



UNIVERSITÀ POLITECNICA DELLE MARCHE
FACOLTÀ DI ECONOMIA “GIORGIO FUÀ”

Corso di Laurea triennale in Economia e Commercio

Tesi di laurea

BITCOIN, BLOCKCHAIN E PA: UNA POSSIBILE INNOVAZIONE

BITCOIN, BLOCKCHAIN AND PA: A POSSIBLE INNOVATION

Relatore:
Prof. Laura Trucchia

Rapporto Finale di:
Davide Spinaci

Anno Accademico 2020/2021

*“If you don't believe it or don't get it,
I don't have the time to try to convince you,
Sorry”*

INTRODUZIONE	1
1. BREVE STORIA DELLA MONETA	2
2. BLOCKCHAIN	5
3. BITCOIN	11
4. CASI D'USO DELLA BLOCKCHAIN	19
4.1 Disinformazione e innovazioni	19
4.2 La blockchain nell'Unione Europea	23
4.3 Il possibile ruolo nella Pubblica Amministrazione	25
4.4 Una potenziale rivoluzione tributaria	29
4.5 Blockchain e misurazione dell'orario di lavoro	31
4.6 Blockchain come strumento di certificazione	34
4.7 Blockchain e il riconoscimento dei titoli di studio UE	37
CONCLUSIONE	40
BIBLIOGRAFIA	42
SITOGRAFIA	43

INTRODUZIONE

Affascinato dal mondo delle criptovalute e della finanza decentralizzata, ho deciso di approfondire nella tesi argomenti come Bitcoin e la blockchain e come quest'ultima possa avere un ruolo da protagonista nella Pubblica Amministrazione.

Nella prima parte si ripercorrerà una breve storia di quello che è stato il denaro nel corso dei secoli, dall'economia del dono al denaro contante, introducendo temi fondamentali come lo scambio di valore e la fiducia, che torneranno utili in seguito.

Successivamente verrà analizzata la blockchain, spiegandone il funzionamento e alcuni aspetti caratterizzanti come quello della sicurezza, fiducia, condivisione e decentralizzazione, analizzandone qualità e limiti. A questa verrà collegato Bitcoin, la sua prima vera e propria applicazione, introducendo la sua nascita, gli sviluppi e le peculiarità.

Infine, dalla seconda parte di tesi, si mostrerà come la blockchain stia avendo un ruolo rilevante negli investimenti europei e su come possa essere utilizzata in ambiti specifici, non limitandosi al solo aspetto finanziario.

Si toccheranno temi come il possibile ruolo nella Pubblica Amministrazione, nel sistema tributario, nella misurazione dell'orario di lavoro e come strumento di certificazione.

1. BREVE STORIA DELLA MONETA

Oggi vediamo la blockchain come una tecnologia innovativa o qualcosa di appena scoperto, in realtà nasce prima di quello che pensiamo. Quello che la costituisce sono un insieme di tecnologie nate tra gli inizi del 1990 e i primi anni del 2000.

Per poter introdurre l'argomento Bitcoin e blockchain, capendo come e perché sono nati, non si parlerà di tecnologia, informatica o matematica, ma di economia e politica. Per farlo, occorre addentrarci nella storia di cosa è stato il denaro e lo scambio di valore per l'umanità.

Le prime civiltà nate sul pianeta non avevano ancora il concetto di denaro per come lo conosciamo oggi, il valore veniva scambiato tramite "economia del dono", che può essere considerata come la prima forma primitiva di scambio di valore.

L'economia del dono era basata su un complesso formato da comunità economicamente autosufficienti, le quali producevano autonomamente gran parte di ciò di cui avevano bisogno, donando le eccedenze agli altri individui della comunità.

Questo sistema era basato su convenzioni, quali l'obbligo di dare e di ricevere o di restituire più di quanto si fosse ricevuto, e non da regole scritte. Dall'altra parte si dava per scontato che qualcun altro ricambiasse il dono; era dunque un sistema basato sulla fiducia reciproca.

Quando la popolazione cominciò a crescere numericamente, si sentì l'esigenza di una forma di scambio di valore più efficace, si è gradualmente passati al baratto.

Il baratto fu importante perché con questo fu possibile superare quelli che erano i limiti di un consumo individuale: producendo e scambiando con altri, ognuno si può specializzare e il valore di ciascun individuo può aumentare dallo scambio.

Il baratto permetteva lo scambio tra due individui solo in caso di doppia coincidenza dei desideri: "doppio" perché con due parti coinvolte, e "coincidenza di desideri" perché con desideri reciprocamente vantaggiosi che si abbinano perfettamente.

Questo comporta problemi di scalabilità, deperibilità (in termini di alimenti, essi hanno diverse tempistiche di conservazione) e frazionabilità (sarebbe impossibile suddividere dei beni indivisibili, come ad esempio una pecora).

Come soluzione a questo problema si cominciò a standardizzare il baratto, cioè veniva scelto un oggetto o un bene comune a tutti, con cui veniva quantificato il valore da dare ad ogni bene (esempio 1 pecora = 5 conchiglie). Dunque, un certo bene, scambiato più degli altri, emerge dal mercato e diventa denaro, con la funzione principale di favorire lo scambio.

Con il passare del tempo, in quasi tutti i paesi gli scambi avvennero in misura sempre più frequente attraverso l'uso di pezzi di metallo di uguale peso: le monete.

Con lo sviluppo e l'estensione dei commerci, le civiltà sentirono il bisogno di dimostrare il proprio potere sulle popolazioni adiacenti. Si cominciò quindi a porre sigilli e figure sulle monete. Queste, oltre che un oggetto di scambio, divennero anche una dimostrazione di economia fiorente, di prestigio e autorità.

Un'altra motivazione all'apposizione del sigillo era la fiducia: permetteva ad una terza parte fiduciaria (inizialmente mercanti e santuari, successivamente lo Stato) di garantire un dato peso e quantità di metallo, quindi garantirne il valore.

Nonostante questo, il valore dichiarato dalla terza parte poteva non essere del tutto veritiero, ma la comunità lo accettava senza timori come mezzo di scambio o riserva di valore, in quanto garantito da un organo fidato.

Un'altra funzione altrettanto importante è dunque la funzione di risparmio. La storia di quei beni che sono diventati denaro perché difficilmente censurabili nello scambio e difficilmente inflazionabili qualora venissero utilizzati per il risparmio, ha iniziato a convergere presto verso l'oro, che però nel corso della storia ha mostrato i suoi limiti: difficile da riconoscere, conservare, scambiare.

Gli strumenti che la società ha gradualmente adottato per riuscire ad aumentare la facilità di verifica e stoccaggio, sono strumenti che hanno sempre tenuto conto della creazione e affidamento in una terza parte fidata. Nel corso del tempo questa tendenza a servirsi di terze parti fidate è andata ad aumentare esponenzialmente, passando dalla girata, al cheque, alla lettera di cambio, tant'è che si è arrivati a vedere il denaro semplicemente come un foglio di carta, dal valore nominale di pochi centesimi, che vede nella terza parte fidata l'unico garante del suo valore.

La blockchain prima e Bitcoin poi nascono per eliminare questa componente di fiducia, una terza parte (mercante, santuario, banca, governo) con il potere di stabilire il valore di una moneta o quando e quanto si può scambiare.

Per millenni ci siamo abituati a dipendere da questo sistema di fiducia a tal punto che un sistema come quello blockchain suscita timore ed è difficile da immaginare nel nostro sistema. Un sistema che permette di fare qualsiasi scambio senza una terza parte è un sistema che potrebbe cambiare il mondo in modo travolgente.

2. BLOCKCHAIN

Descrivere la blockchain tramite un'unica definizione sarebbe complicato e risulterebbe poco chiaro, dal momento in cui essa può essere presentata da diversi punti di vista e prospettive.

Blockchain, che letteralmente significa “catena di blocchi”, è un grande registro digitale, riconducibile ad un libro mastro, in cui le voci sono raggruppate in blocchi concatenati in ordine cronologico, la cui integrità è garantita dall'uso della crittografia.

I blocchi contengono dati (transazioni e/o informazioni: trasferimento di denaro, scambio di messaggi, invio di un file...) la cui validazione è affidata ad un meccanismo di consenso, distribuito su tutti i nodi della rete nel caso delle blockchain pubbliche o su tutti i nodi autorizzati a partecipare al processo di validazione delle transazioni da includere nel registro nel caso di blockchain private.

Pensiamo alla blockchain come a un'enorme banca dati condivisa a cui possono essere aggiunti progressivamente nuovi blocchi. I dati sono dunque accessibili e distribuiti presso tutti i partecipanti della rete, senza necessità di un'autorità centrale.

Non bisogna confondere la blockchain come una tecnologia esclusivamente legata a Bitcoin o alle criptovalute. In realtà è il mondo delle criptovalute ad esistere e funzionare grazie al sistema di blockchain, e non viceversa. Il Bitcoin è un'applicazione, mentre la blockchain è il sistema tramite il quale possono funzionare molte altre applicazioni.

