Capitolo I – Le criptovalute

Sommario: 1.1 Nozioni generali sulle criptovalute. - 1.1.2 Bitcoin. - 1.2 L'evoluzione blockchain. - 1.2.1 Litecoin. - 1.2.2 Ripple. - 1.2.3 Dogecoin. - 1.2.4 Tether. - 1.2.5 Ethereum. - 1.2.6 Binance coin. - 1.2.7 USD COIN. - 1.2.8 Binance USD e BINANCE-PEG BUSD. - 1.2.9 Cardano. - 1.2.10 Solana.

1.1. Nozioni generali sulle criptovalute

Nel corso degli ultimi 20 anni i mercati e gli strumenti finanziari si sono evoluti per rispondere alle esigenze di una società in continua evoluzione, una fra tante velocizzare le transazioni.[1] Gli strumenti utilizzati per lo scambio di beni e servizi sono noti come denaro. Tuttavia, in ragione di un rapido progresso tecnologico, la società è diventata sempre più dinamica e orientata alla velocità e per rispondere a queste esigenze è stato necessario creare nuovi strumenti di scambio, sempre più sofisticati. Negli ultimi anni, nonostante molti non vogliano ammetterlo, uno degli strumenti idonei a rivoluzionare il sistema di pagamento internazionale, e non solo, sono state le criptovalute.

In parole semplici, a cosa ci riferiamo quando parliamo di "criptovalute"? Si tratta di una forma di rappresentazione di valore digitale che, in quanto tale, non può essere scambiata o conservata come una normale banconota e, pertanto, le criptovalute vengono definite anche come valute virtuali. Il termine è composto dall'unione di due parole: cripto e valuta. Con il termine cripto si indica qualcosa di *«nascosto, coperto, simulato»*[2], poiché il funzionamento delle criptovalute si basa sulla crittografia; infatti, possono essere utilizzate solo da chi conosce una specifica "chiave di accesso". Il

[1]BUNJAKU, Flamur; GJORGIEVA-TRAJKOVSKA, Olivera; MITEVA-KACARSKI, Emilija. Cryptocurrencies–advantages and disadvantages. *Journal of Economics*, 2017, 2.1: 31-39.

[2] https://www.treccani.it/vocabolario/cripto/

termine valuta, invece, si riferisce al loro utilizzo, ossia quale mezzo di scambio per l'acquisto di beni e servizi. Ad oggi, purtroppo, non esiste una vera e propria definizione ufficiale di criptovaluta, tuttavia, la Direttiva 2018/843/UE del 30 maggio 2018 ci permette di comprendere cosa non sia una criptovaluta, grazie alla seguente definizione: *"una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo status giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente"*[3]. Sembra indubbio, dunque, che l'emissione e la gestione delle valute virtuali non siano soggette ad alcuna autorità di vigilanza e che le criptovalute, in generale, non debbano essere obbligatoriamente legate ad una valuta legale. La singolarità della criptovaluta deriva dalla possibilità di effettuare scambi in maniera diretta (secondo modalità "peer-to-peer"[4]) e senza la presenza di intermediari finanziari terzi. Infatti, al contrario delle banconote, che sono strumenti sottoposti al controllo degli enti governativi e delle banche, le criptovalute sono totalmente indipendenti e libere da qualsiasi controllo centrale. Per poter utilizzare le criptovalute, infatti, è sufficiente avere a disposizione un qualsiasi dispositivo in grado di connettersi alla rete Internet.

Ma come vengono scambiate e gestite le criptovalute?[5] Lo scambio di una qualsiasi criptovaluta è regolato da un protocollo informatico che determina le regole per poter effettuare le transazioni. Per descrivere questo fenomeno si fa spesso utilizzo della frase

[3] Direttiva UE 2018/843 del 30 maggio 2018, art. 1 (d), cfr. Parlamento Europeo (2018). La definizione di "valuta virtuale" è stata introdotta nell'ordinamento italiano con il d.lgs. n. 90/2017 (art. 1, comma 2, lett. qq) che modificava il d.lgs. n. 231/2007. La definizione è stata nuovamente aggiornata dal d.lgs. 4 ottobre 2019, n. 125, che ha aggiunto: *"la rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalita' di investimento e trasferita, archiviata e negoziata elettronicamente"*.

