



UNIVERSITÀ POLITECNICA DELLE MARCHE  
FACOLTÀ DI ECONOMIA “GIORGIO FUÀ”

---

Corso di Laurea triennale in

**Economia e Commercio**

**IL VALORE DI DOMANI: BLOCKCHAIN E  
CRYPTOASSET**

**THE VALUE OF TOMORROW:  
BLOCKCHAIN AND CRYPTOASSETS**

Relatore:

Prof. Michela Rancan

*Michela Rancan*

Rapporto Finale di:

Dottori Demis

**INDICE**

**Introduzione**

.....3

**CAPITOLO I: La tecnologia Blockchain**

Il funzionamento della Blockchain.....6

Gli attributi principali.....10

Tipologie di Blockchain.....11

**Capitolo II: Ambiti applicativi**

I casi d'uso.....12

I cryptoasset.....16

Tipologia dei cryptoasset.....17

Tassonomia delle cryptovalute.....20

La nuova era digitale.....22

**CAPITOLO III: Contesto attuale e futuro**

Il valore delle cryptovalute.....25

Blockchain e le istituzioni.....28

I rischi.....32

**Conclusioni.....35**

Bibliografia.....36

## INTRODUZIONE

### Il valore

Per Blockchain si intende un tipo di tecnologia che punta a innovare in modo marcato il trasferimento del valore economico. Grazie alle sue caratteristiche potrà assumere un ruolo di assoluto protagonista nel futuro del valore già dai prossimi anni. Per questo, prima di presentare tale innovazione, vale la pena accennare il concetto di valore, a seconda delle fasi storiche e dello sviluppo economico. Il valore può essere infatti considerato una delle istituzioni più antiche, visto che, dall'avvento dell'agricoltura, ha sempre fatto parte della vita degli uomini e ne ha regolato comportamenti e abitudini.

Il baratto è stata la prima forma di scambio di valore. Questo processo consisteva nel mero scambio di beni tra persone. Tale procedimento di scambio poteva sostenere in modo efficiente solo economie naturali come quelle di quel tempo, caratterizzate da piccoli ecosistemi e con pochi beni o servizi scambiabili, dove l'offerta proveniva da pochi agenti economici. Col progredire dell'economia e lo sviluppo del commercio su larga scala, lo scambio di beni e servizi avvenne tra più persone e il problema del soddisfacimento economico dei singoli diventò sempre più stringente. L'utilizzo del baratto presenta tre ordini di problemi, che lo resero un sistema obsoleto col passare degli anni: la mancata frazionabilità dei beni, l'asimmetrica deperibilità tra beni scambiati e la distanza spaziale tra agenti economici.

Proprio per far fronte ai grandi limiti del baratto, si ebbe la necessità di creare un mezzo di scambio, cioè uno strumento che permetta uno scambio indiretto e che ne garantisca l'intermediazione: il denaro. Per valore di scambio del denaro si intende infatti che esso non rappresenta un bene di consumo, né tanto meno un fattore produttivo.

Nel corso dei secoli, molti oggetti hanno svolto la funzione di denaro: pietre, conchiglie, sale, bovini, fino ad arrivare all'uso dei metalli nobili per coniare moneta. In un primo momento quindi, il valore era rappresentato dal valore intrinseco del materiale usato come oggetto di scambio, specie nella moneta metallica, dove prima venne usato l'oro, successivamente l'argento e poi il rame. La moneta fu poi usata pressoché dalla totalità delle popolazioni, vista la sua capacità di contemporaneamente a tre funzioni: mezzo di pagamento, in quanto strumento valutabile e divisibile; unità di conto, permettendo di prezzare ogni merce in funzione delle unità di valuta necessaria per acquistarla; riserva di valore, poiché era capace di trasferire la ricchezza nel tempo, mantenendo intatte le proprie caratteristiche.

Per superare le carenze metalliche, già dal IX secolo si passò all'uso della carta moneta in luogo di quella metallica. Nella seconda metà del 700, anche grazie allo sviluppo delle banche e dell'economia in generale, alla carta moneta venne dato un controvalore garantito dalle riserve d'oro, detenute presso le Banche Centrali secondo il metodo del Gold Standard. Tale standard internazionale fu intrapreso dalla Gran Bretagna e adottato fino al 1914, quando per poter finanziare le spese belliche e post-belliche si preferì stampare moneta, a discrezione delle Banche Centrali.

Negli accordi di Bretton Woods del 1944, venne stabilito che solamente il dollaro, considerata la valuta più importante del globo, venisse usato come valuta di riserva globale e fosse ancora garantito in termini di contenuto aureo, tramite l'istituzione di

tassi di cambio fissi per le altre valute nazionali, tutte agganciate al valore del dollaro statunitense.

L'elevata inflazione degli inizi anni 70<sup>1</sup> e altre difficoltà economiche generali, portarono alla fine della convertibilità del dollaro in oro, consacrando l'avvento della politica monetaria inflazionistica e dell'uso della moneta fiat: moneta il cui valore non è ancorato al prezzo di nessun tipo di materia prima. Il sistema tutt'ora vigente implica l'uso di tassi flessibili, stabiliti a seconda dalle economie degli Stati e dalla fiducia che il mercato ripone verso questi. In sostanza, il valore della moneta è dato dalla quantità e qualità di beni e servizi che si possono acquistare in cambio di essa.

Recentemente si è assistito all'ultimo step evolutivo del concetto di valore, rappresentato dalla completa smaterializzazione della moneta. Dagli inizi anni 2000 infatti, ha avuto luogo un processo di continua sostituzione della banconota classica con la moneta elettronica (carte di debito o carte di credito). Per la prima volta il valore economico fu reso intangibile e legato indissolubilmente alla telecomunicazione e allo sviluppo tecnologico. Inoltre, il settore finanziario ha dovuto trovare strumenti per adeguarsi al fenomeno della globalizzazione che ha portato alla pressoché libera circolazione dei capitali fra le diverse nazioni. Ed è proprio in questo contesto che l'argomento che andrò a presentare di seguito si propone di occupare una posizione di primo piano. Partiremo dal descrivere le caratteristiche tecniche del Blockchain, per poi passare ai suoi casi d'uso più rilevanti. Infine, verrà mostrato il quadro generale in cui tale tecnologia si inserisce, definendo il valore che fin qui ha avuto e prendendo in considerazione l'attuale atteggiamento delle varie istituzioni riguardo tale tecnologia.

## **CAPITOLO I: LA TECNOLOGIA BLOCKCHAIN**

### **1.1 FUNZIONAMENTO DELLA BLOCKCHAIN**

Nel 2008 l'economia mondiale era nel mezzo di una delle più grandi crisi finanziarie della storia che vedeva come protagoniste grandi società di intermediazione finanziaria. Nei periodi successivi iniziarono così i primi grandi interrogativi riguardo al funzionamento del sistema finanziario fino a quel momento. In tale contesto, nell'ottobre 2008 Satoshi Nakamoto, pseudonimo di un autore o di un gruppo di autori la cui entità è ancora sconosciuta<sup>2</sup>, pubblicò un white paper denominato "Bitcoin: A Peer to Peer Electronic Cash System", documento che in sole nove pagine descrisse un progetto alquanto rivoluzionario: un sistema di scambio di denaro attraverso strumenti crittografici, senza l'ausilio dei classici intermediari. Fu proprio in quella occasione che fu introdotta e resa pubblica per la prima volta in assoluto la tecnologia Blockchain. Nell'anno seguente tale strumento tecnologico fu implementato ed usato per la prima volta per l'acquisto di un bene tangibile: una pizza.