Esistono blockchain globali, come appunto quella di Bitcoin, e blockchain realizzabili per aziende, per una comunità separata o per un fine specifico.

Ogni blocco ha una capienza massima: una volta che il blocco viene riempito questo viene crittograficamente sigillato, chiuso, in modo che non possa più essere riaperto.

Una volta chiuso il sistema utilizza la cosiddetta “funzione di hash” ¹ che permette di trasformare un qualsiasi tipo di dato in una stringa alfanumerica e quindi di riassumere tutte le informazioni contenute nel blocco in un codice.

Chiuso un blocco si passa al successivo, dove vengono inserite delle nuove informazioni. Il primo dato che viene inserito nel nuovo blocco è il codice hash del blocco precedente e così avviene per tutti i blocchi successivi ².

La funzione di hash ha l'importante caratteristica di essere univoca: è possibile trasformare qualsiasi informazione in un codice, che sarà immutabile e dal quale non si potrà mai risalire alle informazioni che lo hanno generato.

Una funzione importante di questo codice è capire se è presente un'intrusione nel sistema. Le informazioni del blocco X generano il codice Y; se si provasse a modificare anche un solo dato al loro interno, aggiungendo, eliminando o cambiando

¹ L'hash è la colla che tiene insieme i blocchi. L'hashing serve infatti per collegare e condensare gruppi di transazioni in blocchi, oltre che per produrre collegamenti crittografici tra ciascun blocco, creando effettivamente una blockchain. In un certo senso, l'hash è ciò che conferisce un'identità unica ad ogni blocco. Se immaginiamo un blocco come un pezzo di puzzle, l'hash è ciò che ne definisce la forma, in modo che si possa agganciare solo al blocco cronologicamente precedente e successivo.

² Si dice catena di blocchi consequenziali e incatenati, perché ogni blocco può essere generato solo dopo la chiusura del blocco precedente e può essere generato solo se viene inserito il codice hash riassuntivo del blocco precedente.

qualche informazione (anche un dettaglio banale, come modificare un “grazie” in un “grazie!”) il codice hash cambierebbe totalmente, generando il cd. “effetto farfalla”³. Quindi un individuo per cambiare o manipolare un’informazione dovrebbe trovare il blocco nella quale questa è contenuta e riuscire a modificarla (premessi che sia tecnicamente possibile farlo), così facendo porterebbe al cambiamento di tutti i codici, il sistema si accorgerebbe della presenza di un’intrusione ed estrometterebbe l’individuo dalla blockchain.

Un’ulteriore caratteristica della blockchain è il fatto di essere condivisa e decentralizzata. La blockchain non risiede in un solo computer o server, non esiste in un punto fisso, ma è una copia infinita della catena di blocchi, presente su ogni dispositivo collegato a quella rete.

Nel caso della blockchain di Bitcoin, ognuno di noi potrebbe scaricarla sul proprio pc, in questo modo si scaricherebbe una copia di tutte le transazioni e informazioni che sono nate e evolute nella blockchain dal primo giorno (3 gennaio 2009) ad oggi.

Un ultimo aspetto fondamentale che emerge è dunque quello della sicurezza. Se un computer subisse un attacco hacker, questo non farebbe nessun danno alla blockchain ma solo a una copia della blockchain. Da quel momento il sistema si accorgerebbe che la copia del dispositivo attaccato è diversa da quella distribuita in tutti gli altri computer del mondo; essa sarà riconosciuta come corrotta, perché contenente informazioni e codici diversi da quelli degli altri; posizione che comporta l’estromissione dalla rete.

³ In matematica e fisica l’effetto farfalla è una locuzione che racchiude in sé la nozione tecnica di dipendenza sensibile alle condizioni iniziali. L’idea è che piccole variazioni nelle condizioni iniziali producano grandi variazioni nel comportamento a lungo termine di un sistema.

La blockchain è dunque una tecnologia sicura perché per hackerarla totalmente si dovrebbero attaccare contemporaneamente almeno il 50%+1 (ovvero la maggioranza) di tutti i dispositivi che la contengono ⁴.

Nell'ipotetico caso in cui si riuscisse ad attaccare la maggioranza dei nodi, la blockchain rilevarebbe due informazioni contrastanti: da una parte il 50%+1 dei dispositivi contenenti il codice X, dall'altra parte il 50%-1 contenenti codice Z. Basandosi su funzioni matematiche e algoritmiche il sistema si fiderebbe dunque di X, costituendo la maggioranza, anche se contenente informazioni manomesse.

Attaccare però il 50%+1 di tutti i nodi è spesso estremamente costoso in termini monetari, di tempo impiegato e capacità informatiche da applicare.

Prendendo come esempio la blockchain di Bitcoin, un attacco al 51%, senza considerare che è tecnicamente impossibile da attuare con le tecnologie attuali, richiederebbe un'enorme quantità di denaro e tempo ⁵.

La blockchain è dunque inattaccabile e crittograficamente sicura. L'opzione più conveniente è far parte del sistema e accettarne regole e condizioni, invece di provare a forzarlo.

⁴ Un attacco del 51% è un potenziale attacco a Bitcoin o altri network sulla blockchain, in cui una singola entità riesce a prendere il controllo della maggioranza dell'hash rate. L'attaccante avrebbe sufficiente potenza di mining da consentirgli di provare a invertire transazioni effettuate precedentemente, portando a un double-spending (truffa che consiste nello spendere lo stesso titolo valutario due o più volte). Un attacco di successo permetterebbe anche di impedire la conferma di alcune transazioni, o di impedire il mining di altri miners, portando al cd. "monopolio di mining".

⁵ Un attacco al 51% sulla blockchain di Bitcoin consumerebbe in energia elettrica un valore vicino al PIL di tutti i paesi del mondo messi insieme; provare a sottrarre dei soldi, quando per farlo se ne dovrebbero spendere più di quelli che si otterrebbero una volta concluso l'attacco, renderebbe l'azione priva di senso economico.

Nella blockchain di Bitcoin, per far funzionare questa catena di blocchi serve qualcuno che, in maniera informatica, con i propri dispositivi, possa controllare e verificare che le informazioni siano corrette, per poi inserirle nei blocchi. Questo lavoro viene svolto dai cosiddetti miners (termine che fa riferimento ai minatori di oro, in quanto, come questi si occupano di estrazione della materia prima, i miners “estraggono” bitcoin attraverso la potenza di calcolo dei loro dispositivi e dal quale ne ricevono ricompense).

I miners agiscono in una blockchain parallela dove raccolgono i dati che ogni utente vuole inserire nella blockchain (ad esempio Laura invia 5 bitcoin a Simona), leggono e analizzano i dati del trasferimento e controllano che questo possa effettivamente avvenire (nel nostro esempio che Laura detenga realmente 5 bitcoin e se Simona possa riceverli). Il miner, pertanto, interroga il sistema e chiede che vengano controllate tutte le informazioni dei blocchi precedenti, per verificare che quell'operazione possa andare a termine.

Tutte queste operazioni vengono effettuate automaticamente dal dispositivo o dispositivi che il miner utilizza, usando la loro forza computazionale.

In conclusione, i nostri bitcoin (o le nostre proprietà o i nostri dati) sono asset digitali stabiliti solo e unicamente dalla condivisione di tutte le transazioni. Non c'è un posto fisico o fisso dove risiedono, ma in tempo reale vengono controllate tutte le informazioni precedenti e si è a conoscenza che in quel preciso istante si è proprietari di quel preciso asset.

Con la blockchain non si sta parlando solo di soldi ma di dati, informazioni. Fino a pochi anni fa abbiamo sempre dato valore agli scambi commerciali, cioè allo scambio di moneta. Oggi l'evoluzione tecnologica ci permette di cambiare prospettiva, sostituendo i metalli preziosi, la moneta o un organo centrale che ci dice quanto questa valga o quando debba essere stampata, con una struttura alla portata di tutti che permette di conoscere un valore a cui tutti hanno accesso: i dati.

Le informazioni che scambiamo, sono il valore stesso di quello scambio. È un qualcosa di difficile da comprendere e paradossalmente banale, una cosa mai successa prima nella storia dell'uomo. Qualcosa che sarà per forza una rivoluzione che cambierà il modo di pensare del pianeta.

3. BITCOIN

La strada che ha portato alla nascita di Bitcoin non è stato un avvenimento improvviso e inaspettato, come si potrebbe pensare, ma è stata costruita sulle idee di tante persone per diversi anni.

Bitcoin deve la sua nascita ad un movimento nato negli anni '90 chiamato Cypherpunk, formato da gruppi di attivisti politici e della privacy digitale. La loro missione era utilizzare la tecnologia e la crittografia per creare un denaro digitale che fosse decentralizzato e anonimo, come l'oro o il denaro contante, ma aggiornato al mondo di internet. Sognavano uno scambio di valore non censurabile, non controllabile e non manipolabile, che potesse essere scambiato da persona a persona facilmente, velocemente e a bassi costi.