[4] Termine con cui si designa, in telematica, un sistema (spesso abbreviato nella forma *P2P*) che consente a un utente di scambiare informazioni, programmi, banche dati e materiali con altri utenti in quel momento collegati, in un regime di assoluta autonomia (senza cioè passare per un server centrale). [Treccani]

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

"the code is law"[6], ad indicare che il codice (informatico) è legge, ed è al di sopra di ogni volontà di intervento umano. La maggior parte dei protocolli è basata sulla *distributed ledger technology*, una sorta di libro mastro condiviso (o *blockchain*[7]), che conserva la storia delle transazioni; inoltre, l'intero sistema è gestito da una rete decentralizzata di partecipanti, chiamati **nodi**, che aggiornano, conservano e consultano il *distributed ledger*. Per servirsi in maniera sicura delle criptovalute viene utilizzata la crittografia, particolare tecnica consistente nella rappresentazione di un messaggio in modo tale che l'informazione in esso contenuta possa essere recepita solo dal destinatario[8]. In questo caso, lo strumento informatico offusca il messaggio per renderlo indecifrabile a persone non autorizzate. Storicamente, la crittografia veniva impiegata principalmente in ambito militare[9] e dai servizi segreti, per proteggere la fuga di informazioni classificate. Uno dei primi a produrre messaggi criptati fu Giulio Cesare, creando il cosiddetto Cifrario di Cesare. Tuttavia, nonostante questa lunga storia, i primi tentativi di utilizzare la crittografia per costruire valute digitali risalgono solamente alla fine degli anni Ottanta. Sicuramente, anche l'avvento di Internet ne ha incentivato l'utilizzo, creando ambienti sicuri dove poter effettuare pagamenti online.

Nel 1998, il famoso informatico Wei Dai è stato il primo a proporre una criptovaluta con il nome di B-money[10]. Nella descrizione del funzionamento del **protocollo[11] di B-money** emerge come l'obiettivo dell'informatico fosse quello di creare un sistema in grado di sostituire i servizi forniti dalle istituzioni governative e finanziarie. Il protocollo si basa sull'assunto che lo scopo di una qualsiasi comunità consista nel raggiungere

---

[6] https://www.forbes.com/sites/forbesbusinesscouncil/2022/05/17/code-is-law-during-the-age-of-blockchain/

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

[8] https://www.treccani.it/enciclopedia/crittografia/

[9] BUNJAKU, Flamur; GJORGIEVA-TRAJKOVSKA, Olivera; MITEVA-KACARSKI, Emilija. Cryptocurrencies–advantages and disadvantages. *Journal of Economics*, 2017, 2.1: 31-39.

[10] DUMITRESCU, George Cornel. Bitcoin–a brief analysis of the advantages and disadvantages. *Global Economic Observer*, 2017, 5.2: 63-71.

[11] Insieme di procedure che permettono l'instaurazione, il mantenimento e l'abbattimento di collegamenti interattivi fra soggetti trasmittenti e riceventi. La definizione del p. di comunicazione permette di far cooperare entità di comunicazione remote stabilendo la corretta sequenza di procedure da usare nello scambio di informazioni, nonché le temporizzazioni degli eventi associati. [Treccani]

un'efficace cooperazione tra tutti i partecipanti. Tale cooperazione richiede, però, un mezzo di scambio veloce (tendenzialmente il denaro) per evitare di affidarsi alla pratica del baratto. Inoltre, insieme ad esso, risulta necessario un sistema in grado di far rispettare i contratti all'interno della comunità, senza non può mai essere garantito il buon esito di uno scambio di una merce con l'altra. Il protocollo risolve questi problemi prevedendo l'associazione ad ogni individuo di un conto che definisca la proprietà del denaro. Il conto non è identificabile tramite nome e cognome del proprietario, ma viene associato ad uno pseudonimo digitale (ad esempio una chiave pubblica), con la quale si entra a far parte di una rete dove ogni messaggio è firmato e criptato dal mittente al suo ricevitore. Il protocollo determina, poi, delle regole per aggiornare il saldo del conto. All'interno della comunità è possibile creare denaro risolvendo un problema computazionale irrisolto. Il premio per la risoluzione del problema consta in unità monetarie ed è parametrato al costo della potenza di calcolo utilizzata dal partecipante per risolvere il problema. Tutti gli altri partecipanti alla rete avranno, così, un credito di X unità monetarie con chi ha condiviso la soluzione. Ogni membro della comunità che volesse trasmettere unità monetarie di cui è proprietario attraverso un contratto, lo potrà fare comunicando tramite pseudonimi. I contraenti possono rendere un contratto valido solamente designando un arbitro obbligato ad intervenire in caso di disputa e accantonando una somma a titolo di risarcimento su di uno speciale conto identificato tramite un *security hash*,[12] il quale racchiude le informazioni dell'intero contratto. Ogni partecipante deve firmare il contratto contenuto nell'*hash* utilizzando la propria chiave privata. Infine, per concludere il contratto, ogni contraente invia un messaggio all'intera comunità e alcuni nodi, definiti **server,** conservano le informazioni relative

