UNIVERSITÀ POLITECNICA DELLE MARCHE

FACOLTÀ DI ECONOMIA "GIORGIO FUÀ"

Corso di Laurea triennale in Economia Aziendale

DIGITAL ECONOMY E UN MONDO BITCOIN

DIGITAL ECONOMY AND A BITCOIN WORLD

Relatore:
Prof. Mariano Cesari

Rapporto Finale di:
Giovanni Toscani

Anno Accademico 2020/2021

INDICE

INTRODUZIONE

La digital transformation ha profondamente mutato ogni settore della vita dell'uomo. L'economia, la finanza e la stessa organizzazione della società vivono ad oggi una fase di grande cambiamento, promossa dalle radicali innovazioni tecnologiche degli ultimi decenni. In questo contesto, una delle più interessanti novità riguarda le evoluzioni dei sistemi di pagamento, su tutte quelle legate alle nuove opportunità offerte dall'informatica, quali le c.d. valute virtuali (o criptovalute). Le valute virtuali hanno difatti catturato via via un sempre maggior interesse, vuoi per l'introduzione di tecniche altamente innovative adottate per le operazioni di pagamento e di trasmissione di moneta, vuoi per la portata rivoluzionaria non solo in ambito economico ma anche sociale e geopolitico. Nell'ottica comune, l'associazione di criptovaluta al nome "Bitcoin" è immediata, quasi scontata: Bitcoin è ad oggi il sistema monetario alternativo più diffuso, nonché il più conosciuto e riconosciuto a livello globale.

Questo lavoro ha proprio l'obiettivo di mettere in evidenza questa innovazione monetaria di cui si sente sempre più parlare, partendo dai suoi fondamenti storici per poi andare a descrivere le sue caratteristiche, i suoi pregi e i suoi limiti per poi finire con un cenno anche alle altre criptovalute in circolazione.

Nel primo capitolo viene introdotto il concetto di Digital Economy e si parlerà delle trasformazioni che la maggior parte dei settori produttivi stanno avendo a causa della digital transformation.

Proseguendo, nel secondo capitolo si evidenza l'evoluzione storica e la nascita di questa nuova moneta digitale finendo con il terzo capitolo in sui si andranno a trattare le caratteristiche, i pregi e gli aspetti tecnici del Bitcoin per poi concludere con un breve cenno alle altre criptovalute.

DIGITAL ECONOMY

1.1 - I fattori disruptive dei modelli di business tradizionali

In questi anni, nella maggior parte dei settori, i modelli di business stanno cambiando radicalmente e stanno mutando le determinanti per il loro successo.

Questo cambiamento è generato dalla pervasività nei sistemi economici e sociali, in gran parte del mondo, di tre fenomeni distinti, ma fortemente interdipendenti, comunemente descritti con i termini inglesi the digital, sharing e green.

Le tecnologie digitali, la logica della condivisione (concretamente attuata attraverso piattaforme digitali) e l'ottimizzazione dell'impatto ambientale delle attività umane stanno per un verso favorendo la nascita di modelli di business, e conseguentemente imprese, completamente nuovi; per l'altro, costringendo quelli esistenti a innovarsi radicalmente. La potenza di questi tre fenomeni deriva

dall'avere natura molto composita: tecnologica, economica e sociale al tempo stesso; inoltre, della loro stretta interdipendenza. Questo spiega la pervasività del cambiamento che stanno generando sui sistemi economico-produttivi e sociali a qualsiasi latitudine, a prescindere dalle differenze di ricchezza, tradizioni, assetti sociali.

Le tecnologie digitali e l'approccio green sono ormai determinanti in tutti i comparti manifatturieri senza davvero alcune esclusione; la sharing economy, basata su piattaforme digitali e spesso finalizzata a migliorare la sostenibilità ambientale (e sociale) dell'agire umano, è ormai pervasiva nei servizi: dai trasporti al turismo, alla distribuzione, alla consulenza.

1.2 - Cos'è la digital economy?

Il fenomeno della digitalizzazione include i processi di conversione delle informazioni in forma digitale e lo sviluppo di tecnologia per gestire e sfruttare economicamente le norme ammontare di risorse digitali generate da tali processi.

Esso poggia su un complesso di tecnologie fortemente interdipendenti, riguardanti internet, le infrastrutture di comunicazione rete, l'hardware, le mobile applications, i servizi ICT, e sta innervando tutti i sistemi produttivi e sociali attraverso innovazioni quali cloud technologies, Internet of Things (IOT), advanced automation, big data analytics, social network.

Il fortissimo impatto dell'economia digitale deriva dal fatto di essere tanto pervasivo, quanto rapido; a riguardo, basti ricordare alcuni semplici dati: nel

2015, il mondo aveva circa 7,2 miliardi di abitanti e ben tre miliardi di utenti internet attivi; due miliardi di account attivi sui social network; nei paesi avanzati, si stima che il tempo medio di presenza delle persone in internet si di 4,4 ore; Google è stata fondata nel 2016.

Ora stando piuttosto difficile tracciarne con precisione i confini, l'economia digitale può essere fatta rientrare nel macrosettore dell'information and communication technologies (ICT) che nel 2013 ha rappresentato quasi il 6% dell'intero valore aggiunto realizzato nei paesi OCSE, con un picco di poco meno dell' 11% in Korea; si stima che entro i prossimi 5 anni circa, nei paesi avanzati, il complesso di produzioni legate al digitale genererà un valore aggiunto intorno al 15% del totale.