In quegli anni, nei forum di Cypherpunk, circolavano diversi esperimenti su varie forme di denaro digitale. Adam Back, ricercatore britannico, creò hashcash, che in seguito divenne un componente centrale del protocollo Bitcoin. Wei Dai, ingegnere informatico, ne progettò un altro chiamato b-money. Nel 1998 Nick Szabo, informatico e crittografo, inviò il suo progetto di denaro digitale chiamato bit gold a un piccolo gruppo di persone interessate tra cui Wei Dai e Hal Finney (quest'ultimo fu sviluppatore e ingegnere informatico, aiutò Satoshi Nakamoto a migliorare il software Bitcoin nell'autunno del 2008, prima che venisse rilasciato).

Il concetto dietro bit gold era molto simile a bitcoin: un token digitale scarso come l'oro, che poteva essere inviato elettronicamente senza dover passare attraverso un'autorità centrale come una banca.

Dietro lo pseudonimo di Satoshi Nakamoto si nasconde il creatore di Bitcoin, che nell'autunno del 2008 pubblicò online un documento (cd. "white paper") dove dichiarava di aver creato un sistema di pagamento che non avesse bisogno di banche, capace di superare qualsiasi limite geografico e politico, immune all'inflazione e basato su un protocollo. Ancora oggi non si conosce la sua vera identità, o se dietro vi si nasconda un gruppo di persone o un solo individuo.

Nel 2009 lanciò definitivamente questa tecnologia. Il rilascio fu comunicato esclusivamente via e-mail su "The Cryptography Mailing List", nel sito "metzdowd.com" e tramite e-mail private ad Adam Back, Wei Dai e Hal Finney.⁶

Nel 2011, proprio quando la tecnologia iniziò ad attirare una maggiore attenzione, le e-mail si interruppero. Improvvisamente Satoshi scomparve senza lasciare tracce; non si ebbero sue notizie nemmeno nel 2016, quando venne proposto per la nomina al premio Nobel in Economia.

⁶ Nonostante non contasse di grandi numeri, la community era molto forte e unita. La nascita e gli sviluppi di Bitcoin sono anche merito di tutte le persone che con il tempo e proprie conoscenze hanno dato un apporto a questa tecnologia. La community si è gradualmente ampliata e ancora oggi migliaia di persone lavorano ogni giorno per contribuire al protocollo.

Bitcoin – codice BTC – è la prima criptovaluta mai inventata basata su blockchain; è la prima applicazione riuscita di questa innovazione e la prima tecnologia che ha reso possibile lo scambio di valore tra persone senza bisogno di un intermediario.

È la più popolare e la più capitalizzata sul mercato. Ha ispirato tutte le criptovalute create in seguito, chiamate per questo “altcoins”, da “alternative coins”.

La frazione più piccola in cui si può dividere un bitcoin viene chiamata satoshi, in onore di Satoshi Nakamoto. Nello stesso modo in cui un euro è divisibile in 100 centesimi, un bitcoin è divisibile in 100,000,000 satoshi; la frazione minima è dunque 0,00000001.

Bitcoin arriva in un mondo dove non era minimamente immaginabile una sua esistenza, dove nessuno si aspetta di fare guadagni o speculare. I primi sviluppatori non erano persone che sognavano di comprare una Ferrari facendo trading, ma nerd da garage che cercavano di fare qualcosa di eccezionale ed unico per la comunità. Le idee si sono poi diffuse gradualmente, in maniera organica e senza aspettative. Bitcoin è il coronamento della passione, sforzi e idee di tanti sognatori ⁷.

Come già spiegato in precedenza, la blockchain funziona grazie a dati che vengono verificati, autenticati e inseriti nei blocchi dai miners, attraverso i loro dispositivi.

⁷ Ci son stati dei tentativi precedenti di creare qualcosa di simile a Bitcoin ma furono concentrati nelle mani di alcune società. Ad esempio, Paypal cercò di creare un nuovo tipo di denaro che fosse completamente privato e non manipolabile. Il problema è che queste società sono facili da bloccare e potenzialmente sanzionabili. Con Bitcoin si è riusciti ad evitare questo problema e ormai la sua ascesa non è arrestabile.

Tali dispositivi devono essere costantemente accesi ed efficienti, quindi i miners sostengono costi di elettricità e di hardware; non meno importanti sono il tempo e le conoscenze impiegate. Il sistema, come “ringraziamento” per credere in questa tecnologia, il suo progetto e i suoi scopi, li incentiva, ricompensandoli in bitcoin. La ricompensa è proporzionata a quanta potenza computazionale un individuo dà al sistema.

La formula di emissione di Bitcoin è ben scandita: ogni 10 minuti viene creato un nuovo blocco e con esso la ricompensa totale in bitcoin, divisa tra tutti quelli che hanno contribuito al funzionamento della rete. L'emissione di btc corrisponde alla chiusura del blocco.

L'algoritmo calcola la potenza totale a disposizione della rete e livella la complessità del calcolo da compiere per poter chiudere un blocco, facendo in modo di chiuderlo ogni 10 minuti. Non importa quindi quante informazioni ci siano, quante di queste siano vere, false o complesse, ogni 10 minuti il blocco viene chiuso e si passa al successivo. Se la potenza computazionale messa a disposizione della rete aumenta, la difficoltà dell'algoritmo da risolvere si innalzerà, al contrario si abbasserà.

Il primo blocco di una catena blockchain è noto come Blocco di Genesi; quello di Bitcoin è avvenuto il 3 gennaio 2009. Satoshi Nakamoto decise di enfatizzare questo evento scrivendo un messaggio all'interno dell'unica transazione presente nel blocco: “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”.

La frase si riferisce al titolo di un articolo del 3 gennaio 2009 del Times, traducibile in: “Il cancelliere ipotizza un secondo salvataggio per le banche”.

All'epoca si era infatti in piena crisi finanziaria e con questo commento probabilmente volle lasciare un segno nella blockchain su uno degli stimoli che lo spinsero a creare Bitcoin, una sorta di inaugurazione della nascita di una nuova politica monetaria.

I primi blocchi chiusi generavano ognuno 50 bitcoin, ogni 4 anni la formula dimezza la ricompensa: 25 nel 2013, 12,5 nel 2017, 6,25 oggi, fino ad arrivare a 0 più o meno nel 2136 quando si raggiungerà il 21milionesimo btc. Questo rende btc un asset che si deflaziona, aumentando il valore anno dopo anno, a parità di domanda.

Il valore di bitcoin non è stato stabilito al momento della sua creazione, né risente dell'inflazione, dell'economia di uno Stato, delle scelte di un governo o delle decisioni di una banca centrale, ma il suo valore deriva dal prezzo che il mercato gli riconosce. Come qualsiasi asset scarso, più persone sono disposte a comprarlo, tanto più il suo costo aumenta. A guidare il suo prezzo è quindi la legge della domanda e dell'offerta.

Satoshi stabilì un massimo di 21 milioni di bitcoin, con l'idea che la limitata disponibilità avrebbe garantito scarsità e una maggiore stabilità del suo valore.

Fino ad ora sono stati estratti circa 19 milioni di bitcoin e il prezzo è passato da 0 agli attuali 56.000\$ (dati al 29 Marzo 2021). La capitalizzazione di mercato complessiva è quindi passata da 0 a 1 trilione di dollari in circa 12 anni.

Va sottolineato che l'aumentare del valore di bitcoin non ha disegnato un arco di crescita costante; la sua volatilità ha spinto il suo prezzo (e lo spinge tuttora) a dei picchi di valore molto alti e molto bassi. Tuttavia, dalla sua nascita ad oggi, il suo valore è cresciuto più di qualsiasi altro asset.