La Blockchain è essenzialmente uno strumento tecnologico che permette la creazione e gestione di un grande database strutturato in blocchi (appunto "catena dei blocchi") tra loro collegati in rete dove la gestione delle transazioni è condivisibile tra più nodi. I dati contenuti nel database vengono condivisi e replicati contemporaneamente tra tutti i

---

<sup>1</sup> A seguito della crisi petrolifera, il presidente americano Nixon ruppe il trattato di Bretton Woods

<sup>2</sup> Si suppone che si tratti di un gruppo di soggetti, perché tale progetto richiede competenze trasversali quali finanza, matematica, politica economica e informatica

membri del network. L'architettura permette che ogni transazione avviata sulla rete sia validata dalla rete stessa tramite analisi di ogni singolo blocco. Ciascun blocco rappresenta dunque un archivio per tutte le transazioni e per tutto lo storico di ciascuna transazione. È possibile aggiungere nuovi blocchi di informazioni, ma non è invece esclusa la modifica o la rimozione di blocchi precedentemente aggiunti alla catena senza l'approvazione dei nodi della rete.

Il funzionamento appena descritto riesce ad ovviare al problema, molto comune sul web, della double spending, ossia non permette la clonazione di dati in modo illimitato.

Colonna portante sulla quale poggia l'intera architettura Blockchain è la procedura Hash: algoritmo utilizzato nella crittografia che prende qualsiasi testo come input e produce come output un risultato formato da un numero definito di caratteri. Tale processo, noto anche come "firma digitale", consiste quindi nel calcolare l'hash del documento e nel crittografarlo con la chiave privata. L'intero procedimento si avvale infatti di una coppia di chiavi: chiave pubblica e chiave privata; dalla chiave privata si ottiene la chiave pubblica e non viceversa. Questo implica che la chiave pubblica può essere distribuita ad altre persone senza compromettere la chiave privata.

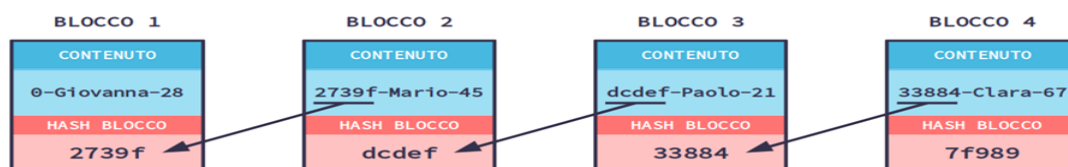


Immagine 1.1: simulazione della procedura Hash. Fonte:Criptoaiuto

La tecnologia in oggetto fa parte della più ampia famiglia delle tecnologie di Distributed Ledger, ossia sistemi che si basano su un libro mastro distribuito, dove le transazioni

vengono messe in blocco e legate una all'altra da una chiave crittografica. Il sistema prevede un organo centrale, ossia il protocollo originale su cui posa l'intera piattaforma, il quale delega tanti organi decentralizzati al controllo di transazioni circoscritte a determinate condizioni. All'uopo viene istituita una governance comune che stabilisce le norme di coordinamento e gestione dei vari nuclei decentralizzati. Il tutto viene organizzato tramite una piattaforma peertopeer: l'utente non viene indirizzato ad un server centrale, ma viene connesso direttamente ad altri utenti.

Dunque nessuno è il quindi il vero proprietario della rete usata. Tale sistema rappresenta un punto di rottura molto importante rispetto a come, finora, siamo abituati a concepire la rete Internet. Fino al white paper di Nakamoto infatti, vigeva solamente il sistema centralized ledger, dove tutto era gestito da una singola autorità, che controllava e deteneva la proprietà della rete. Il sistema generale si basava quasi esclusivamente sulla fiducia riposta dagli agenti sull'autorità. Ovviamente, rispetto alla fiducia, il Decentralized ledger technology garantisce molta più sicurezza a tutti i vari membri.

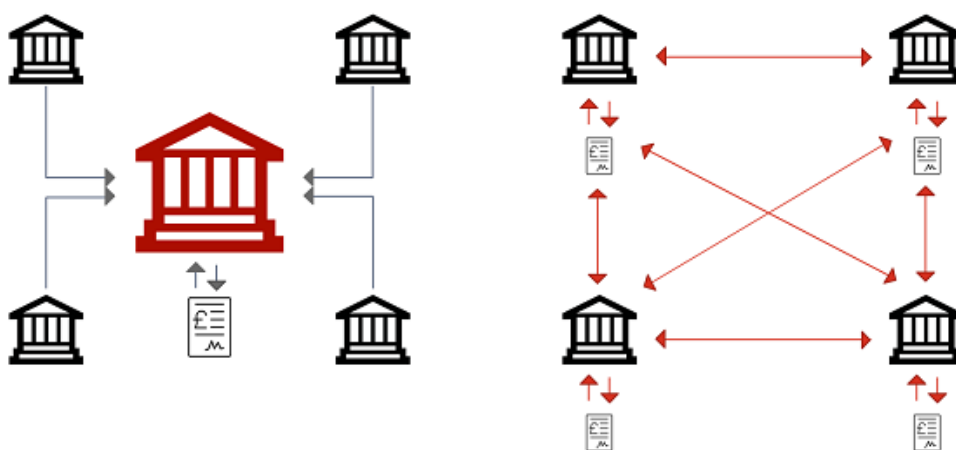


Immagine 1.2: tecnologia centralizzata vs tecnologia decentralizzata. Fonte: Openwt



I nodi sono essenzialmente i server dei vari partecipanti. Il funzionamento della Blockchain viene supportato dall'attività di mining, ossia l'attività di creazione dei singoli blocchi. I soggetti addetti a tale attività sono detti “miner”<sup>3</sup>, nodi a cui viene affidato il compito di estrarre i token in cambio di una ricompensa (di solito in cryptovalute). I miner, per adempiere alla loro mansione, si servono del protocollo Proof of work: algoritmo di consenso che verifica l'accuratezza dei dati. Tale congegno, per impedire abusi di servizio, richiede ad ogni miner di sfruttare la propria potenza di calcolo per risolvere problemi matematici.

Risolta la Proof of work, il miner lo annuncia agli altri miner, i quali verificano la correttezza del lavoro svolto. Se il lavoro eseguito viene accettato, il nuovo blocco viene immesso nel database e si procede alla creazione del blocco successivo. Dunque il miner, oltre a sviluppare la struttura della Blockchain, ne regola anche la sua sicurezza. Come già ripetuto, l'inclusione dell'hash di tutti i blocchi precedenti in ogni singolo blocco rende estremamente complesso modificare le transazioni, visto che la modifica andrà a interessare tutti i blocchi della catena. Se si vuole alterare una transazione quindi è necessario alterare la maggioranza dei blocchi contemporaneamente.

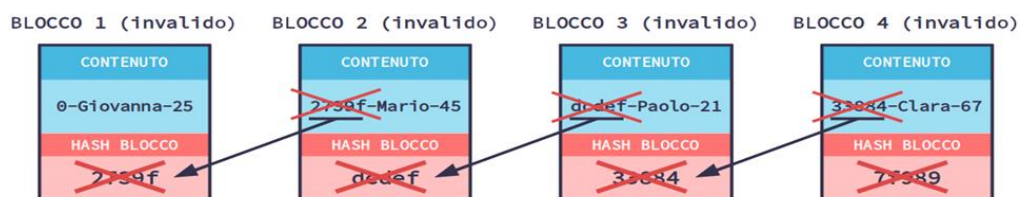


Immagine 1.3: esempio di manomissione a seguito della modificazione di un singolo dato. Fonte: Criptoaiuto

Altro algoritmo ideato di recente per rimpiazzare il Proof of work è quello del “Proof of Stake”, adottato sempre più spesso dalle Blockchain di recente costituzione visto che

<sup>3</sup> Dall'inglese minatore, richiamando l'attività di “estrazione” svolta per creare nuovi blocchi

risulta più veloce ed efficiente rispetto al Proof of Work tradizionale. Il PoS infatti differisce dal PoW in quanto non concede il diritto ad estrarre il blocco successivo a chiunque riesca a risolvere il quiz matematico, ma solo ai miner che possiedono maggiori quote di token nella piattaforma. Chiaramente il PoS tende a privilegiare i nodi con più partecipazioni rispetto al PoW, garantendo maggiore sicurezza in cambio di meno inclusione a livello operativo.