Questa crescita non sta avvenendo senza squilibri; in particolare, con un forte aumento della concentrazione o addirittura la formazione di monopoli che avendo dimensione praticamente globali raggiungono un potere superiore anche a quello di molti governi nazionali.

La maggior parte dei settori produttivi, sia manufatturieri sia di servizi, stanno attraversando una digital transformation che ne sta modificando la struttura e le dinamiche competitive con inevitabili rilevanti riflessi sul modello di business delle imprese. Queste trasformazioni sono già oggi evidenti in comparti come le telecomunicazioni, l'editoria e l'entertainment, il turismo, i servizi sanitari e alla persona, il retail, i servizi bancari. In molti casi, l'affermarsi di nuove offerte

basate sulla digitalizzazione del prodotto o del servizio hanno avuto un effetto disruptive su sistemi produttivi fino ad allora molto consolidati. Per esempio, il fatturato mondiale dei prodotti discografici(registrati) è crollato da circa 20 miliardi di dollari nel 2005 a poco più di 14 nel 2013 e 2014. Le telecomunicazioni sono un'altro settore fortemente impattato dalla rivoluzione digitale, in particolare dal lato della diminuzione della redditività operativa e dei cash flows. I social media, infatti, hanno aperto nuovi canali di comunicazione che stanno riducendo il business "voice" e "messaging" delle Telco; per esempio, si stima che negli Stati Uniti, la telefonia fissa e mobile abbia generato nel 2016 circa un terzo del business, mentre nel 2010 era oltre il 50%; al contrario i ricavi da gestione dati è arrivato a circa 2/3 del totale. Lo sviluppo digitale, tuttavia, non rappresenta solo una minaccia per le imprese di telecomunicazioni, ma offre loro l'opportunità di innovare il proprio business model e sviluppare nuove modalità di creazione di valori per i propri clienti. Una manifestazione delle tecnologie digitali che sto avendo un impatto cruciale nelle industrie e nei mercati è l'affermazione del "piattaforme" digitali: ambiti ove si aggregano insiemi di persone per svolgere attività nuove o realizzare in modo nuovo (basato appunto sulla digitalizzazione delle informazioni) attività tradizionali. Già oggi, qualsiasi organizzazione strutturata ha sviluppato una propria piattaforma digitale, attraverso la quale gestisce le relazioni e gli scambi con i soggetti esterni, innanzi tutto i clienti ai fornitori, sviluppa una parte crescente della propria

comunicazione e attua parti sempre più rilevanti di organizzazione delle attività interne. La rilevanza delle piattaforme risulta evidente dalla loro diffusione e pervasività in molte funzioni aziendali: dalla gestione delle relazioni con il cliente allo “smart working”, dall’automazione dei processi produttivi alla gestione delle procedure amministrative. Parallelamente, si è assistito a un grande sviluppo di nuove forme di offerta basate su piattaforme digitali; esse si sono manifestate in: siti di e-commerce e le diverse tipologie di marketplaces; social networks; fornitori di informazioni e contenuti; gestori di “comunità” di soggetti aggregati attorno a un’esigenza comune. Con modalità diverse, hanno rappresentato l’infrastruttura basilare per l’affermarsi dei modelli di sharing e pooling economy.

Anche queste piattaforme stanno favorendo un'innovazione profonda di molti servizi, non solo nelle modalità di loro erogazione e fruizione, ma anche negli aspetti fondamentali della value proposition e quindi dei contenuti. Un esempio molto significativo a riguardo, di cui sarà interessante verificare gli effetti nei prossimi anni, è rappresentato dai Massive open online courses (MOOC) ormai concorrenti tradizionali dell'offerta formativa tradizionale, soprattutto di livello universitario e professionale.

I modelli di business basati sul digitale sono fondati su alcuni fondamentali componenti che li distinguono fortemente da quelli tradizionali:

- Concept adatto a soddisfare nuove esigenze degli utenti, legate in particolare ai comportamenti “social”
- Presidio delle tecnologie abilitanti
- dimensione tale da sfruttare al meglio le esternalità di rete
- capacità di acquisizione e gestione dei dati
- potenziale diffusione globale
- diffusione internazionale sin dalle prime fasi del ciclo di vita.

Le Tecnologie digitali, insieme alle innovazioni nell'ambito dell'automazione, stanno, infine, creando le condizioni per radicali miglioramenti dei processi di produzione industriale. Favoriscono, in primo luogo, un forte aumento della flessibilità e quindi il raggiungimento di condizioni di elevata efficienza anche a piccoli lotti di produzione; viene drasticamente ridimensionato il potenziale delle " economie di scala” nella creazione di un vantaggio competitivo di costo. rendono inoltre più rapidi e meno costosi i passaggi tra le varie fasi del processo produttivo, con effetti positivi sulla produttività e sulla possibilità e costo di adattamento del prodotto finale alle specifiche richieste del cliente. Aumentando la precisione nell'utilizzo delle macchine e dei sistemi di controllo, le tecnologie digitali determinano anche un aumento della qualità e una diminuzione degli sprechi con importanti benefici sul piano sia dei costi, sia dell'impatto ambientale dell'attività produttiva.