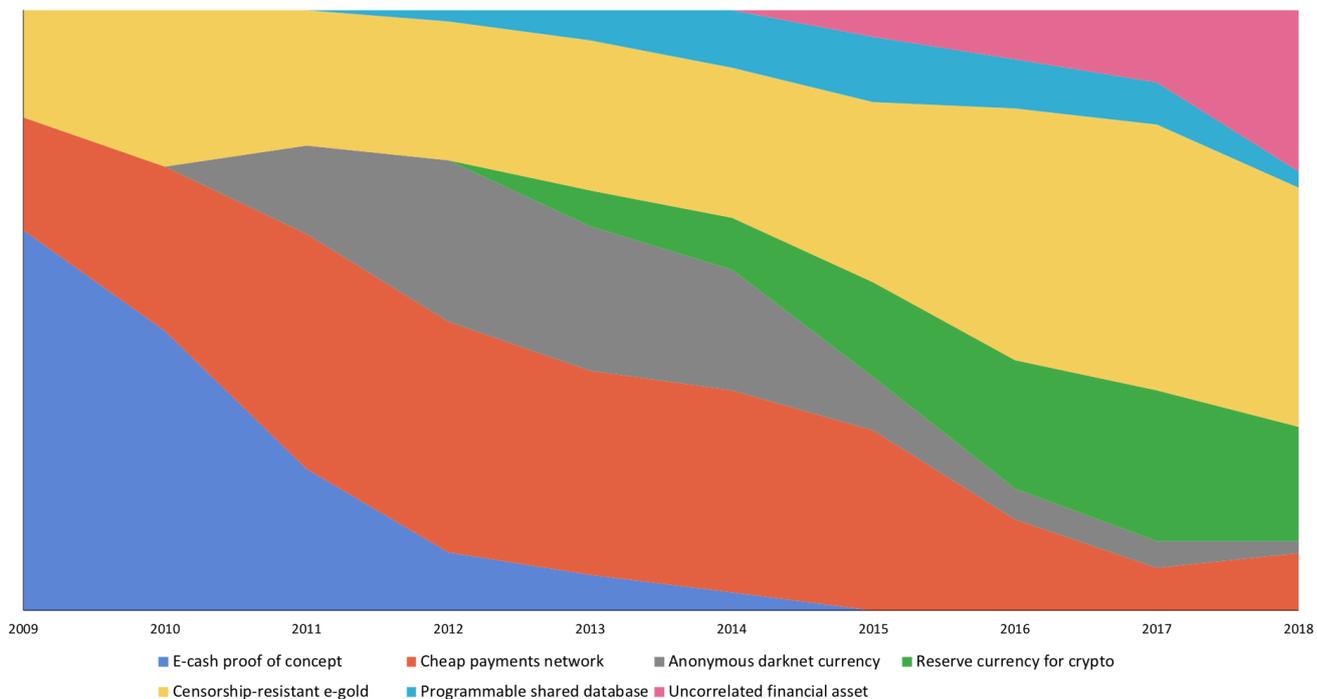
Qua si può vedere la crescita percentuale del prezzo di bitcoin, da Luglio 2018 ad Aprile 2021, paragonata con altri indici. ⁸



	FTSE MIB	+ 15,14%	(indice della borsa di Milano)
	XAU	+ 33,05%	(oro)
	S&P500	+ 63,98%	(500 aziende USA a maggior capitalizzazione)
	Amazon	+ 207,49%	
	Bitcoin	+ 2530,81%	

⁸ Fonte: <https://it.tradingview.com/chart/>

Anche la percezione e i pensieri delle persone su cosa rappresenti Bitcoin sono cambiati e maturati nel corso degli anni: ⁹



Nonostante l'entusiasmo intorno a Bitcoin come potenziale strumento di pagamento del futuro, dal 2018 ad oggi si è consolidato maggiormente come bene rifugio¹⁰ e forma di investimento, fino a diventare un vero e proprio asset finanziario. Sta crescendo anche la narrativa, spesso fuorviante, che lo vede come un sistema troppo energivoro.

Si sono invece indebolite quelle idee che vedevano bitcoin come moneta del darknet o usata dai truffatori e come rete di pagamento economica.

⁹ Fonte: https://medium.com/@nic__carter/visions-of-bitcoin-4b7b7cbcd24c

¹⁰ Quel tipo di bene su cui le persone investono o ripongono i propri risparmi, soprattutto in momenti di contrazione economica. Per questo il mercato ha ribattezzato Bitcoin come oro digitale.

La crescente fiducia nella sua tecnologia ha portato gli investitori a considerarlo un investimento a medio-lungo termine. A consolidare questa posizione, infatti, Bitcoin sta ottenendo grandi investimenti di fondi istituzionali; in tanti si sono già mossi per investire parte delle proprie risorse in questo asset (tra i più famosi MicroStrategy, Tesla, Galaxy Digital Holdings, Grayscale, BlackRock).

Il raggiungimento di una regolamentazione chiara nei prossimi mesi potrebbe sancire la consacrazione di Bitcoin come nuovo asset di investimento ufficialmente riconosciuto.

Di tutte le criptovalute, Bitcoin è la più longeva, forte e sicura. In 12 anni ha risposto alle crisi economiche (2008, 2012 e periodo covid 2020) mostrando anticorpi resistenti e passando il test del tempo.

4. CASI D'USO DELLA BLOCKCHAIN

4.1 Disinformazione e innovazioni

Negli anni in cui i primi computer diventavano accessibili al pubblico, il loro utilizzo era molto complesso per un utente sprovvisto di conoscenze informatiche. Mancava un'interfaccia grafica semplice, dotata di strumenti che eliminassero la necessità di apprendere competenze specifiche. Questo limitava le potenzialità della tecnologia e i modi in cui poteva essere utilizzata.

La tecnologia blockchain e le criptovalute stanno attraversando un periodo simile: essendo ancora in fase di definizione, con continui e rapidi sviluppi, può capitare che l'interazione dell'utente avvenga tramite procedure macchinose che il più delle volte richiedono l'apprendimento di nuove competenze.

Spesso, inoltre, ci si affida alle analisi estremamente semplificate dei media o ad opinioni circolanti sui social, che portano ad una comprensione parziale o sbagliata dell'argomento, impedendo di afferrarne il reale potenziale.

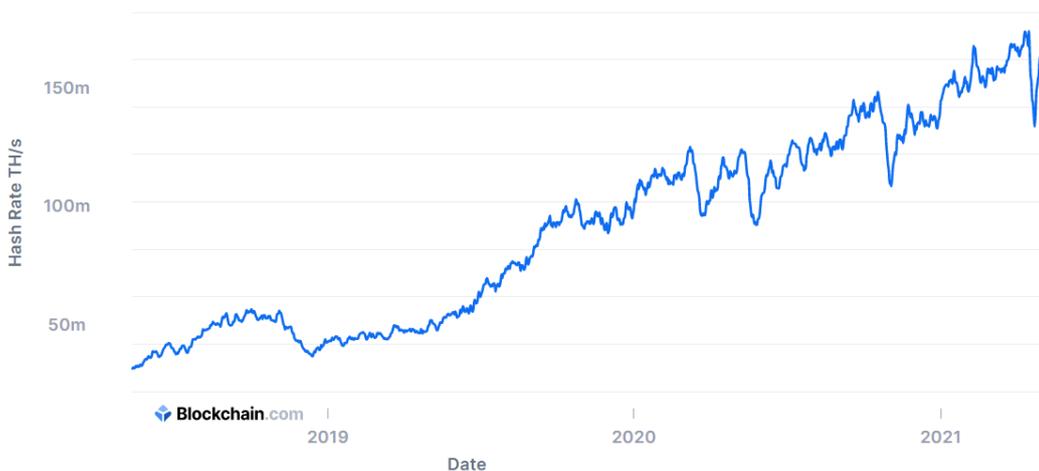
In Italia c'è molta disinformazione sia nell'opinione pubblica che nella divulgazione dei media, che il più delle volte si limitano a una trattazione delle criptovalute solo di natura speculativa. È raro sentir parlare delle ragioni per cui è nato un progetto, delle caratteristiche della sua blockchain e del modo in cui aiuterebbe a risolvere un problema. Per esempio, se le uniche notizie divulgate su Apple fossero quelle relative al suo valore in borsa, un lettore non sarebbe in grado di associarla all'iPhone o ad altri prodotti perché non ne avrebbe mai sentito parlare.

In generale, si sente spesso che le criptovalute siano sinonimo di truffa, o di come queste siano il mezzo preferito dai criminali per riciclare denaro. L'assenza di intermediari finanziari, unito alla natura "pseudo-anonima" delle transazioni, può favorire operazioni di riciclaggio, in quanto non è presente un organismo che funge da controllore e segnalatore di attività sospette alle autorità competenti, ma blockchain e criptovalute non nascono per favorire tali comportamenti. Questi, infatti, sono praticabili tramite qualsiasi forma di scambio di valore. Le criptovalute e la loro tecnologia, al contrario, possono essere una possibile soluzione a questi problemi.

Alla luce di queste considerazioni, occorre chiedersi come mai una tecnologia a cui si attribuisce un potenziale tanto elevato abbia finora trovato applicazioni tanto limitate. Un primo problema è che la blockchain, come spiegato in precedenza, essendo un complesso network di computer, consuma una grande quantità di energia elettrica. Nel grafico si vede l'andamento dell'hash rate di Bitcoin, ossia il numero di calcoli al secondo necessari per processare le transazioni. Il trend positivo di crescita si traduce in un maggior consumo di energia elettrica.