## 1.2 ATTRIBUTI PRINCIPALI

Come detto in precedenza, l'aspetto più innovativo della Blockchain è quello della decentralizzazione, ovvero la possibilità di gestire le informazioni senza un'autorità centrale che convalida le diverse transazioni. Altre caratteristiche innovative che risiedono nell'architettura di tale tecnologia e che ne stanno determinando l'ascesa nel mondo economico sono le seguenti:

- *immutabilità*: i dati, una volta inseriti nella Blockchain, non possono più essere alterati o rimossi in alcun modo grazie alla continua sorveglianza dei miner
- *anonimato*: le informazioni possono essere del tutto anonime o parzialmente anonime, a seconda del tipo di protocollo Blockchain
- *trasparenza*: le informazioni sono pubbliche e aperte ai partecipanti
- *Open source*: qualunque sviluppatore può contribuire al progetto, in quanto il codice sorgente è online e a disposizione della collettività
- *Sicurezza e validità*: strumenti crittografici garantiscono la sicurezza complessiva delle informazioni grazie a robusti algoritmi di consenso
- *Disponibilità*: le transazioni sono eseguite in continuazione. Gli unici limiti sono quelli insiti nel protocollo

- *Programmabilità dei trasferimenti*: possibilità di programmare determinate azioni che vengono effettuate al verificarsi di certe condizioni

### **1.3 TIPOLOGIA DI BLOCKCHAIN**

#### Blockchain pubblica

Prima Blockchain ad essere stata creata e risulta ancora la più usata in assoluto, anche perché viene adottata dai cryptoasset. Carattere comune di questa tipologia di Blockchain è quello di essere aperte al pubblico e a qualsiasi individuo voglia parteciparvi. Gli utenti utilizzano un meccanismo di consenso distribuito per raggiungere una decisione e mantenere una copia del libro mastro sul proprio nodo locale, sotto la continua supervisione dei miner, i quali possono essere qualsiasi utente. Il vantaggio maggiore che offre la Blockchain pubblica è quello di creare un effetto rete, ossia possibilità di correlare entità eterogenee ed utenti.

#### Blockchain private

Caratteristica principale di questa tipologia è quella di limitare il numero di accesso alla network: possono accedervi solo un determinato gruppo di persone o organizzazioni. Le piattaforme di questo tipo utilizzano di solito protocolli di consenso più sofisticati del PoW, come il PoS. Le autorizzazioni di scrittura sono centralizzate all'interno di una

sola organizzazione. Questa tipologia di Blockchain “sacrifica” infatti la decentralizzazione in cambio di maggiore spazio di archiviazione velocità di esecuzione, riduzione dei costi e un miglior controllo dei partecipanti. La Blockchain privata è utilizzata maggiormente da istituzioni finanziarie, visto che risultano ideali per risolvere questioni di riciclaggio di denaro o valutazioni dei clienti. Le transazioni sono di solito meno costose rispetto alle Blockchain pubbliche, poiché la validazione passa solamente da pochi nodi considerati affidabili.

### Blockchain consorzi

Simile alla Blockchain privata, con l’unica differenza che il processo di consenso è controllato non da un’entità centrale ma da un preselezionato insieme di nodi. Il diritto di leggere la Blockchain può essere pubblico o limitato ai partecipanti, mentre il diritto di scrittura spetta solamente a quei nodi scelti a priori. La tipologia in oggetto è usata in gran parte da istituzioni finanziarie (consorzi di banche), specie per erogare prestiti sindacati. Viene usato spesso anche per garantire la sincronicità tra invio della merce e ricezione del pagamento nel commercio internazionale.

## **CAPITOLO II: AMBITI APPLICATIVI**

### **2.1 CASI D’USO**

#### Servizi finanziari

Quello finanziario è il settore dove l’applicazione è più coerente con l’idea di base con cui la tecnologia Blockchain è stata ideata. Inoltre, la continua crescita delle transazioni transfrontaliere necessita sempre più di strumenti tecnologici sempre più avanzati per

poter accelerare i tempi e ridurre i costi di transazione. L'interesse delle banche nei confronti della Blockchain ha cominciato a maturare fin da subito: Goldman Sachs, Barclays e USB hanno dichiarato di recente che potrebbero usare tale tecnologia su diversi ambiti operativi fra qualche anno. Un consorzio composto da 9 istituti di credito internazionali, a cui aderisce anche Unicredit, ha avviato nel 2016 un progetto chiamato We.trade, piattaforma digitale Distributed Ledger che tramite Smart Contract interconnette fornitori, clienti e banche, in modo da gestire, monitorare e proteggere le transazioni commerciali tra imprese europee. L'intero processo commerciale viene registrato e reso completamente visibile nell'interfaccia del database. Inoltre grazie ai Smart Contract viene garantito il pagamento automatico una volta rispettati tutti gli accordi contrattuali.

### Servizi assicurativi

Alcune società assicurative hanno da tempo iniziato a puntare alla Blockchain per la gestione dei contratti e la registrazione delle transazioni, specialmente per quel che riguarda la gestione dei reclami e delle conseguenti liquidazioni. Ad esempio, AXA ha iniziato a implementare Smart Contract per la compensazione automatica agli assicurati i cui voli sono in ritardo. Il risarcimento avviene in questo caso in modo automatico e veloce, prendendo come riferimento la transazione dell'acquisto del biglietto.

In generale, grazie alla Blockchain, le attività assicurative quali cespiti dei beni possono essere registrate e identificate in modo univoco, permettendo la loro immediata verifica, escludendo qualsiasi comportamento elusivo dai parte degli assicurati.

### Gestione profili personali

Come già visto in precedenza, la tecnologia Blockchain permette di conservare in modo immutabile e certificato i dati degli utenti che vi partecipano. Queste caratteristiche possono incrementare l'efficienza su numerosi settori. Caso d'uso molto rilevante è quello che riguarda la gestione della proprietà. Nel mercato immobiliare, la conservazione dei dati di proprietà delle case e le caratteristiche delle stesse all'interno di una Blockchain assicurerebbe a una maggiore trasparenza, incrementando notevolmente l'efficienza della compravendita immobiliare, senza passare per le agenzie immobiliari.

Vale lo stesso per quanto riguarda la gestione delle proprietà dei terreni: la Blockchain potrebbe migliorare drasticamente l'affidabilità dei dati relativi possesso dei terreni, specie nei paesi emergenti dove corruzione e mancanza di informazioni sono problemi di difficile risoluzione. Qualunque passaggio di proprietà diventerebbe quindi più trasparente. In generale, quasi tutte le tipologie di compravendite online, sempre più importanti per volumi d'affari, potranno essere più facili e sicure sia per i compratori che per i venditori.