Storia del Bitcoin

2.1 - Fondamenti storici

Il bitcoin è la prima criptovaluta al mondo, non soltanto per mero ordine cronologico ma anche per quanto riguarda l'estensione del mercato. Nato nel 2008 come un'evoluzione (o meglio, una "messa in pratica") del concetto di criptovaluta, Bitcoin ha vissuto quasi un decennio in un crescendo di popolarità, diffusione e crescita del valore, il tutto costellato anche da innumerevoli tensioni e interrogativi. Una maggior comprensione del fenomeno deve necessariamente passare da uno studio delle sue radici storiche, in particolar modo per meglio comprendere successivamente le implicazioni economiche, sociali e politiche attuali e future.

2.2 - Origini delle cryptovalute

Un primissimo riferimento al concetto di criptovaluta, o criptomoneta, risale al 1982, in uno scritto di David Chaum, "Blind Signatures for Untraceable Payamentes", nel quale egli ipotizzava per una primitiva forma di firma digitale realizzata tramite l'applicazione di una serie di algoritmi. In tal modo, un soggetto poteva ottenere la facoltà di nascondere un certo messaggio prima di firmarlo e "convalidarlo". Lo stesso autore evidenziava le potenzialità di quest'aspetto nel

campo dei sistemi di pagamenti, che possono ricondursi alla possibilità di slegarsi dal controllo dalle autorità e all'adozione di forme anonime tramite l'utilizzo di pseudonimi, senza tuttavia trovarne una vera realizzazione pratica. Le teorizzazioni di Chaum catturarono successivamente gli interessi degli attivisti del Movimento Cyberpunk, che le inclusero nel 1994 nel Manifesto dei Cripto-Anarchici. Gli anarchici del Manifesto identificarono il sistema di crittografia e cifratura proposto da Chaum in uno strumento che potenzialmente potesse essere molto utile nella loro lotta al "potere sovrano". In altre parole, questo sistema è stato considerato come uno strumento funzionale alla lotta dell'individuo nell'affermare la propria sovranità nei confronti dello Stato. Le idee di Chaum sono state ulteriormente sviluppate, almeno a livello teorico, da Wei Dai nella mailing list Cypherpunks, il quale perviene ad una prima ideazione vera e propria di criptovaluta. Egli descrisse un sistema "che consente ad un gruppo di pseudonimi digitali non tracciabili di effettuare vicendevolmente pagamenti in denaro e di assicurare il rispetto di contratti senza aiuti esterni", spiegando come giungere, ad un prototipo di criptovaluta, denominata B-Money, sfruttando una serie di passaggi informatici. Tuttavia, nonostante i progressi dell'Information Technology e le interessanti potenzialità d'utilizzo delle nuove valute, l'innovativo meccanismo teorizzato si scontrava con l'incapacità di una sua implementazione pratica efficace; il problema più grande riguardava il fenomeno della double spending (ossia, il processo mediante il quale si rende possibile

duplicare lo stesso gettone e spenderlo due volte). La portata rivoluzionaria di Bitcoin risiede proprio in questo aspetto: per la prima volta, a partire dalle iniziali teorie di Chaum, si giunge ad un sistema in linea con le idee di Wei Dei ma che al tempo stesso risolve i sopracitati limiti "tecnici", gli stessi limiti che avevano impedito la realizzazione reale di una criptomoneta.

2.3 - Protocollo Bitcoin: Nakamoto Satoshi

Il dominio "Bitcoin" è apparso per la prima volta il 18 agosto 2008, precisamente nell'atto di registrazione di "bitcoin.org" su anonymousspeech.com. Il vero e proprio rilascio è avvenuto pochi mesi più tardi, attraverso la pubblicazione online di "Bitcoin A peer-to-peer electronic cash system" 7 , un documento sottoscritto da parte di un programmatore sconosciuto, noto con lo pseudonimo di Satoshi Nakamoto. Questo documento è universalmente riconosciuto come il "Protocollo Bitcoin", che pone le fondamenta e disegna le guidelines di tutto il progetto. L'identità di colui (o coloro) che si cela dietro Nakamoto è tutt'oggi ancora ignota, nonostante siano state elaborate numerose teorie a riguardo. Tuttavia, Nakamoto ha interrotto il suo diretto coinvolgimento in Bitcoin durante la metà del 2010, trasferendo diversi domini di sua proprietà ad alcuni membri della comunità Bitcoin e consegnando il codice sorgente a Gavin Andersen, il suo più stretto collaboratore. Il concept iniziale del Protocollo è piuttosto elaborato: esso introduce un meccanismo per trasferire denaro digitale senza l'utilizzo di intermediari finanziari o servizi centralizzati, basato quindi su un sistema

decentrato peer-to-peer puro, in cui un ruolo di primo livello lo assumono i nodi della rete e la crittografia. Il lancio ufficiale di Bitcoin è invece da ricondurre al 3 gennaio 2009, attraverso il rilascio in rete della prima versione Bitcoin 0.1. In questa occasione, è stato generato il primo blocco di 50 BTC (il cosiddetto "genesis block"). Le versioni dalla 0.1.0 fino alla 0.1.5 erano inizialmente supportate solo da Windows 2000, Windows NT e Windows XP. Successivamente al primo rilascio, Satoshi ha lavorato per perfezionare il client, correggendo alcuni errori di comunicazione tra i nodi e migliorando l'usabilità del client (per esempio, si è deciso di impedire l'inserimento di dettagli e spiegazioni sulle transazioni dei coin). Il primo trasferimento di gettoni avvenne virtualmente tra Nakamoto e Hal Finney, tuttavia per la prima transazione in termini reali bisogna attendere la fine del 2010, non appena fu resa disponibile la commercializzazione pubblica delle nuove criptovalute. In quel caso, l'oggetto della transazione si manifestò nell'acquisto di due pizze per un ammontare di 10.000 bitcoin, un evento piuttosto curioso che ha portato alla nascita di un "apposito" tasso di cambio pizza/bitcoin.