Total Hash Rate (TH/s)

The estimated number of terahashes per second on the bitcoin network

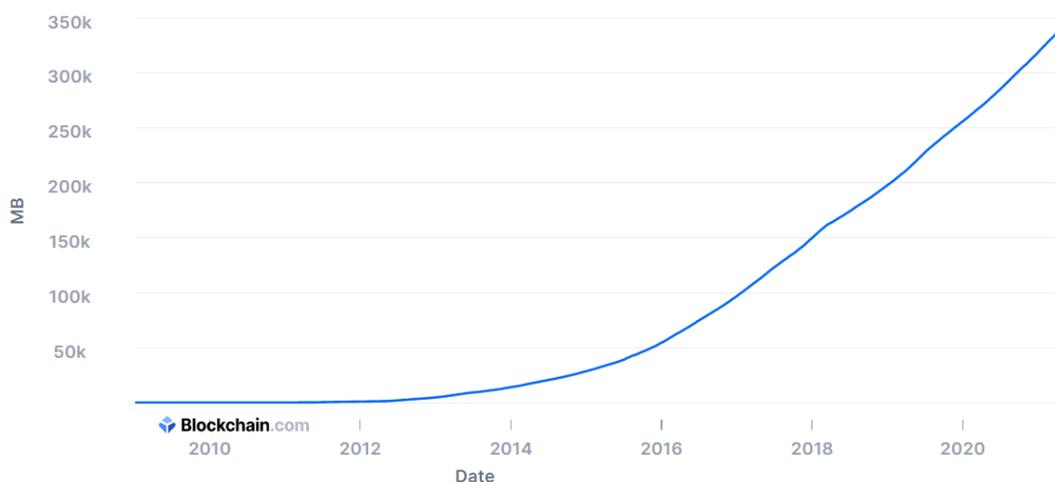


Un secondo problema è che il sistema diventa sempre più complesso all'aumentare di nuovi utenti, perciò sempre più lento nell'effettuare i controlli per la scrittura dei nuovi blocchi. Un terzo problema è che esistono limiti fisici dovuti alla capacità di gestione delle informazioni. Queste non vengono mai cancellate una volta inserite nella blockchain, perciò è lecito domandarsi fino a quando sarà possibile inserire nuovi blocchi alla catena, e quanto spazio di archiviazione sarà necessario per supportare la crescita del network.

Ad esempio, nel 2012 la dimensione della blockchain di Bitcoin su ogni nodo era di circa 216 MB, contro gli oltre 360 GB del 2021.¹¹ La necessità di strumenti hardware aggiuntivi potrebbe limitare le potenzialità di sviluppo della blockchain.

Blockchain Size (MB)

The total size of the blockchain minus database indexes in megabytes.



¹¹ Grafico al 11/05/2021 – fonte “Blockchain.com”

Al tempo stesso sappiamo che le informazioni non vengono mai cancellate una volta inserite nella blockchain e questo potrebbe creare problemi. Si pensi ad una legge inserita oggi ma che fra qualche anno potrebbe richiedere una modifica o la cancellazione. Si dovrebbe cercare una soluzione in modo che un nuovo blocco, contenente una modifica, vada ad annullare o “aggiornare” il blocco precedente; cosa che al momento risulta difficile da applicare.

Ad oggi, i lati negativi vengono spesso estremamente esaltati e sono tali da limitarne la diffusione, ma ciò non significa che in un immediato futuro non potranno esserci le condizioni per una più facile applicabilità di questa tecnologia, date da una maggiore sostenibilità ambientale e temporale per la parte hardware, evoluzioni nella sicurezza informatica e un’evoluzione nei pregiudizi delle persone su questi temi.

4.2 La blockchain nell'Unione Europea

L'aspetto rivoluzionario di questa tecnologia non si limita solo all'aspetto finanziario, ma può avere anche altre applicazioni. Per questo motivo, c'è grande attenzione sul tema, con rilevanti investimenti da parte di banche, imprese, e Stati.

La ragione principale che spinge molti Stati a scommettere sullo sviluppo di applicazioni blockchain è quella di raccogliere, verificare e condividere dati in modo sicuro, trasparente e nel rispetto delle regole di riservatezza.

Secondo l'Osservatorio europeo sulla blockchain¹², tale tecnologia è utile per risolvere alcuni problemi nei rapporti con le pubbliche amministrazioni come fiducia, trasparenza e sicurezza.

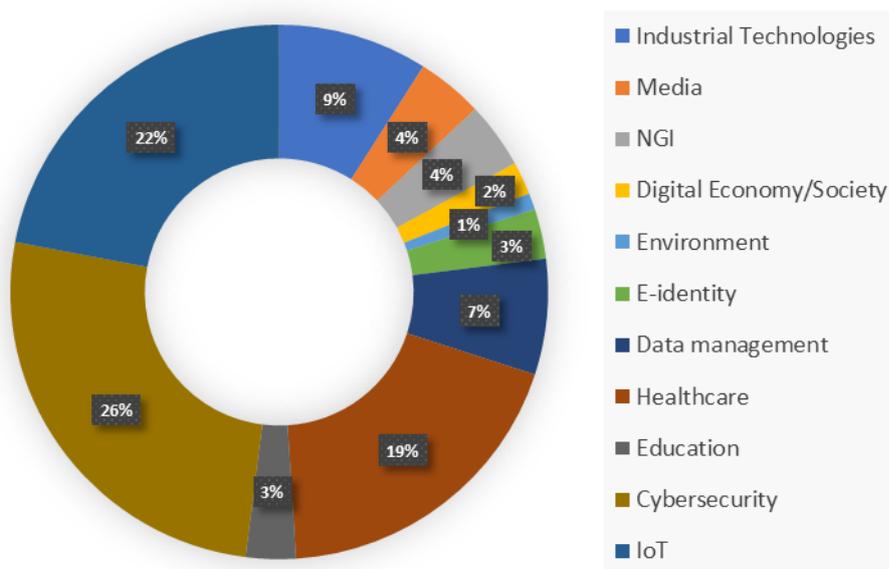
La blockchain può dunque rappresentare un passo importante per la digitalizzazione e rinnovamento delle Pubbliche Amministrazioni. Potrebbe portare ad una riduzione dei costi e degli sprechi di tempo. Inoltre, la condivisione di dati, sia nei rapporti intra-governativi che fra il pubblico e i privati, porterebbe ad una riduzione della complessità burocratica e della distanza tra i cittadini e le istituzioni. Per le imprese, invece, un database condiviso può aiutare nei rapporti con lo Stato per quanto riguarda la semplificazione degli adempimenti formali.

¹² Organo creato dalla Commissione Europea al fine di monitorare e creare conoscenza sulle iniziative blockchain in Europa.

Da Febbraio 2019, l'Unione Europea ha investito oltre 340 milioni di euro per lanciare progetti col fine di migliorare l'efficienza del settore pubblico attraverso sistemi di blockchain.

I settori nei quali la Commissione ha indirizzato gli investimenti sono vari: gestione dell'identità personale dei cittadini, tassazione, voto digitale, gestione del sistema pensionistico e dei certificati universitari.¹³

Blockchain EU funded projects per sector and future technologies



¹³ <https://www.fasi.biz/it/notizie/novita/20920-blockchain-a-quali-progetti-sono-andati-i-fondi-europei.html>

4.3 Il possibile ruolo nella Pubblica Amministrazione

La pubblica amministrazione è da sempre affetta da una necessità di snellimento, semplificazione e maggior interoperabilità con i cittadini. La blockchain consente di ripensare i sistemi di informazione, promuovere la fiducia degli utenti e creare nuove opportunità prestazionali.

Rispetto a questa tecnologia la P.A. può essere un soggetto attivo, cioè operare come un “motore”, mettendo a disposizione della comunità dati da condividere, oppure essere un soggetto passivo, cioè fruire della blockchain per fornire servizi in modo più rapido ed efficiente.

La blockchain può aiutare a garantire la standardizzazione, l'immutabilità dei dati e la loro sicurezza. Di conseguenza porterebbe alla riduzione di contenziosi sulle transazioni e a perfezionare l'automazione dei processi, migliorando la produttività complessiva del sistema pubblico. La principale caratteristica è quella di ridurre il costo della fiducia necessario al perfezionamento di una transazione, intesa come scambio informativo o di valore, garantendo al tempo stesso certezza della sua esecuzione. In quei contesti in cui il costo della fiducia è una componente rilevante del costo transazionale, queste tecnologie possono ridurre inefficienze e semplificare i livelli di intermediazione.

In queste considerazioni il riferimento va a quella che viene chiamata blockchain “permissioned”¹⁴. Al contrario, la versione pura o “aperta” della blockchain risulta poco utile per impieghi pubblici.

Per promuovere un alto livello di adozione e allocare le risorse finanziarie per lo sviluppo dei progetti, occorre chiarire quale blockchain favorire in ambito pubblico e per quali finalità. Tutti aspirano ad un’amministrazione dotata di alto grado di automazione e interconnessione, occorre però evitare un impiego non controllato della blockchain con rischi di frammentazione tra le singole esperienze pubbliche. Qualora essa fosse utilizzata ricorrendo a protocolli non comunicanti tra loro, se ne avrebbe uno sviluppo significativamente circoscritto, fine a sé stesso.