Oltre alla gestione dei dati di proprietà, Blockchain può prendere parte a numerose organizzazioni che necessitano di un'accurata gestione dell'identità dei vari utenti. La gestione dell'identità nella piattaforma in oggetto si basa sul concetto di Decentralized ID, che permette di implementare un'infrastruttura decentralizzata di chiavi pubbliche. I DID definiscono in modo standard le identità per gli individui e per le organizzazioni, creando identificatori permanenti che, a differenza di un dominio o un indirizzo IP, non permettono la modificazione di nessun dato. Il proprietario dell'identità controlla il DID, tramite la propria chiave privata associata a quella pubblica. Siccome il controllo

su un DID viene realizzato interamente utilizzando la crittografia, non è necessaria alcuna autorità centrale.

Nell'ambito delle attività notarili e nella gestione delle proprietà intellettuali la tracciabilità e la difesa della propria identità permettono di contrastare casi di contraffazione. Rilevanti sono soprattutto i vantaggi che possono trarre le diverse pubbliche amministrazioni nel controllo preciso dei dati. Per esempio a livello sanitario si può arrivare ad una migliore efficienza nel controllo dei pazienti e delle relative cure tramite un monitoraggio continuo e sistematico dei farmaci somministrati. Per la Pubblica Amministrazione potrebbe essere un'arma importante contro l'evasione fiscale, potendo schedare le situazioni patrimoniali dei contribuenti in modo puntuale.

### Sharing Economy

Il settore in oggetto è composto prevalentemente da società che hanno un business model basato principalmente sulle informazioni fornite degli utenti, in modo da istituire piattaforme dove domanda e offerta si incontrano. In questo scenario al momento la maggior parte dei ricavi è destinata ai servizi di intermediazione, la quale avviene in modo centralizzato. Gli utenti non vengono quindi ricompensati pienamente per il loro servizio offerto. La Blockchain permetterebbe di azzerare il costo di intermediazione.

### Energia

Anche il mercato energetico è stato gestito solamente tramite centralizzazione: per effettuare transazioni bisogna in ogni caso trattare con intermediari o terze parti. Per cui il cliente è costretto a pagare sempre qualcosa in più. L'energia potrebbe però diventare presto una risorsa condivisa: i singoli individui potrebbero produrre energia elettrica e

distribuirli a consumatori, detenendo tutte le transazioni sul database Blockchain. Tale aspetto può assicurare anche la trasparenza nell'uso e nel monitoraggio delle diverse forme di energia usate, in un momento dove i problemi ambientali sono sempre più stringenti.

### Tracciabilità alimentare

La Blockchain permette di tracciare in modo trasparente il percorso di un prodotto, dalla sua ideazione fino alla sua commercializzazione. Tale tracciatura fornisce un maggior valore al prodotto, rafforzandone il marchio, specie per tutti quei prodotti di elevata qualità, che sono spesso soggetti a fenomeni di contraffazioni (si pensi al caso dei prodotti Made in Italy<sup>4</sup>). In questo momento sono molte le aziende che hanno accolto la tecnologia Blockchain in questo settore: tra le più famose, due colossi del settore alimentare quali Barilla e Carrefour. Entrambe, tramite l'uso di un QR code riescono a far riconoscere la storia del prodotto ad ogni cliente, che può scegliere in maniera sicuramente più consapevole cosa portare nelle loro tavole.

## **2.2 I CRYPTOASSET**

Oltre ai diversi casi d'uso appena elencati, l'avvento della tecnologia in oggetto ha dato luogo alla nascita dei cryptoasset. La prima Blockchain mai progettata fu proprio quella della cryptovaluta del Bitcoin, la quale ha fatto da battistrada all'uso di tale strumento anche per gli altri ambiti di applicazione. Si iniziò a parlare di cryptovalute proprio nel 2008, quando con la pubblicazione del suddetto white paper di Satoshi Nakamoto, venne descritta per la prima volta l'innovativa idea di moneta virtuale, ossia un sistema

---

<sup>4</sup> Secondo Coldiretti i prodotti italiani venduti all'estero 6 su 10 sono alterati o contraffatti



di pagamento che si possa servire di un sistema decentralizzato peer to peer (piattaforma Blockchain pubblica), senza dover passare per alcuna autorità pubblica.

Il tipo di moneta creata più di dieci anni fa viene rappresentata nei vari database sottoforma di token, racchiudendo in sé le caratteristiche della banconota e della moneta elettronica, con la differenza che non necessita la regolazione degli intermediari. La nascita di questo tipo di sistema di pagamento è spiegata proprio dal desiderio, con chiare influenze anarchiche e liberali, di emancipazione dalle autorità centrali, che con le varie regolamentazioni non permettono il completo controllo del denaro da parte dei possessori e addirittura, come nel caso della crisi dei subprime nel 2007, può ledere in modo critico le situazioni economiche dei privati. Sostituendo il sistema centralizzato con quello decentralizzato garantito dalla Blockchain non vi è separazione tra banche e clienti, per cui ogni utente che converte i propri capitali in cryptoasset gestisce il proprio denaro in modo pienamente autonomo e consapevole, dovendo rispettare solamente le regole date dal software dall'open source della piattaforma usata.

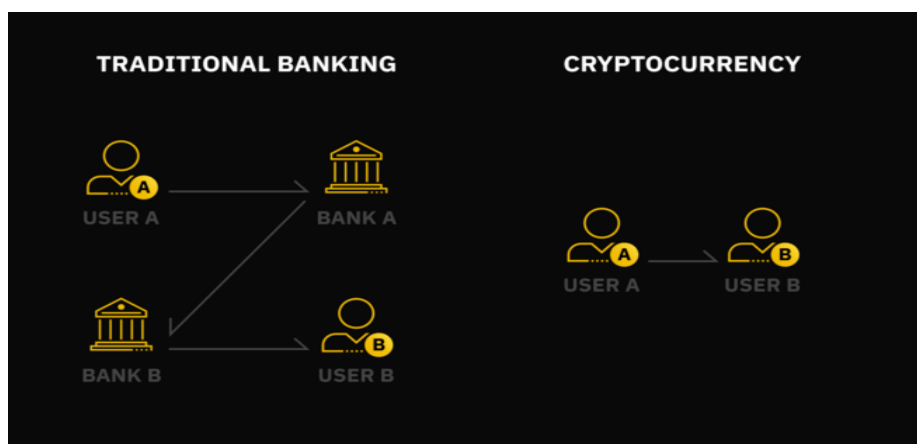


Immagine 2.1: confronto tra transazioni tradizionali e transazioni con criptovalute. Fonte: Binancevision

## 2.3 TIPOLOGIA CRYPTOASSET

Uno degli aspetti sicuramente più rivoluzionari ed affascinanti dello strumento in questione consiste nel fatto che chiunque può crearlo da zero. Una volta creata la Blockchain su cui poggerà tutto il sistema della moneta virtuale bisogna definire le modalità di distribuzione della stessa: mining, conio, ovvero la vendita effettuata per la sostenibilità dell'ecosistema e hard fork, duplicazione di una piattaforma Blockchain per far nascere un'altra con autonomia operativa.

Dopo il Bitcoin, nel 2014 vennero create le cosiddette “altcoin”, ossia altre cryptovalute, nate nel tentativo superare alcuni limiti tecnici dei Bitcoin e di apporre miglioramenti ai servizi di pagamento. Come abbiamo potuto appurare, in questo settore le barriere di entrata sono piuttosto basse, permettendo di avere in pochi anni a disposizione numerosi tipi di cryptoasset, con caratteristiche molto eterogenee. In ogni caso si possono classificare in due macro-categorie: cryptoasset fungibili e cryptoasset non fungibili.