UN MONDO BITCOIN

3.1 - Cos'è Bitcoin?

Bitcoin è un sistema elettronico di pagamento peer-to-peer, alternativo al tradizionale sistema bancario, che funziona per mezzo del bitcoin, una moneta virtuale creata appositamente per il sistema (abbreviata anche in BTC o XBT). Occorre innanzi tutto sottolineare una prima distinzione: Bitcoin è sia valuta che sistema di pagamento. Questo porta a dover distinguere tra Bitcoin maiuscolo, con cui ci si riferisce alla tecnologia e alla rete, da bitcoin minuscolo, riferito alla valuta-token in sé per sé. L'intento di Bitcoin è quello di permettere l'invio di gettoni in maniera veloce, sicura ed economica attraverso la rete, proponendo dunque un modello decentralizzato, ossia senza l'intervento di alcun soggetto con funzioni di controllo e coordinamento. Bitcoin nasce dalla Rete e per la Rete: è un sistema basato su di un software opensource, ossia non protetto da copyright e nel quale gli utenti stessi possono apportare migliorie, contribuendo alla sua evoluzione ed al suo perfezionamento, aprendosi anche ad implementazioni "indipendenti" del Protocollo. Inoltre, Bitcoin non ha alcun supporto fisico, le valute possono essere memorizzate in portafogli installati localmente (wallet) mediante un apposito software su dispositivi elettronici (ad esempio pc, smartphone, tablet etc..) o in portafogli online la cui gestione è demandata a specifici portali che offrono questo tipo di servizio. L'integrità e l'autenticità delle

transazioni sono poi garantite dalla crittografia e dalla blockchain, un registro pubblico e condiviso (liberamente accessibile da ogni utente della rete) sul quale si basa l'intero sistema Bitcoin; in altre parole, la blockchain svolge funzioni simili ad un libro mastro online, annotando tutte transazioni mai effettuate e gli utenti partecipanti alla Rete. V'è infine da considerare che, prima dell'iscrizione nel registro, tutte le transazioni vengono verificate da alcuni utenti chiamati miner, i quali, come si approfondirà successivamente, vengono ricompensati con l'emissione di nuovi bitcoin.

3.2 - Anonimato e disintermediazione

Bitcoin promette di superare tutti i limiti del sistema monetario e finanziario tradizionale. Per realizzare il suo fine, Bitcoin poggia essenzialmente su due pilastri: preservare un certo grado di anonimità nel suo utilizzo ed adottare un sistema decentralizzato, che sia totalmente indipendente da qualsivoglia controllo esterno di tipo bancario o governativo. La sfida principale di Bitcoin è forse proprio quest'ultimo punto, che è alla base dell'esistenza stessa di Bitcoin: proporre un sistema decentrato, che sia del tutto indipendente da intermediari bancari o organismi governativi, senza comprometterne l'efficienza; in altre parole, esso si presenta come una forma radicale di disintermediazione, che comporta la sottrazione di una funzione tipicamente pubblica – la gestone di un sistema di pagamento e della relativa contabilità – ad un operatore tipicamente privato – il settore bancario. È poi grazie alla rete e alla crittografia che Bitcoin

consente pagamenti diretti da un utente all'altro (ossia transazioni peerto-peer) in modo efficace, veloce, economico e sicuro. L'ambizione è sicuramente alta: in una sorta di "democratizzazione finanziaria", Bitcoin pone al centro del suo stesso funzionamento la rete nel suo complesso, in cui ogni utente (o "nodo") ha funzioni di controllo e di garanzia delle transazioni; ogni utente con un indirizzo Bitcoin può connettersi alla rete e interagire con gli altri nodi, validare ed autorizzare transazioni, controllare il registro pubblico ed eventualmente segnalare errori al resto della rete. In definitiva, gli utilizzatori di Bitcoin non pongono la fiducia su un ente terzo per la gestione e uso dei propri fondi/guadagni, cosa che ha portato Bitcoin ad essere spesso definito anche come sistema "trust-less". Ma la disintermediazione portata avanti da Bitcoin non si conclude qui. La mancanza di un intermediario o di un ente di controllo centrale assume la sua massima espressione in relazione alla creazione di nuova base monetaria: Bitcoin crea ed emette una nuova moneta, che è completamente fuori dal controllo governativo o bancario. Si potrebbe profilare, in altre parole, il rischio di una pericolosa immissione di nuova liquidità sul mercato, che non è controllata né autorizzata dalle autorità monetarie. Dato questo scenario, è naturale comprendere le preoccupazioni e gli interrogativi attorno agli effetti che Bitcoin possa avere sull'intera macroeconomia. Bitcoin punta inoltre a garantire una maggiore riservatezza nelle transazioni. Tuttavia, l'anonimità non può considerarsi assoluta; si parla, piuttosto, di "pseudo-anonimità". Sebbene, almeno in apparenza, la