Nel Piano Triennale elaborato dal Team per la Trasformazione Digitale e l’Agenzia per l’Italia Digitale si sconsiglia l’utilizzo della blockchain alle autorità pubbliche, in particolare se messa a raffronto con i database centralizzati. Al contrario l’iniziativa europea si muove in una direzione diversa.

¹⁴ Le blockchain permissioned, dette anche “chiuse” o “private”, usano un layer di controllo degli accessi per controllare chi accede alla rete. Sono quindi caratterizzate da un accesso alla rete ristretto ad alcuni partecipanti autorizzati e da un processo di validazione assegnato ad un gruppo ristretto di attori. Le regole che riguardano la definizione dei soggetti coinvolti, le modalità di introduzione dei dati e il modo di risolvere eventuali controversie vengono stabilite convenzionalmente.

È stato istituito l'European Blockchain Service Infrastructure (EBSI)¹⁵, con l'obiettivo di realizzare servizi pubblici a livello europeo basati su blockchain.

Lo sviluppo di un'infrastruttura blockchain europea consentirebbe di condividere in modo sicuro alcune informazioni, come quelle sui dati doganali e fiscali dei Paesi dell'Unione, documenti di audit di progetti finanziati da agenzie europee, certificazioni notarili o certificazioni transfrontaliere di diplomi, qualifiche personali, identità digitali, atti catastali, brevetti e cartelle cliniche.

Un altro impiego possibile è relativo al contrasto alla corruzione. La corruzione presuppone l'opacità amministrativa e tale tecnologia al contrario può rendere più trasparenti le procedure, in particolare nel settore dei contratti pubblici di servizi.

Il mantenimento dell'anonimato dell'offerente, la stabilità delle informazioni di gara circolanti e la maggiore efficienza nei controlli incrociati di legalità sui partecipanti alla procedura di appalto, sono tutti elementi che sono agevolmente assicurabili tramite l'utilizzo della blockchain, consentendo di realizzare una strategia di contrasto al fenomeno corruttivo nel settore specifico degli appalti pubblici. In questi campi di interesse amministrativo, insomma, potrebbero essere fornite soluzioni informatiche in grado di rimediare o ridurre alcune inefficienze.

¹⁵ Come riportato sul sito della Commissione Europea: "EBSI consiste in una rete di nodi interconnessi che eseguono un'infrastruttura di servizi basata su blockchain. Ciascun membro della European Blockchain Partnership (i 27 Stati membri dell'UE, Norvegia, Liechtenstein e Commissione europea) gestirà almeno un nodo.

L'infrastruttura è composta da diversi livelli tra cui: un livello base contenente l'infrastruttura di base, la connettività, la blockchain e lo storage necessario; un livello di servizi di base che consentirà tutti i casi d'uso e le applicazioni basati su EBSI; livelli dedicati a casi d'uso e applicazioni specifiche.

Consentirà alle organizzazioni pubbliche (ed eventualmente anche private) di sviluppare applicazioni che si connettono e utilizzano l'infrastruttura EBSI."

Un'indicazione più precisa sembra provenire dall'ultimo decreto semplificazioni, con riferimento a "tecnologie basate su registri distribuiti", in cui la blockchain è individuata come base tecnologica da cui derivare un miglioramento della comunicazione tra pubblica amministrazione e utenza.

Sebbene sia evidente il riconoscimento del legislatore sull'importanza di tali tecniche, permangono alcune criticità. In primo luogo, sembra mancare un'architettura infrastrutturale di riferimento all'interno della quale implementare la tecnologia blockchain. In secondo luogo, è carente la regolamentazione giuridica con il rischio di trascurare l'obiettivo dell'interoperabilità, ritenuto uno dei fattori chiave per garantire una effettiva digitalizzazione. Infine, l'attuale regime normativo "facoltizza, ma non obbliga le autorità pubbliche a rendere disponibili sulla piattaforma digitale i propri atti", con il rischio di frenare l'innovazione per la pigrizia di rivoluzionare un assetto sicuramente consolidato.

L'impiego della blockchain da parte di soggetti pubblici è dunque fonte di dilemmi; a seconda di come si inquadra il fenomeno, si può essere portati a dare maggior peso all'aspetto protettivo, scoraggiandone l'uso a favore di altre soluzioni, o a privilegiare l'aspetto innovativo e le sue potenzialità, incentivandone l'uso.

4.4 Una potenziale rivoluzione tributaria

In uno studio di “Pwc”, si discute su “come la blockchain potrebbe divenire un possibile mezzo nel passaggio di ripensamento dei meccanismi di tassazione; non una soluzione in sé, ma utile per la transizione a nuovi meccanismi di tassazione nell'economia digitale”.

Dal report emerge che i contribuenti e la società in generale, hanno un necessario bisogno di ripristinare la fiducia nel sistema fiscale e la blockchain rappresenta proprio lo strumento atto a rimarginare la “tradizionale contesa” tra fisco, contribuenti ed evasori.

“L’art. 53 della Costituzione nella sua prima parte recita: «Tutti sono tenuti a concorrere alle spese pubbliche in ragione della loro capacità contributiva».

L’art. 1 del Dpr 917/1986 si esprime in tal modo: «Presupposto dell’imposta sul reddito delle persone fisiche è il possesso di redditi in denaro o in natura rientranti nelle categorie indicate nell’articolo 6».

Quindi ciò che fa scaturire l’obbligo di contribuzione alle pubbliche spese, è indicato nel c.d. “possesso di redditi”. Nel nostro sistema tributario il concetto di reddito è quindi indicato come “prodotto” riconducibile ad un’attività o ad un atto di gestione produttivo di un incremento patrimoniale. Nel momento in cui un soggetto svolge un’attività che gli porta un incremento di ricchezza, su tale incremento viene parametrata l’imposizione fiscale.

Secondo altri, il concetto di reddito dovrebbe essere inteso come “spesa-consumo”, ossia si definisce quale sia la capacità contributiva di un soggetto in base a quanto esso spenda per l’acquisto di beni o servizi.

In base a questa teoria, per operare una potenziale rivoluzione del sistema tributario, occorre preliminarmente introdurre una moneta digitale, sostitutiva del denaro contante, e registrare gli scambi della stessa su un sistema blockchain creato a tale scopo¹⁶. Andrebbe poi modificata la concezione legislativa di reddito, attualmente inteso come “prodotto”, passando ad una concezione di reddito inteso come “spesa-consumo”.

In questo modo ogni acquisto sarà immediatamente visibile, seppur crittografato, sulla blockchain e la spesa compiuta sarà dunque evidente. Da ciò deriva direttamente la possibilità di ricostruire in termini chiari e senza dubbi quantitativi il reddito, rendendo in tal modo impossibile ogni tentativo di occultamento della base imponibile.

¹⁶ La Banca Centrale Europea ha già pubblicato un rapporto "A digital euro", su quella che probabilmente sarà la prima moneta digitale dell'Eurozona.

L'euro digitale non sarà altro che l'equivalente dell'euro cartaceo ma in un formato virtuale. Un modo per abbracciare l'innovazione tecnologica finanziaria e avvicinarsi al mondo delle blockchain. Il termine tecnico è CBDC (Central Bank Digital Currency).

L'intera infrastruttura verrà controllata e gestita dalla BCE, basandosi su un registro pubblico, simile alla blockchain. L'euro digitale verrà immesso dalla BCE direttamente nelle tasche dei cittadini, tramite un wallet (portafoglio) digitale.

I motivi che spingono alla sua creazione sono principalmente 3:

- Fungere da alternativa alle banconote fisiche.
- Riduzione dei costi: il sistema di scambio di euro attuale ha dei costi impliciti relativamente alti.
- Alternativa alle criptovalute private: già da diversi anni esistono criptovalute che replicano l'euro o il dollaro, le cd. “stablecoin”. Queste fanno concorrenza alle valute tradizionali e per questo sono mal viste. Ad esempio, Tether (USDT) ha un volume di scambio giornaliero di circa 55 miliardi di dollari ogni giorno.

4.5 Blockchain e misurazione dell'orario di lavoro

Il tempo della prestazione, nel rapporto di lavoro subordinato, costituisce il parametro con cui determinare l'oggetto dello scambio contrattuale.

La direttiva n. 2003 / 88 rimette agli Stati membri il compito di adottare le "misure necessarie" per garantire il rispetto di periodi minimi di riposo e del limite massimo settimanale del lavoro. Alla luce delle condizioni di debolezza in cui versa il lavoratore, deve essere impedita ogni condotta potenzialmente lesiva da parte del datore. Di conseguenza, per proteggere la sicurezza e la salute dei lavoratori, diventa essenziale predisporre un sistema in grado di stabilire il numero delle ore lavorate e la loro collocazione nel tempo, in maniera affidabile ed accessibile; a tal fine si potrebbe utilizzare la blockchain.