### Cryptoasset fungibili

- *payments token*: le cryptovalute più tradizionali, cui obiettivo è quello di assicurare i pagamenti peer-to-peer e gestire il saldo dei vari utenti nei loro wallet digitali
- *investments token*: fungono da investimento finanziario per chi li possiede. Come gli investimenti tradizionali, la loro gamma di applicazione è molto vasta: si possono avere

token che rappresentano titoli azionari, altri che rappresentano la proprietà di un bene fisico o digitale e altri ancora che rappresentano il valore di strumenti derivati. Dunque qualsiasi strumento finanziario può essere oggetto di “tokenizzazione”. Caso d’uso che ha trovato un’applicazione piuttosto consistente è quello relativo alla raccolta fondi per le aziende, le quali immettono azioni sul mercato sottoforma di token. I titoli soggetti a trasformazione in token garantiscono una maggiore liquidità visto che sono caratterizzati dall’azzeramento di tempi e costi di esecuzione. Inoltre, i piccoli imprenditori potrebbero trovare molto vantaggioso l’uso dei token di investimento, i quali possono far realizzare investimenti frazionari, visto i token possono frazionare i vari asset. Tuttavia in questa fattispecie, si ha meno discrezione nella gestione dei token. La compravendita di token comparabili ai classici strumenti finanziari deve infatti rispettare le regole di collocamento in uso: ossia la ICO dei token viene sottoposta a regolamentazione, dando luogo alla Security Token Offering (STO).

- *utilities token*: destinati all’utilizzo di servizi o di prodotti messi a disposizione dalla Blockchain di riferimento. Questo tipo di token comprende una vasta gamma di ambiti applicativi, anche se in parecchi si è ancora in fase di ideazione, specie perché si ha difficoltà nel regolamentare tali strumenti: le normali cryptovalute presentano una chiara analogia con il contante tradizionale, gli utility token non hanno nessun corrispettivo univoco, per cui non è semplice inquadrare il loro settore normativo di appartenenza.

### Token non fungibili

Ogni unità ha caratteristiche differenti rispetto alle altre. Questi strumenti sono solitamente utilizzati per combattere la contraffazione, visto che danno rilievo all'unicità degli oggetti, garantendo la qualità e la loro originalità.

## **2.4 TASSONOMIA DELLE CRYPTOVALUTE**

### Bitcoin

Prima cryptovaluta ad essere stata sviluppata, rimane ancora quella più scelta visto che ancora oggi è quella che ha ottenuto maggiori capitalizzazioni di mercato (di recente ha superato i 1000 miliardi di capitalizzazione). Molti sostengono che fra pochi anni possa essere considerata un vero e proprio mezzo di scambio ed unità di conto. Soggetta a mining tramite PoW, la sua più grande peculiarità è quella di avere un limite massimo prestabilito dal protocollo di Nakamoto di 21 milioni di unità, escludendo a priori fenomeni inflazionistici. Ogni Bitcoin è divisibile in 100000000 satoshi, rendendolo altamente scalabile. Negli anni si sono poi sviluppati vari hard fork, tra cui Bitcoin Cash e Bitcoin Sv, Blockchain che differiscono dalla Blockchain “madre” per quanto riguarda dimensione dei blocchi, algoritmo e commissioni di transazioni.

### Ethereum

Nata nel 2013 e ha rappresentato fin da subito la prima grande alternativa al Bitcoin. Tuttora è la seconda cryptovaluta per importanza, con un numero di capitalizzazioni inferiore solo al Bitcoin. Ha dato il via alla seconda generazione di piattaforme Blockchain, più sofisticate di quelle precedenti, dove la piattaforma non è più concepita come un mero libro mastro, ma in grado di adempiere a funzioni più complesse. I token vengono chiamati Ether. Oltre a non avere nessun limite quantitativo massimo, Ethereum non solo consente di effettuare transazioni, ma, a differenza di Bitcoin, permette l'esecuzione di smart contract. Per tale motivo Ethereum può contare su maggiori prospettive di crescita rispetto alla cryptovaluta rivale, anche perché è in via di progettazione Ethereum 2.0.<sup>5</sup>

### Litecoin

Nata direttamente da Bitcoin e concepita nel 2011 da Charlie Lee, ex software engineer di Google che voleva apporre maggiore velocità alle cryptovalute. Litecoin è quindi caratterizzata proprio da una maggiore velocità nella creazione dei blocchi (quattro volte maggiore a Bitcoin). Il mining, reso più accessibile, garantisce una celerità nettamente maggiore per quanto riguarda il pagamento online. Per il resto Bitcoin e Litecoin hanno una architettura piuttosto simile.

### Monero

A differenza delle altre cryptovalute, Monero opera tramite particolari firme digitali risalenti agli inizi degli anni 90, che garantiscono la massima privacy e il completo anonimato nelle transazioni. La sua architettura non permette infatti di isolare ed

---

<sup>5</sup> Upgrade progettato nel 2015 e con algoritmo di consenso di Proof of Stake in luogo del Proof of Work

identificare la firma dell'utente reale, la quale viene aggregata e "mescolata" in un gruppo di altre firme crittografiche, per cui rende estremamente complesso qualunque tentativo di identificazione della singola chiave privata.

## **2.5 LA NUOVA ERA DIGITALE**

### Web 3.0

Gli inizi degli anni 90 hanno visto nascere il web 1.0, una rete di siti statici che offriva la mera navigazione ipertestuale tra pagine, escludendo qualsiasi interazione tra i vari utenti. La comunicazione peer2peer avveniva esclusivamente via e-mail. Nel 2004 l'avvento dei blog e dei social network cambiò totalmente lo scenario digitale, aprendo le porte all'era del web 2.0. Cominciarono poi a svilupparsi i primi servizi centralizzati (Google, Amazon, Facebook), dove gli utenti potevano interagire in modo semplice e diretto tra loro. Il web 2.0 portò con sé il fenomeno dei Big Data, che si riferisce al continuo proliferare di informazioni personali dei vari utenti iscritti che vanno a confluire nei server delle multinazionali che ne diventano possessori latenti. Le società sfruttano tale mole di informazioni personali per dedurre comportamenti e abitudini, consentendo precisi livelli di profilazione della popolazione. Spesso le grandi quantità di dati raccolti dai servizi centralizzati hanno leso i diritti di privacy e di sicurezza degli utenti. Proprio per contrastare questi tipi di problemi negli ultimi anni si sta

implementando il web 3.0, avente l'obiettivo di creare piattaforme online sempre più sicure e trasparenti, in modo da restituire la proprietà dei dati più sensibili agli utenti, senza alcun tipo di alterazione da parte di sistemi centralizzati. Questa nuova concezione della rete Internet può essere realizzata grazie alle garanzie date proprio dalle caratteristiche tecniche della Blockchain. Per cui il passaggio dal web 2.0 al web 3.0, ovvero da sistemi centralizzati a sistemi decentralizzati, sembra rivoluzionare oltre che il concetto di valore, anche il mondo digitale, rendendolo molto più "democratico", includendo anche gli utenti privati e non solo poche aziende.

#### Finanza decentralizzata

La finanza decentralizza, o Defi, rappresenta un nuovo ecosistema che unisce tecnologia e finanza. I protocolli informatici si sviluppano sulla base di network decentralizzati, servendosi principalmente di Smart Contract pubblica tramite l'uso della Blockchain. Il principale scopo della Defi è quello di far recuperare affidabilità verso il sistema finanziario. Innanzitutto la Defi non va confusa con il mondo Fintech (Financial Technology), caratterizzato dalla mera evoluzione di servizi finanziari tramite nuove tecnologie. La Defi intende invece migliorare il quadro generale dei servizi finanziari, in particolare istituendo nuovi business model. Per esempio, tra gli obiettivi più ambiziosi che la Defi si propone di raggiungere nei prossimi anni vi è quello di concedere prestiti quasi istantanei, bypassando i lunghi iter approvativi che risultano molto complessi e costosi per le banche. Infatti, una migliore efficienza in tale settore può avere effetti nei tassi di interesse, grazie soprattutto alla diminuzione delle asimmetrie informative tra privati e intermediari, i quali, in vista di una migliore selezione dei clienti potranno

contare su un minor rischio di controparte, contribuendo all'abbassamento dei tassi. I finanziamenti saranno quindi meno onerosi e più accessibili, beneficiando l'investimento privato e i consumi in generale.