tracciabilità non sia sufficientemente forte da risalire all'identità dei singoli operatori, ogni transazione è concretamente e potenzialmente tracciabile. Il sistema funziona tramite un meccanismo di doppia chiave, pubblica e privata. Tutte le transazioni, per essere identificate e successivamente autorizzate, necessitano di entrambe le chiavi, che sono facilmente assimilabili allo username alla password per accedere alla posta elettronica, ad un social network, ad un sistema di internet banking o a qualunque servizio online. Delle due, solo la chiave pubblica sarà visibile al pubblico. La chiave privata servirà al singolo utente per "confermare" la transazione. Inoltre, per garantire una maggiore sicurezza il sistema predispone la possibilità di generare una serie infinita di coppie di chiavi in capo ad ogni utente (da cui, la crescente difficoltà nell'identificare il soggetto a cui appartengono, di volta in volta, le varie chiavi). La possibilità di risalire al soggetto fisico è poi insita nella stessa blockchain che, rendendo pubbliche tutte le informazioni sulle transazioni e le relative chiavi identificatrici, consente di ricostruire tutte le entrate e le uscite di un utente giungendo infine ad identificarlo fisicamente qualora una delle sue transazioni sia in qualche modo legata al mondo reale. Si può dunque asserire che, sebbene le evidenti difficoltà di tracciabilità originate dal sistema, la pseudo-anonimità preserva una possibilità di intervento delle autorità pur provvedendo a tutelare maggiormente la privacy degli utenti.

3.3 - La moneta “a prova di censura”

“Una valuta digitale anonima e a prova di censura”: così l’Electronic Frontier Foundation (Associazione no profit che si occupa di libertà civili all’interno del contesto digitale) definisce il Bitcoin, relativamente al fatto che qualsiasi transazione avvenga tramite questa valuta, risulti non tracciabile né censurabile. Ne deriva uno degli aspetti più discussi sul tema: se da una parte esiste il dubbio circa l’effettiva esistenza dell’anonimato, dall’altro ci si domanda se questo possa essere considerato un bene o meno. Relativamente al primo punto: per quanto a livello puramente teorico sia impossibile ricollegare una transazione all’individuo che l’ha effettuata, nella realtà, occorre tenere presente che vengono sempre lasciati degli “indizi”: ad ogni transazione; movimento; inserimento di Bitcoin in un wallet corrispondono sempre elementi che possono facilmente essere individuati attraverso sistemi di tracciamento, i quali sono già a disposizione delle agenzie governative. Basti pensare alla semplice raccolta storica di dati che, se analizzati da esperti, possono facilmente condurre all’individuazione di un profilo univoco. Relativamente al secondo aspetto: naturalmente è intuibile, una volta assunto l’anonimato come condizione verificata nella maggior parte dei casi, quanti aspetti positivi e allo stesso tempo negativi esso possa apportare: l’anonimato facilita ovviamente tutte quelle operazioni illegali che necessitano di tale condizione per la loro realizzazione. Esistono tuttavia aspetti positivi di portata non indifferente: chiunque, nel rispetto delle leggi, può sfruttare la

condizione di anonimato nello svolgere le proprie attività sottraendosi al controllo perenne delle autorità. Occorre inoltre tenere presente come in molti paesi, caratterizzati ad esempio da una tassazione particolarmente alta o dal prelievo (di denaro contante) limitato e ristretto, l'alternativa proposta da una moneta anonima e autonoma potrebbe risultare particolarmente interessante, soprattutto in un'ottica di attrazione per nuove forme di investimento.

3.4 - Bitcoin come "contante digitale"

Il sistema Bitcoin ha tuttavia il limite di poter funzionare solo per mezzo del bitcoin valuta; in altre parole, nonostante la nascita di piattaforme di scambio dedicate abbia in parte ovviato a tale problema, gli utenti della rete Bitcoin possono trasferirsi solo e soltanto bitcoin. All'interno di questo contesto, per una piena affermazione di Bitcoin è necessario che la valuta proposta sia in qualche modo preferita alle valute a corso legale, in forza di caratteristiche che maggiormente soddisfino le esigenze dell'utilizzatore. Prima dell'avvento delle criptovalute, era d'uso comune suddividere la moneta circolante essenzialmente in due categorie, le valute fisiche (come il contante) e le valute elettroniche (come i depositi presso un conto corrente bancario). Il contante ha il pregio di essere facilmente accessibile da chiunque, senza il bisogno di essere titolari di un conto corrente presso una banca o in possesso di dispositivi elettronici. Inoltre, è privo di costi di transazione ed è anonimo, in quanto colui che usufruisce del contante non ha il dovere di indicare la propria identità, né tantomeno il beneficiario o la

causale del pagamento. Con l'avvento della moneta elettronica, che si può ricondurre alla creazione della prima carta di credito nel 1958, l'economia ha ottenuto un nuovo sistema di pagamenti che ha introdotto numerosi vantaggi, come quello di un più agevole utilizzo, l'essere infinitamente divisibile e consentire il pagamento a distanza tramite il telefono o internet; d'altra parte, questa tipologia di moneta necessita obbligatoriamente di un coordinamento e una gestione da parte un intermediario e per gli utilizzatori ha lo svantaggio di essere sempre tracciabile. L'intento di Bitcoin è quello di inserirsi a cavallo di queste due monete, di coniugare ed unire a sé i vantaggi dell'una e dell'altra tipologia. Per questo motivo è stato da molti ribattezzato come "contante digitale": Bitcoin tenta di carpire tutte le facilitazioni elettroniche tipiche della moneta "digitale", conservando allo stesso tempo l'anonimità garantita dalla moneta fisica, il "contante", e l'indipendenza dall'intermediazione di un soggetto terzo.