Nell'ordinamento italiano, l'istituto deputato a registrare l'orario di lavoro è da ricercare nel libro unico del lavoro, introdotto dal d.l n. 112/2008. Tra gli obblighi di scritturazione a cui è tenuto il datore di lavoro privato rientra il calendario delle presenze, dal quale deve risultare "per ogni giorno, il numero di ore di lavoro effettuate da ciascun lavoratore subordinato, nonché l'indicazione delle ore di straordinario, eventuali assenze, ferie e riposi".

Con il d.lgs n. 151 del 2015, nel quadro della complessiva riforma cd. "jobs Act", il legislatore aveva previsto un'importante novità: il libro unico del lavoro si sarebbe dovuto tenere in modalità telematica presso il Ministero del Lavoro.

Le resistenze sollevate dagli operatori del settore, a causa delle temute difficoltà esecutive nella compilazione, hanno portato prima a posticipare l'entrata in vigore della disposizione, poi alla sua definitiva abrogazione. La dematerializzazione di tale adempimento avrebbe però consentito una sua più agevole consultazione, nonché una riduzione degli errori, dei tempi e dei costi nella gestione documentale.

A questi fini sarebbe particolarmente efficace il ricorso alla tecnologia blockchain. Essa, infatti, per le sue caratteristiche strutturali, garantisce la trasparenza delle operazioni e la riservatezza dei contenuti.

Servirsi della blockchain impone di valutare il suo rapporto con la disciplina sulla protezione dei dati personali, bilanciandolo con la loro libera circolazione.

Nel corso degli anni, al crescere della consapevolezza sul valore da attribuire ai dati personali, si è accompagnata una graduale evoluzione nel Regolamento UE 2016/679. La libera circolazione dei dati costituisce il presupposto per sviluppare il mercato digitale europeo e il legislatore ha cercato di bilanciare questa esigenza con quella della loro protezione.

Tuttavia, alcune caratteristiche della blockchain sollevano problemi di coerenza con la normativa privacy. La distribuzione diffusa nei vari nodi delle informazioni personali contrasta con il principio di minimizzazione, esponendo l'interessato a rischi potenziali di trattamenti indiscriminati. Inoltre, la disintermediazione si pone in conflitto con la necessaria individuazione di titolare e responsabile del trattamento, figure chiave sulle quali fa perno l'intero Regolamento 2016/679.

Considerati questi aspetti, un modo per superare questi limiti potrebbe essere quello di adottare una blockchain permissioned (che in questo caso potrebbe essere composta da datori, lavoratori, enti previdenziali, amministrazione fiscale e organi di vigilanza, costituendo ciascuno un nodo). La sua struttura centralizzata permetterebbe di far coincidere il titolare con il soggetto che stabilisce chi può accedervi, garantendo una maggiore sicurezza a beneficio di tutti i partecipanti alla rete e del sistema nel suo complesso. Inoltre, adottando soluzioni di “*privacy by design*”, il titolare del trattamento potrebbe controllare i propri dati e selezionare i soggetti autorizzati alla loro elaborazione.

Alcuni dei profili più caratterizzanti della blockchain, tuttavia, sarebbero esclusi e resterebbe un sistema centralizzato che gode di una sicurezza rafforzata.

Per tutelare la sicurezza e salute del lavoratore gli Stati hanno l'obbligo di imporre ai datori di predisporre un sistema oggettivo di misurazione della durata dell'orario giornaliero. Nell'ottica interna, la misurazione datoriale è vincolata al rispetto della duplice condizione di un'adeguata informativa e della conformità alla normativa privacy.

Alla luce di ciò il legislatore può offrire l'occasione per implementare ed utilizzare la tecnologia blockchain.

4.6 Blockchain come strumento di certificazione

La verificabilità dell'effettiva esistenza e validità delle certificazioni è un fattore cruciale per assicurare la regolarità di alcune procedure e permettere di godere di benefici connessi a tali certificazioni.

Per quanto riguarda l'istruzione, in Italia i soggetti che erogano titoli di studio con valore legale sono prevalentemente istituzioni statali. In Unione Europea o fuori dall'UE altre nazioni adottano sistemi diversi.

La costante circolazione di studenti e lavoratori nel mondo richiede l'esigenza di accordi sul mutuo riconoscimento dei titoli di studio, minimizzandone gli aspetti burocratici e di verifica.

Per la formazione, invece, esistono molteplici soggetti titolati ad erogare servizi di formazione, prevalentemente di natura privata, con più complessità di verifica.

Nell'attuale regime basato essenzialmente sulla multilateralità e sul documento cartaceo ci sono principalmente due criticità:

- La verifica è complessa e potenzialmente costosa (anche in termini di tempo)
- La verifica può essere ostacolata dalle condizioni sociopolitiche del Paese in cui l'ente risiede o nel caso in cui il titolare delle certificazioni non sia più in possesso dei documenti cartacei (o non) comprovanti

La blockchain potrebbe essere la tecnologia per poter registrare e garantire dovunque, in registri affidabili e condivisi, il riconoscimento di titoli di studio, di formazione, documenti o certificati di qualità di alimenti, beni o servizi.

Secondo la nostra normativa (DPR 445/20/12/2000), un certificato è un documento rilasciato da un' amministrazione pubblica che attesta che un soggetto è titolare di un certo stato.

Tuttavia ci sono molti privati che rilasciano titoli, per esempio percorsi di formazione, spesso con validità internazionale, che accerta che un ente o una persona possa eseguire compiti specifici o operare in determinati settori, oppure certificazioni oggetto di valutazione in sede concorsuale o reclutamento professionale.

Nell'ambito delle iniziative di "blockchain in education"¹⁷, l'UE ha individuato dei criteri su come deve essere la gestione delle certificazioni, articolata su tre processi¹⁸:

- Issuing: un certificato viene istanziato a proposito di un singolo fatto, con memorizzazione in un registro centralizzato.
- Sharing: il destinatario presenta il certificato ad un terzo al fine di esibire i titoli necessari o richiesti
- Verification: il terzo può verificare la veridicità del certificato attraverso l'interazione con il registro.

¹⁷ Il rapporto introduce i principi fondamentali della blockchain concentrandosi sul suo potenziale per il settore dell'istruzione. Propone otto scenari per l'applicazione di questa tecnologia in un contesto educativo, basati sullo stato attuale dello sviluppo e della sua distribuzione.

¹⁸ Fonte: <https://bit.ly/35dOGbL> , pag. 25

I processi descritti possono essere realizzati attraverso un sistema basato su blockchain, questa permette di superare gran parte dei problemi legati ai certificati: quelli tradizionali in forma materiale possono essere facilmente falsificati e i loro controlli sono spesso onerosi e impegnativi, anche la forma dematerializzata è potenzialmente manipolabile ¹⁹.

Questo sistema può fornire un servizio anche a paesi non aderenti al progetto dell'UE o al di fuori delle convenzioni internazionali.

L'utilizzo delle soluzioni basate sulla blockchain assicura la tutela dei soggetti deboli, riduce gli oneri per i soggetti che effettuano le verifiche, garantisce registri aperti su base internazionale, solidi rispetto alle crisi internazionali e alle crisi umanitarie, tecnicamente non alterabili, non censurabili e resistenti a guasti o aggressioni.

¹⁹ Si tratta di un fenomeno di vaste proporzioni e in costante espansione nell'ultimo ventennio, favorito anche dalle opportunità del commercio on-line dei titoli.

Per avere una più chiara idea della dimensione del problema, si pensi che è stato accertato come una delle maggiori fabbriche di titoli al mondo, con sede in Pakistan, tra il 1997 e il 2016 abbia venduto circa 8 milioni di titoli falsi ad acquirenti di 191 paesi diversi (Ezell, 2019). O come nei soli Stati Uniti vengano venduti mensilmente circa 400 certificati fasulli di dottorati di ricerca (WES, 2017).

4.7 Blockchain e il riconoscimento dei titoli di studio UE

La mobilità studentesca e lavorativa offre vantaggi indiscutibili alla crescita personale e delle organizzazioni. Nonostante queste opportunità si siano moltiplicate negli ultimi anni, è ancora evidente la complessità procedurale del sistema di riconoscimento di titoli di studio in termini di costi, tempi e verifiche dell'autenticità.

Se una persona intende lavorare o studiare in un altro paese, sarà necessario che gli vengano riconosciuti i titoli di studio o certificazioni già conseguite. Poiché ad oggi questo sistema è ancora quasi totalmente basato su documentazione cartacea, le procedure di recupero di documenti implicano una serie di costi, che tutte le parti coinvolte devono sostenere:

- Le istituzioni che devono produrre i documenti
- Le istituzioni che devono riceverli, valutarli e riconoscerli
- Le persone che devono affrontare e sostenere questi iter burocratici

Inoltre, può capitare che durante il procedimento si riscontrino delle difficoltà, dovute a molteplici ragioni e soprattutto chi verifica l'autenticità dei titoli potrebbe non essere in grado di individuare eventuali contraffazioni.