Altri possibili vantaggi possono aver luogo nel mercato finanziario, dove le emissioni dei vari titoli, quali azioni, contratti derivati e contratti assicurativi, potrà avvenire in modo più snello e veloce.

Rispetto alla finanza tradizionale, regolare le attività operative e le transazioni tramite Smart Contract, garantisce trasparenza, la quale verrà seguita da maggiore fiducia e consenso da parte dei privati. Inoltre, l'ascesa della Defi svilupperà il fenomeno del KYC, ossia del "Know Your Customer" (conosci il cliente): i dati delle varie identità delle persone verranno immessi nella Blockchain e conservati in modo immutabile. Il Kyc può essere vantaggioso soprattutto per gli istituti di intermediazione che devono concedere finanziamenti, visto che tutt'ora sostengono costi ingenti per analizzare i meriti di credito dei vari clienti e per limitare le varie asimmetrie che di norma esistono in tale fattispecie.

Anche le autorità governative potranno ottenere grandi benefici, grazie alle identità precise e immutabili dei vari cittadini all'interno di database, con la possibilità di limitare fenomeni distorsivi molto comuni nell'economia odierna, quali riciclaggio di denaro ed evasione fiscale. La Defi è ancora in via di sperimentazione, anche perché quello finanziario è un ambiente delicato, per cui è ancora in dubbio se il suo supporto possa apportare una vera e propria efficienza a livello operativo. In aggiunta, risulta fondamentale in ogni caso una buona educazione finanziaria di base, la quale non



dipende dalle forme di tecnologie in uso. Rimando al prossimo capitolo l'analisi dei possibili limiti e svantaggi di fondo della Defi, in quanto ricalcano quelle delle Distributed Ledger Technologies di cui fa parte.

## **CAPITOLO III: CONTESTO ATTUALE E FUTURO**

### **3.1 IL VALORE DEI CRYPTOASSET**

Le cryptovalute sono nate principalmente come alternativa alla moneta tradizionale. Tuttavia, la quota di cryptovalute utilizzate per i pagamenti è piuttosto limitata: solamente 284000 transazioni in tutto il mondo avvengono in Bitcoin di transazioni su base giornaliera<sup>6</sup>. Il mercato ha trasformato questi strumenti digitali in veri e propri strumenti di investimento da inserire in portafoglio. Fin da subito, il mercato delle cryptovalute si è distinto per il suo carattere estremamente capzioso, in uno scenario di fondo dove gli investitori hanno cercato di valutare approcci diversi alla costruzione del portafoglio, specie a seguito della crisi del 2008, optando sempre di più per la diversificazione degli strumenti finanziari. Inoltre, grazie all'esplosione dei siti trading online che danno la possibilità a molti utenti di poter investire i propri capitali

direttamente da casa, le transazioni sono aumentate vertiginosamente, così come la quota di investitori meno esperti.

Il valore dei cryptoasset viene stabilito in base a tre livelli dimensionali. Il primo è dato dalla blockchain su cui poggia e alle relative funzioni che riesce a espletare. L'analisi della piattaforma Blockchain deve riguardare non solo l'innovatività e sicurezza della struttura tecnica, ma anche e soprattutto la sua futura longevità e le sue prospettive di sviluppo. La seconda modalità di definizione del valore è quella scelta maggiormente per le monete digitali: la legge della domanda e dell'offerta. In questo caso si fa riferimento alla classica analisi di politica monetaria, dove il valore viene stabilito in base al tasso attuale e futuro di immissione di unità sul mercato. In questo caso, molta importanza è riservata anche al progetto degli sviluppatori e alla serietà della community che si cela dietro qualsiasi asset digitale.

Terza modalità di determinazione del valore di questi strumenti è quella che si basa sugli aspetti speculativi. Il mercato in oggetto, nato solamente nel 2008, è lungi dall'essere considerato "maturo", per cui la speculazione è un fattore ancora molto centrale, alimentato dalle valutazioni degli agenti i quali cercano di prevedere come possa evolvere il valore di asset che ha la particolarità di non aver nessun elemento finanziario sottostante come valore di riferimento. È proprio questo aspetto speculativo che lascia una serie di interrogativi riguardo il futuro del mercato dei cryptoasset. La speculazione, specie se in atto su vasta scala, porta effetti destabilizzanti importanti. In linea teorica, il tratto speculativo dovrebbe ridursi in seguito al maturare dei cryptoasset. Tuttavia, anche in questo momento, il mercato rimane fortemente legato a fenomeni

---

<sup>6</sup> Dati della Bce

speculativi e non sembra ancora esserci nessun tipo di sicurezza che nei prossimi anni questi trend possano placarsi. Sicuramente un fattore importante per dare una stabilità minima è quello dell'accoppiamento con le valute fiat negli Exchange, potendo integrare i cryptoasset con i preesistenti strumenti finanziari. La maggior parte di questi istituti di scambio accoppia con le valute fiat solo il Bitcoin, il quale però è sua volta accoppiato con tutti gli altri cryptoasset. Col tempo la fama del Bitcoin è cresciuta grazie ad una maggiore copertura mediatica, la quale ha portato ad una maggiore adozione di tale strumento. Il Bitcoin è stato stimato in termini di valore per la prima volta nel 2009: 1 Bitcoin valeva 0,00076294 dollari. Già nel 2013, 1 Bitcoin veniva scambiato per 100 dollari. Nel 2017 1 Bitcoin arrivò a valere ben 20000 dollari (più di 2 milioni e mezzo di crescita in termini percentuali rispetto al 2009). Ad inizio 2021 il valore si aggirava intorno ai 60000 dollari, per poi, proprio in questo periodo, subire un calo improvviso del 300% in pochissimi giorni. Tutto ciò fa intendere che speculazioni e dubbi riguardo questo strumento non sono ancora vicini all'essere superati.

Tuttavia, con il rischio inflazione dovuto alle recenti grandi manovre della Banche Centrali per stimolare l'economia dopo la pandemia<sup>7</sup>, e con la presenza di rendimenti sempre più bassi dei Bond dei mercati più sviluppati, sarà difficile intravedere un crollo di lungo periodo del mercato delle cryptovalute. Come ha di recente dichiarato l'imprenditore Ray Dalio: "Il più grande rischio delle cryptovalute è il loro successo".