3.5 - Blockchain

La blockchain è probabilmente l'innovazione più importante di Bitcoin. Essa consiste in un database che annovera tutte le transazioni eseguite nella rete Bitcoin durante tutta la sua storia, una sorta di registro digitale unico, distribuito, pubblicamente consultabile, permanente e resistente ad alterazioni, mantenuto "in vita" dall'attività congiunta di tutti i nodi del sistema. È possibile vederlo come un'evoluzione del libro mastro, un registro contabile delle sole transazioni in bitcoin. In particolar modo, nella blockchain sono annotate sia l'importo della

transazione che la sigla (lo "pseudonimo") corrispondente a chi la compie. La blockchain è articolata in blocchi di transazioni: ogni nuovo blocco od insieme di operazioni è legato al precedente, formando di riflesso la catena dei blocchi (da cui, appunto, "blockchain"). L'ultimo blocco al termine delle maglie della catena è temporalmente posteriore ad ogni blocco che precede. Avendo accesso al blocco più recente, ogni utente può seguire la catena all'indietro per osservare ogni transazione in bitcoin fatta in precedenza. Tramite questo meccanismo, tutte le transazioni sono perfettamente tracciabili; in questo modo è inoltre risolto per la prima volta il problema della double-spending in maniera distribuita, ossia il sistema assicura che soltanto i reali possessori di una somma possano spenderla, servendosi di un meccanismo a firma digitale tramite chiave pubblica, che verrà successivamente spiegato nel dettaglio. Il funzionamento della blockchain è governato da leggi matematiche e dal software, senza dipendere da alcuna entità di controllo centrale, mentre eventuali modifiche a questo non possono essere effettuate da un singolo nodo. Come anticipato, è tutta la Rete che è adibita al suo controllo, a valutare ed eventualmente integrare le innovazioni proposte da un nodo, tramite un meccanismo di votazione ed approvazione a maggioranza. L'innovazione apportata dalla struttura della Blockchain è risultata talmente importante e funzionale che diversi individui hanno proposto di utilizzarla anche in altri ambiti, come ad esempio quello politico, giuridico, sociale e scientifico. In qualità di registro pubblico irreversibile ed inalterabile per documenti, contratti,

proprietà e beni, la Blockchain può essere utilizzata per contenere informazioni e istruzioni, con applicazioni come gli smart contract o multisignature transaction. Gli smart contract sono contratti informatici in grado di entrare in esecuzione e far rispettare le proprie clausole senza un intervento di un soggetto terzo alle parti. Uno smart contract può prevedere una serie di obblighi, clausole, benefici e sanzioni che sono a carico di una o di tutte le parti del contratto, nelle diverse circostanze. A differenza dei contratti tradizionali, questi contratti possono ricevere informazioni come input e, dopo un'elaborazione basata sulle regole definite, eseguire delle azioni come output. Una delle "nuove" criptovalute che ha incluso l'uso di smart contract nella blockchain è Ethereum. Le transazioni multisignature sono d'altra parte transazioni che possono essere eseguite solamente se c'è l'autorizzazione da parte di più soggetti. Di particolare interesse sono i multisignature script, utilizzati nel commercio online per assicurarsi di avere indietro la somma inviata se la merce non è spedita. Anche in questi casi, il vantaggio introdotto dalla blockchain è quello di non imporre più il bisogno di una terza parte di fiducia per l'esecuzione dei contratti, come un notaio od un intermediario; la piattaforma permette un'esecuzione automatizzata ed affidata alla crittografia, cosa che consente maggiormente di proteggere i partecipanti da rischi di illeciti e che allo stesso tempo riduce le spese di gestione delle pratiche stesse. La blockchain dunque aggiunge una componente non indifferente di maggior trasparenza e di efficienza nella gestione dei costi, nonché anche in

questo caso priva l'esecuzione dei contratti della discrezionalità tipica del fattore umano. Alla luce di questa serie di implicazioni, la blockchain può rivelarsi un'innovazione rivoluzionaria per molte tipologie di contratti e numerose attività di business.

