URL: https://www.jrheum.org/content/28/8/1867 (cit. a p. 59).

[72] "https://www.msdmanuals.com/it-it/professionale/disturbi-del-tessuto -muscoloscheletrico-e-connettivo/vasculite/malattia-di-behçet" (cit. a p. 59).

[73] "https://behcetclinic-pisa.it/behcet-talk-pubblici/" (cit. a p. 60).

[74] Noah Scheinfeld. «Adalimumab (HUMIRA): a review». In: *Journal of drugs in dermatology : JDD* 2.4 (ago. 2003), pp. 375–377. ISSN: 1545-9616. URL: http://europepmc.org/abstract/MED/12884458 (cit. a p. 78).