---

<sup>7</sup> Nel marzo del 2020 la Fed ha tagliato i tassi di interesse e ha avviato un Quantitative Easing dal valore di 700 miliardi di dollari



Immagine 3.1: andamento del prezzo del Bitcoin dal 2012 al 2020. Fonte: Coinbase

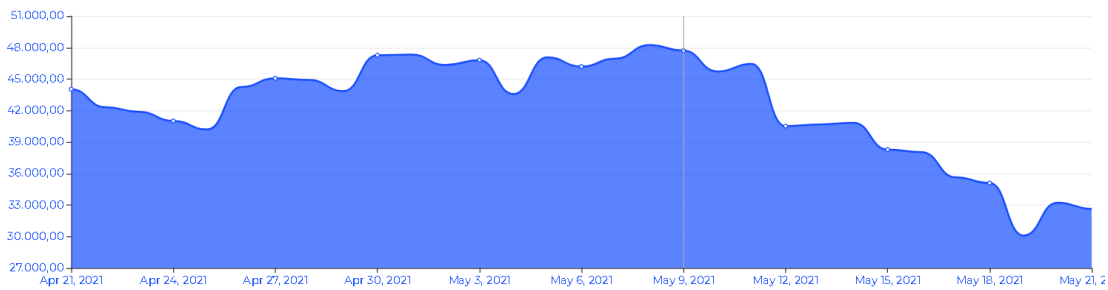


Immagine 3.2: andamento del prezzo del Bitcoin dal 21 aprile al 21 maggio 2021. Fonte: Coinbase

## 3.2 BLOCKCHAIN E LE ISTITUZIONI

### Le autorità governative

Le Blockchain e i cryptoasset sono stati concepiti proprio in un'ottica liberale, con la speranza di arrivare ad una sorta di emancipazione da istituti e da regolamentazioni. L'aumento del numero delle capitalizzazioni e le vertiginose oscillazioni dei prezzi che si sono verificate in questi ultimi anni hanno attirato l'attenzione delle autorità. Ma, proprio perché le Blockchain possono funzionare senza il sostegno di un'istituzione, ci si chiede se regolamentare tale settore sia efficace senza imbattersi in nessun tipo di

contraddizione. Il dibattito su come regolare i cryptoasset verge su cinque punti da prendere in considerazione:

- capire come la nuova tecnologia Blockchain può cambiare il mondo finanziario e non finanziario, visto che le innovazioni promettono di cambiare il modo di operare di molti settori, andando ad intaccare interessi legali
- alcune cryptovalute, grazie al loro funzionamento che garantiscono l'anonimato, facilitano le transazioni illegali che avvengono nel deep-web (mercato nero online) e possono ostacolare le autorità nell'identificazione di attività illecite quali fenomeni di riciclaggio di denaro
- consumatori e investitori nell'operare necessitano di garanzie sottoforma di regole ben precise e uniformi per salvaguardare i loro risparmi
- deve essere garantita una minima stabilità finanziaria in un mercato caratterizzato da un'alta volatilità
- i profitti derivanti dalla speculazione sui cryptoasset, come avviene per tutti gli strumenti finanziari, devono essere tassati e dichiarati

In aggiunta, al contrario di quanto si possa pensare, gli atteggiamenti e le dichiarazioni degli esponenti dei governi nazionali e delle varie istituzioni condizionano estremamente le quotazioni e i volumi di transazioni dei cryptoasset. Caso eclatante è quello rappresentato dalle esternazioni di Elon Musk, Ceo di Tesla, che tramite dei semplici Tweet ha prima fatto schizzare il prezzo delle monete digitali dichiarando che rappresentano il futuro e che la sua casa automobilistica avrebbe accettato cryptovalute per le transazioni. Recentemente, egli stesso ha fatto marcia indietro spiegando che l'attività di mining è troppo inquinante, provocando il recente crollo dei Bitcoin in pochissime ore. Le notizie più rilevanti però rimangono quelle che riguardano divieti

generici imposti dagli stati. Uno degli stati con maggiore attenzione normativa è la Cina, che di recente ha emesso un nuovo ban nei confronti del Bitcoin, dove la banca centrale ha imposto agli istituti finanziari e alle compagnie di pagamenti di non accettare criptoasset per le transazioni, provocando una perdita del 13% nel mercato. La stessa Cina però ha ampiamente riconosciuto l'interesse nei confronti della tecnologia Blockchain, avendo stanziato 150 miliardi per lo studio di una piattaforma istituzionale. Gli Stati Uniti hanno effettuato vari interventi legislativi, ma solo a livello di singoli stati (California, Arizona, New Jersey, Ohio) per regolamentare la tecnologia Blockchain. Il risultato è quello di aver creato un quadro fiscale disomogeneo tra i vari stati americani. In Europa, la Svizzera è sicuramente lo stato che per primo ha inquadrato a livello normativo la Blockchain, ribadendo l'importanza di una chiara e semplice legislazione in tale settore. L'Italia ha emesso nel 2019 il "Decreto Semplificazioni" dedicato al riconoscimento giuridico delle tecnologie basate sui registri distribuiti, prima fra tutte la Blockchain. A livello comunitario il report "Blockchain for Government and Public Service" ha confermato l'interesse per tale tecnologia per l'uso istituzionale. L'Unione Europea si è anche fatta carico del problema di come garantire i diritti dei cittadini immessi nella piattaforma Blockchain. All'uopo è stato istituito un regolamento, il "General Data Protection Regulation" (GDPR), il quale definisce procedure e linee guida per il trattamento dei dati personali, con l'obiettivo principale di allacciare la nuova tecnologia con la legislazione europea sul trattamento dei dati personali. Il GDPR sancisce la cancellazione dei dati nel momento in cui non sono più necessari, richiedere la modifica dei dati personali e limitarne il loro utilizzo.

In tutto il mondo sono ancora molti gli stati nazionali che hanno proibito, del tutto o solo come mezzo di pagamento i cryptoasset.<sup>8</sup>

In ogni caso, anche nei paesi che hanno visto di buon occhio la tecnologia Blockchain e i vari cryptoasset, esiste ancora molta incertezza e il cammino per una completa e chiara regolamentazione di questo settore sembra ancora essere lontano un po' ovunque.

### Le Banche Centrali

L'eventuale adozione della moneta digitale delle Banche Centrali rappresenterebbe il vero punto di svolta per questo tipo di tecnologia e per l'economia del futuro. Sono almeno quindici gli istituti centrali nel mondo che stanno progettando delle Valute Digitali di Banca Central (Central Bank Digital Currency, CBDC), moneta fiat emessa direttamente dalle autorità centrali che possa avere corso legale e quindi potenzialmente usata per qualunque tipo di transazione. Molte altre Banche Centrali si sono rilevate ancora molto scettiche e stanno solamente esplorando attivamente rischi e benefici di questi strumenti. I vertici del G7 sostengono che nessun progetto di moneta digitale globale possa essere avviato senza una stabile normativa di controllo. La stessa Cristine Lagarde ha di recente ribadito che i Bitcoin andrebbero regolati prima di essere considerati una vera e propria valuta, considerando i cryptoasset come asset altamente speculativi, richiamando il ruolo che stanno avendo nel ruolo del riciclaggio di denaro. Di pari passo è il pensiero della Financial Conduct Authority del Regno Unito che ha avvertito i risparmiatori del rischio di grandi perdite che potrebbero portare investimenti in questo tipo di asset.

---

<sup>8</sup> Algeria, Egitto, Marocco, Vietnam, Iran, Bangladesh, Arabia Saudita, Russia, Taiwan, Ecuador, Bolivia, Pakistan,

Proprio nel secondo semestre di quest'anno partiranno le sperimentazioni dell'euro digitale, a seguito del report emesso dall Bce nell'ottobre del 2020 che ne ha sancito le caratteristiche. L'euro digitale avrà le stesse caratteristiche del contante, sarà reso disponibile a tutti i cittadini e utilizzabile tramite App nel telefono. Differirà dalle classiche cryptovalute per essere controllato da un database a livello centrale. Anche Jerome Powell, presidente della Federal Reserve, ha manifestato che il 2021 potrà essere un anno importante per il dollaro digitale, considerandolo come un progetto di primaria importanza.