Cenni generali sulle altre criptovalute

Il successo del progetto di Satoshi, unito all'allettante prospettiva di guadagno ed una buona dose di creatività, ha aperto ad una massiccia proliferazione di nuove criptovalute, anche chiamate "alt-coin" (alterative coins), realizzate per i più svariati fini e operative in sempre più eterogenei settori. Basti pensare che, il 1° aprile 2017, il sito coinmarketcap.com annoverava circa 780 diverse monete virtuali ed il loro numero è tutt'oggi in continuo aumento, sebbene alcune di queste siano rimaste sul mercato per un periodo piuttosto breve. La struttura di queste nuove valute non è molto diversa dallo standard realizzato da Bitcoin, infatti nella maggior parte dei casi i programmatori-ideatori hanno preferito implementare piccole differenziazioni rispetto a drastiche modifiche: si possono facilmente riconoscere valute che introducono migliorie tecniche nel protocollo (come, ad esempio, Litecoin), altre che puntano sul rafforzamento dell'anonimato o che si differenziano per la quantità o il taglio disponibile in modo da favorire micro-transazioni (Dogecoin), o ancora valute di recentissima ideazione emesse per favorire l'adozione di comportamenti socialmente od eticamente auspicabili

(Zipcoin). Di portata più rilevante sono le innovazioni introdotte da Nautiluscoin e Friecoin: la prima, attraverso la creazione di un apposito fondo di stabilizzazione, tenta di sopperire al problema dell'alta volatilità che normalmente caratterizza tutte le valute virtuali; la seconda invece istituisce una "tassa di stazionamento", ossia un prelievo forzoso del 5 per cento su tutti i depositi dormienti, in modo da favorire un più frequente utilizzo e una maggior circolazione della moneta. Una nota a parte meriterebbero Ethereum e Ripple, che risultano ad oggi alcuni dei progetti più ambiziosi ed innovativi nell'ambito delle criptovalute e che stanno catturando sempre maggiore interesse da parte di numerosi stakeholder. Sostanzialmente, come Bitcoin, Ethereum è una piattaforma decentralizzata per transazioni peer-to-peer, che tuttavia si concentra principalmente sugli smart contract; il bacino di contratti (e potenzialmente di utenti) sottostanti Ethereum è dunque più ampio rispetto a Bitcoin (comprende, ad esempio, anche i contratti di assicurazione o di proprietà intellettuale) ed il sistema funziona attraverso un'apposita unità di conto, gli Ether, che il sistema utilizza per remunerare la realizzazione a tempo dei suddetti contratti. Con una capitalizzazione di mercato pari a quasi 43 miliardi di dollari, Ripple è una delle piattaforme più diffuse al mondo e una dei principali rivali di Bitcoin. Tuttavia, più che una moneta virtuale, Ripple è un protocollo internet, con cui si possono effettuare e ricevere pagamenti, sulla falsariga di Paypal. A Ripple si può associare un conto corrente di moneta reale, ed è in particolare costituito da un network, da una borsa e da una

valuta virtuale, anch'essa basata su un codice di crittografia e, come Bitcoin, punta a bypassare l'intermediazione bancaria attraverso un sistema decentralizzato peer-to-peer. La differenza principale risiede nel fatto che Ripple offre la possibilità di scambiare diverse valute, garantendo inoltre più elevati meccanismi di sicurezza grazie alla creazione di registri delle transazioni chiamati "Ledger". La contemporanea presenza sul mercato di questo elevato numero di nuove monete conduce ad una situazione di concorrenza. In questo scenario, Bitcoin gode del "vantaggio della prima mossa": se un attore è interessato ad adottare una criptovaluta al posto delle valute tradizionali, il bitcoin è la scelta più ovvia. È la più conosciuta, ha una rete di utenti più estesa ed ha costi di conversione con le valute tradizionali relativamente bassi. D'altra parte, le alt-coins possono dar vita a modifiche e migliorie sulla base degli insuccessi di Bitcoin, sfruttando i vantaggi derivanti dal giocare la "seconda mossa". Le innovative applicazioni proposte da Ripple ed Ethereum, ad esempio, sembrano accogliere un sempre più vivo interesse del mercato, però se ci si focalizzasse sulla sola capacità di fungere da moneta, è doveroso notare che nella maggior parte dei casi le alt-coin soffrono gli stessi limiti di Bitcoin. Limiti che sollevano comprensibili dubbi sull'effettiva capacità di queste di fungere da moneta alternativa. Inoltre, gli stessi utenti generalmente considerano le nuove alt-coin alla stregua di forme di investimento speculativo piuttosto che come tipico mezzo di scambio. Il motivo è tutto da ricercare nella forte variabilità del loro valore, poiché, equiparate ad attività

finanziarie e non a valute vere e proprie, sono dominate dalle dinamiche tipiche dei mercati finanziari, tutt'altro che stabilizzatrici. La mancanza di strumenti di stabilizzazione del potere di acquisto legati alla gestione dell'offerta di moneta contribuisce ad aumentare l'ampiezza delle variazioni dei prezzi (si ricordi che, le valute digitali basate sulla tecnologia blockchain hanno per la stragrande maggioranza un'emissione di moneta esogena e predeterminata). Da queste considerazioni si può supporre che, sebbene la prospettiva di un "sorpasso" da parte di una o più alt-coin sia interessante e poggi le basi su solide motivazioni, la sensazione generale tende ad essere di forte scetticismo circa questa possibilità. Tuttavia, quali sono le implicazioni della concorrenza? La questione ha indotto la dottrina ad interrogarsi sui possibili effetti che la libera concorrenza possa avere sulla qualità del bitcoin e sulla sua funzione monetaria, senza però convergere verso una visione comune; in particolare, ci si chiede se la competizione fra una molteplicità di monete digitali possa comportare un problema o se si incaricherà di far emergere quelle maggiormente capaci di assicurare ai loro utenti un potere di acquisto ragionevolmente costante. In accordo con la corrente keynesiana, la presenza di una pluralità di monete deve essere necessariamente vista come un problema da risolvere ed una situazione da contrastare, in quanto si pone quale ostacolo verso il raggiungimento dell'obiettivo di unificazione monetaria. Di opinione diametralmente opposta è quella parte di dottrina di area liberista che, ispirata alle idee di von Hayek, è favorevole al free banking, reputando tale

pluralità come un'opportunità ed una ricchezza da promuovere in vista di un miglioramento della competitività non solo del sistema monetario, ma di tutta l'economia globale.