La blockchain può supportare il riconoscimento dei titoli e la loro spendibilità all'estero, dove le informazioni relative ad un titolo di studio non possono essere violate o manipolate in nessun modo, promuovendo la mobilità internazionale di studenti, ricercatori e lavoratori.

Ciò rende possibile una digitalizzazione delle certificazioni che dà l'opportunità alla persona di presentare il proprio titolo ad un'istituzione accademica o potenziale datore di lavoro, in modo rapido, economico e sicuro per tutti i soggetti coinvolti.

Esempio:

Mario ha conseguito una laurea in economia presso l'UNIVPM. L'università, oltre che a rilasciare l'attestato in forma cartacea, lo emette anche sotto forma di token, un "oggetto digitale" che può essere inviato a Mario.

Questa credenziale conferisce un titolo a Mario e comprova il conseguimento dell'attestato, garantendo l'autenticità dello stesso e dei dati in esso riportati.

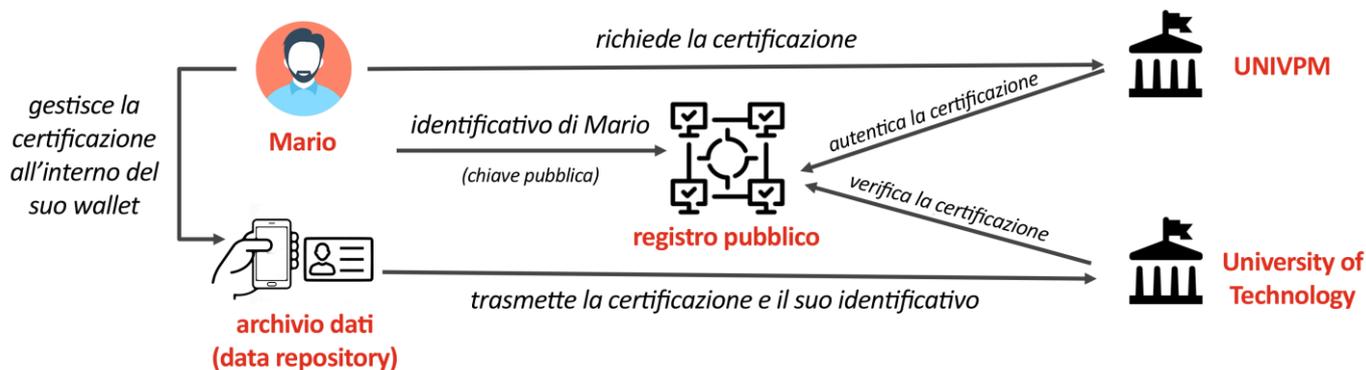
Come un qualsiasi certificato, quest'ultimo rimane in possesso dell'utente all'interno del suo "portfolio digitale".

Mario, a seguito della laurea, vorrebbe frequentare la specialistica presso l'University of Technology di Danzica, dove gli viene richiesto di fornire il titolo di studio che comprova la sua laurea.

Mario, semplicemente utilizzando un'apposita app che segue degli standard predefiniti, condivide direttamente il suo titolo di studio in forma elettronica.

In tal modo l'università di Danzica è autonomamente e rapidamente in grado di constatare l'effettivo conseguimento della laurea presso l'UNIVPM, con relativo voto e data di emissione, senza bisogno di altre procedure.

Il funzionamento del modello è rappresentato di seguito: ²⁰



Le istituzioni di diversi stati dell'UE hanno già adottato soluzioni basate su blockchain. D'altro canto, l'adozione di differenti soluzioni implica un rischio di frammentazione e difficoltà di interoperabilità dei diversi sistemi, minando la diffusione armonica e ottimale di questa tecnologia all'interno dello spazio europeo. Con l'obiettivo di risolvere questo problema, come citato in precedenza, nel 2018 è stato siglato un accordo di cooperazione²¹ per la realizzazione di un'infrastruttura comune europea dei servizi blockchain ("EBSI"), a riprova del ruolo strategico e del valore che questa tecnologia già riveste anche nell'ambito delle politiche di istruzione e formazione.

²⁰ Fonte: <https://www.pwc.com/it/it/publications/assets/docs/blockchain-and-digital-identity.pdf>

²¹ "European Blockchain Partnership". Fonte: <https://bit.ly/3grnziu>

CONCLUSIONE

Parlare di Bitcoin significa raccontare una delle più interessanti invenzioni tecnologiche e monetarie degli ultimi 20 anni, se non della storia dell'uomo.

È conosciuto principalmente come criptovaluta, ma è molto più di questo. Considerarlo solo una moneta virtuale sarebbe come considerare internet solo come scambio di e-mail.

Se Internet ha democratizzato l'accesso alle informazioni, la diffusione di dati e la possibilità di accedere alla conoscenza, Bitcoin ha democratizzato l'accesso alle risorse finanziarie, allo scambio di denaro e alla trasparenza delle informazioni, mettendo in discussione l'attuale sistema finanziario globale.

Per quel che riguarda la blockchain, le sue applicazioni non si limitano solo alle criptovalute, poiché è reputata una delle tecnologie più innovative a disposizione di imprese, governi e società. Consente di raccogliere, verificare e condividere dati in modo sicuro e trasparente. È un sistema in cui l'autorità può passare dall'essere concentrata su poche entità centrali ad essere equamente distribuita, dove intermediari e garanti vengono sostituiti da un sistema incorruttibile nel quale riporre la nostra fiducia.

La blockchain ha però dei limiti, estremamente esaltati, in termini di sostenibilità ambientale e temporale, il che spiega perché abbia trovato fino ad oggi una limitata applicazione.

Probabilmente ci vorrà del tempo per valutare la sua reale applicabilità, sia in termini di adeguatezza infrastrutturale, sia in termini di conoscenze e abitudini degli utenti, che dovranno essere in grado di accettare, utilizzare ed apprezzare questa tecnologia.

L'informatica viaggia tre volte più veloce dell'industria tradizionale, che a sua volta sarebbe tre volte più veloce del settore pubblico. Se pareggiare i tempi sembra impossibile, almeno si può tentare di recuperare un gap.

Nella strada verso l'innovazione basata sulle tecnologie dell'informazione, che rappresentano il fondamento di tutti i sistemi economici innovativi moderni, offre un contributo anche la blockchain.

È una grande opportunità per l'Europa e gli Stati membri per ripensare i propri sistemi di informazione, promuovere la fiducia degli utenti e la protezione dei dati personali, contribuire a creare nuove opportunità commerciali a vantaggio di cittadini, servizi pubblici e aziende.

BIBLIOGRAFIA

- Ammous S. (2018). The Bitcoin Standard: The Decentralized Alternative to Central Banking; John Wiley & Sons Inc.
- Antonopoulos A.M (2019). Mastering Bitcoin; Independently published.
- Attico N. (2018). Blockchain, guida all'ecosistema; Guerini Next.
- Campagnano M, Iacono M, (2021). Blockchain come certificazione robusta del curriculum rispetto alle crisi; Federalismi.it, p. 23-29.
- Castellucci S. (2021). Blockchain e misurazione dell'orario di lavoro; Federalismi.it, p. 45-52.
- Chiap G, Ranalli J, Bianchi R, (2019). Blockchain, tecnologia e applicazioni per il business; Hoepli, p. 7-13.
- Comandini G.L (2020). Da Zero alla Luna, la blockchain: quando, come, perché sta cambiando il mondo; Dario Flaccovio Editore.
- Maccari P. (2015). Le forme monetarie nella storia; Pearson, p. 1-9
- Macchia M. (2021). Blockchain e pubblica amministrazione; Federalismi.it, p. 117-129.
- Nakamoto S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System; <https://bitcoin.org>, p. 1-5.
- PwC Consulting (2016). FinTech e Blockchain: Come costruire Valore; <http://www.pwc.com>, p. 10-18
- Trainito R, Monaco M, Galasso G, (2021). Blockchain e mutuo riconoscimento dei titoli di studio nell'UE; Federalismi.it, p. 167-174.

SITOGRAFIA

- <https://academy.binance.com/it>
- <https://academy.youngplatform.com/it/>
- <https://bitcoin.org/it/>
- <https://blockchain4innovation.it/>
- <https://cryptonomist.ch/>
- <https://coinmarketcap.com/>
- https://ec.europa.eu/info/index_it
- <https://en.bitcoin.it/wiki/>
- <https://federalismi.it/>
- <https://ilsole24ore.com/>
- <https://investopedia.com/>
- <https://it.tradingview.com/>
- <https://medium.com/>
- <https://money.it/>
- <https://pwc.com>
- <https://storiologia.it/>
- <https://wikipedia.org/>