In generale sono tutti progetti ambiziosi e ancora non sono molti chiari visto i numerosi aspetti che le Banche Centrali devono considerare, quali sicurezza dei mezzi di pagamenti e i vari costi rispetto alla banconota tradizionale. La moneta digitale deve anche adeguarsi alle politiche economiche intraprese dalle Banche Centrali, in particolar modo per quel che riguarda la trasmissione della politica monetaria.

### **3.3 I RISCHI**

La tecnologia Blockchain viene configurata come un punto di svolta capace di cambiare il valore. Il suo è quindi un progetto tanto ambizioso quanto rischioso. Sono molti ancora i dubbi che avvolgono questo tipo di tecnologia e che ne limitano la piena affermazione. Una prima serie di rischi riscontrabili sono quelli legati alla struttura tecnologica. Come succede spesso ai normali database, possono avere luogo



improvvisamente dei bug interni. Per esempio in questi anni la stessa Blockchain del Bitcoin, seppur raramente, ha presentato errori tecnici nel codice applicativo.

La minaccia più importante deriva dai possibili attacchi hacker che possono colpire piattaforma. Il cosiddetto “51% attack” rimane uno dei rischi più discussi. Tale tipo di attacco malevolo può verificarsi quando un gruppo di individui riesce ad impadronirsi del 51% del consenso per effettuare transazioni fraudolente, in modo da alterare il network e le relative transazioni. Tuttavia, questo tipo di attacco risulta molto costoso da effettuare e difficilmente può insidiare le Blockchain più mature, ma può intaccare i cryptoasset da poco istituiti.

Altro problema che sta limitando l’adozione di massa della Blockchain è quello della scalabilità, ossia la capacità del sistema di progredire in funzione delle necessità che l’economia di tutti i giorni richiede. La creazione di blocchi segue un procedimento troppo lento, dando luogo a transazioni che non riescono a seguire il ritmo incessante dei pagamenti tradizionali. Tale tipo di problematica risiede nella natura decentralizzata della piattaforma: se ogni transazione viene eseguita da ogni nodo tramite algoritmi di consenso della rete, la capacità di elaborazione dell’intera rete è limitata alla capacità di elaborazione di quel singolo nodo. Se si vogliono usare invece nodi più potenti, si rischierebbe di creare una struttura centralizzata.

Altro carattere che può risultare problematico è quello relativo alle chiavi per entrare nel database della Blockchain. Come già detto, ogni utente ha a disposizione una chiave

pubblica e una chiave privata, la quale è unica e personale. L'eventuale smarrimento di questa chiave impedisce l'accesso alla piattaforma e quindi la perdita di tutti i fondi.

Spostando l'attenzione verso i cryptoasset e richiamando a quanto detto riguardo al loro mercato, è evidente come il carattere volatile di questi strumenti sia il fattore limitante più importante per molti agenti economici. L'asset in oggetto infatti è caratterizzato da una variazione del prezzo nel tempo che non ha eguali nel mercato finanziario. I cryptotasset sono quindi prodotti speculativi ad alto rischio, con un valore legato esclusivamente ad aspettative future. I fattori esterni, in particolar modo i mass media, sono sempre più influenti per l'andamento del mercato. La forte instabilità porta a molti investitori e molti personaggi influenti, Draghi, Gates e Buffet su tutti, a dubitare del valore effettivo di questi strumenti.

Fattore limitante di recente considerazione è quello che concerne l'impatto ambientale. Gli algoritmi di consenso per costituire nuovi blocchi della catena richiedono calcoli potenti che necessitano determinati tipi di computer ad alto consumo di elettricità. La BCE, la Banca Popolare Cinese e personaggi di spicco (Elon Musk) hanno di recente sottolineato la grande emissione di Co2 richiesta per il sostentamento delle cryptovalute. Basti pensare che una sola transazione effettuata in Bitcoin ha un consumo energetico pari a 4000 pagamenti con normale carta elettronica.

Con l'aumento dei prezzi delle cryptovalute, l'attività di mining si sta espandendo e viene svolta anche da computer meno efficienti e quindi meno sostenibili a livello energetico<sup>9</sup>. L'Università di Cambridge stima che nei prossimi anni il consumo di elettricità in questo settore potrebbe addirittura quadruplicare. È logico constatare come una futura adozione di massa dei cryptoasset sia altamente dannosa per l'ambiente se non si trovano soluzioni alternative alle attuali attività di mining.

## CONCLUSIONI

Partendo dalle caratteristiche tecniche per poi arrivare ai possibili casi d'uso abbiamo analizzato questa tecnologia emergente chiamata Blockchain. Nella maggior parte dei casi i progetti che ruotano attorno a tale sistema sono ancora in fase di progettazione o di mera ideazione. Dunque la Blockchain non ha avuto ancora l'impatto che molti si aspettavano già da subito. Come evidenziato, sono ancora molte le sfide, sia a livello normativo sia a livello tecnico, che la Blockchain deve affrontare per poter essere

---

<sup>9</sup> Il 65% dei Bitcoin è estratto in Cina, paese caratterizzato dall'alto inquinamento dovuto all'uso abbondante del

considerata una vera e propria risorsa per il valore economico e per entrare nella quotidianità delle persone. In particolar modo, risulta ardua la convivenza tre sistemi decentralizzati come la Blockchain e sistemi centralizzati come quelli delle strutture giurisdizionali. In ogni caso, l'innovazione più rilevante è quella che rappresenta il movente filosofico che risiede nella natura decentralizzata della Blockchain, che dalla sua nascita ha mostrato come sia possibile creare una nuova visione dell'economia. Dunque, nonostante i numerosi dubbi che avvolgono l'argomento presentato, è innegabile che la tecnologia Blockchain possa avere nel futuro risvolti pratici positivi, se non addirittura rivoluzionari, andando a modificare radicalmente il concetto di valore, specie in particolari settori come quello finanziario. Tuttavia, siamo ancora all'inizio di questa nuova fase innovativa e ci vorrà ancora molto tempo prima di adeguare tale strumento nella vita di tutti i giorni.

## **BIBLIOGRAFIA**

P.SORGENTONE, *Il Futuro del valore: Blockchain, Cryptoassets e finanza decentralizzata*, Torino 2020, da pagina 188 a pagina 200

N. MROSS, *La rivoluzione Bitcoin*, Stati Uniti 2014

[www.bis.org](http://www.bis.org), *Regolamentazione delle cryptovalute: valutazione delle reazioni dei mercati*, 2018 R.AUER, S.CLAESSENS, da pagina 1 a pagina 12

[www.econstore.eu](http://www.econstore.eu), *The economic potential and risks of cryptoassets*, 2018, M.DEMERTIZIS, G. B.WOLF, da pagina 10 a pagina 13

<https://www.bluerating.com/mercati/181178/criptovalute-sempre-piu-nel-mirino-di-autorita-e-banche-centrali>

<https://www.blockchain4innovation.it/criptovalute/andamento/cose-e-come-funziona-bitcoin-cash/>

<https://cryptohttps://www.coinhouse.com/it/valore-bitcoin/mist.ch/2021/05/19/cina-nuovo-ban-crypto-bitcoin-crolla/>

<https://www.money.it/+Bitcoin-BTC-USD-quotazione>

<https://forbes.it/2021/05/19/il-crollo-delle-criptovalute-il-mercato-scende-di-700-miliardi-bitcoin-sotto-i-40-000/>

<https://www.pandasecurity.com/it/mediacenter/mobile-news/bitcoin-mining/>

<https://www.spindex.it/it/blog/la-classificazione-delle-blockchain/#:~:text=Esistono%20principalmente%20tre%20tipologie%20di,registri%20personalizzati%20per%20applicazioni%20specifiche.>

<https://parentesistoriche.altervista.org/breve-storia-della-moneta/>