CONCLUSIONE

È forse ancora troppo presto per dare un giudizio definitivo sulla realtà Bitcoin, quello che sappiamo per certo è che la realtà BTC ha rappresentato, e tutt'ora rappresenta, un vero e proprio attacco al controllo autoritario dello stato sulle riserve monetarie: rende possibile un libero mercato, nonostante l'ostilità delle legislazioni. Infatti non ci troviamo semplicemente di fronte alla prima moneta elettronica totalmente indipendente e libera, soggetta a convertibilità con altre unità attraverso il cambio di valuta; quanto piuttosto ad un sistema che sembra in grado di capovolgere e rendere inutili le attuali teorie monetariste così come la tecnica bancaria tradizionale.

La realtà delle criptovalute è vista da alcuni come un rischio ma da altra come un grande opportunità e per coglierla in modo profittevole occorre che l'esperienza e la piena consapevolezza dei cambiamenti che sono in atto prevalgano su quel tipo di euforia generica ma soprattutto confusa che solitamente circonda queste tematiche.

Occorre sì riconoscerne gli aspetti positivi e rivoluzionari, ma allo stesso tempo individuare e ponderare anche i punti deboli e le meno o più evidenti falle. D'altra parte, si tratta in ogni caso di un sistema informatico, e in quanto tale comprende sempre un potenziale bug, un malfunzionamento, a prescindere dalla profondità in cui giace l'errore.

Le opinioni ancora oggi dopo molti anni dalla sua nascita sono molteplici, nonostante il suo valore sia cresciuto vertiginosamente negli ultimi anni fino ad arrivare ad un prezzo attuale di 40 mila euro per singolo Bitcoin, molti critici sono dell'ipotesi che si tratti solo di una bolla speculativi pronta a scoppiare.

Dalla parte opposta invece troviamo coloro che sostengono che il valore di un singolo Bitcoin possa arrivare anche a 100 mila euro, molti sono convinti che questa moneta abbia un asset decisamente solido. Tra i numerosi sostenitori troviamo ad esempio Steve Wozniak, co-fondatore di Apple, ha da poco espresso un giudizio positivo in merito al Bitcoin considerandolo come il miracolo matematico più grande di sempre e che rappresenta l'equivalente digitale dell'oro.

BIBLIOGRAFIA E SITOGRAFIA

Economia e gestione delle imprese, F. Fontana, M. Caroli, McGraw-Hill Education, 2017.

Amato M. e Fantacci L., "Per un pugno di Bitcoin", Egea, Università Bocconi Editore, 2016.

Capoti D., Colacchi E. e Maggioni M., "Bitcoin Revolution: La moneta digitale alla conquista del mondo", Ulrico Hoepli Editore S.p.A, 2015.

Jay Palmer Fawcett, "Bitcoin regulations and investigations: A proposal for U.S. policies", ProQuest LLC, Ann Arbor, 2016.

Mancini M., "Valute virtuali e Bitcoin", Il Mulino, 2015.

Luther W. L., "Bitcoin and the Future of Digital payments", The Indipendent Review, 2016.

Capoti D., Colacchi E. e Maggioni M., "Bitcoin Revolution: La moneta digitale alla conquista del mondo", Ulrico Hoepli Editore S.p.A., Milano, 2015.

https://it.wikipedia.org/wiki/Bitcoin

https://www.consob.it/web/investor-education/criptovalute

https://www.exeo.it/Start/Index.aspx

https://cryptonomist.ch/

https://www.digital-leaders.it/

RINGRAZIAMENTI

Il lavoro svolto per scrivere la presente tesi di laurea è stato estremamente stimolante, assolutamente fondamentale è stato il supporto delle persone che mi sono state accanto e con cui mi sono confrontato in questo ultimo periodo.

In primo luogo vorrei ringraziare il Prof. Mariano Cesari per avermi avvicinato e accresciuto la mia curiosità, tramite le sue lezioni, verso la Digital Economy. Tema attuale soprattutto per quanto riguarda l'aspetto del Bitcoin ed è proprio per questo che ho scelto il Prof. Mariano Cesari come relatore di questa tesi.

Un enorme ringraziamento anche al Dott. Francesco Tonelli per la sua disponibilità e la competenza dimostrata.

Questo lavoro è anche merito del supporto delle persone che mi sono sempre state vicine nella vita quotidiana, primi tra tutti i miei genitori, mio fratello Davide e i miei nonni che non hanno mai esitato a starmi accanto e darmi sempre il loro sostegno in ogni momento.

Un ringraziamento speciale a colui che considero come un fratello, un amico, una spalla, Matteo, con cui ho condiviso questo intero cammino universitario e non solo…

Infine ringrazio gli amici di una vita con cui sono cresciuto e i miei compagni di corso più stretti, divenuti molto di più che semplici compagni di studio, con cui ho condiviso questo importante percorso.