[12] È una funzione non invertibile in grado di ricevere un qualsiasi input espresso come una stringa di dati di qualsiasi lunghezza e restituire una stringa di lunghezza prefissata, detta digest. La parola viene dal verbo inglese to hash, ovvero sminuzzare, pasticciare, che designa originariamente una polpettina fatta di avanzi di carne e verdure; per estensione, indica un composto eterogeneo cui viene data una forma incerta: *"To make a hash of something"*. Nelle applicazioni crittografiche la funzione di hash ha 3 proprietà: il medesimo input restituirà sempre il medesimo output, a patto che sia utilizzato lo stesso algoritmo; due stringhe in input differenti daranno sempre outputs differenti; la funzione di hash non è mai reversibile, dunque dall'output è impossibile risalire all'input. Tale funzione è utile per rappresentare in poco spazio informazioni complesse e verificarne rapidamente l'autenticità, consiste, sostanzialmente, in una "impronta digitale" di dati digitali. Infatti, disponendo dell'informazione, è sufficiente calcolare nuovamente l'hash dell'informazione e confrontarlo con il precedente.

all’aggiornamento dei conti**.** Questi soggetti sono collegati tra loro secondo sistema **Usenet**[13], ossia una rete formata da migliaia di server tra loro interconnessi, ognuno dei quali raccoglie articoli (news, messaggi, o post) che le persone aventi accesso alla rete stessa inviano ad un archivio ad accesso pubblico, organizzato secondo gerarchie tematiche che contengono varie discussioni sullo stesso tema. I partecipanti ad una transazione devono verificare che il messaggio sia stato ricevuto ed elaborato da un sottoinsieme di server. Per far sì che i server siano affidabili, Wei Dai ha ipotizzato un meccanismo attraverso il quale ogni server deposita su un conto speciale una somma a titolo di multa o premio per comportamenti non conformi. Inoltre, i server sono obbligati, periodicamente, a comunicare la quantità di denaro creato e le loro proprietà, in modo da controllare che la somma totale dei saldi dei conti non sia superiore alla quantità totale di denaro creato, scongiurando, così, ogni possibilità che i server, in caso di collusione totale, possano creare moneta a costo zero. Dall’analisi di questo protocollo traspira vivamente l’intento di creare un sistema dotato di un mezzo di scambio efficiente e in grado di far rispettare i contratti. L'obiettivo dei cosiddetti cripto-anarchici sembrava, così, più vicino: diventare indipendenti da intermediari finanziari e liberarsi dalla morsa del capitalismo corporativista, in cui il controllo indiscriminato della creazione di moneta è la minaccia più grave. Questo protocollo, tuttavia, risultava essere ancora ben lontano dai sistemi blockchain di cui parleremo in seguito, ma certamente ha gettato delle basi fondamentali per la creazione di Bitcoin.

Un altro importante passo è stato realizzato nel 2005, quando Nick Szabo, uno scienziato informatico, pubblicò sul suo sito web un post su **Bit-Gold**. L’idea di Szabo scaturì dall’analisi dei problemi derivanti dall’utilizzo del denaro nel sistema economico occidentale e dalle funzioni di beni rifugio dei metalli preziosi. La moneta, così come la conosciamo, ed il valore ad essa associato dipendono dalla fiducia che l’intera comunità

[13] L'espressione *usenet* è una parola macedonia, dall'inglese *user network*, traducibile in italiano con "rete utente".

ripone su degli enti terzi, ovvero le autorità centrali che la emettono. Tuttavia, i numerosi episodi inflazionistici ed iperinflazionistici che si sono succeduti nel corso della storia costituiscono prova di una fiducia mal riposta. La soluzione di Szabo consiste in un protocollo in base al quale *bit* infalsificabili potrebbero essere creati *online* con una dipendenza minima da terze parti fidate, in modo da poter essere archiviati, trasferiti e analizzati in modo sicuro. La proposta per Bit Gold si basa sul lavoro di calcolo per ottenere una stringa di *bit*, partendo da una stringa di sfida e usando funzioni chiamate "**funzione puzzle client**", "**funzione proof-of-work**[14]" o "**funzione benchmark sicura**". Il protocollo prevede la creazione, su di una rete pubblica, della stringa di sfida. Un utente della rete (che chiameremo Alice) risolve il problema generando una nuova stringa di *bits* utilizzando la funzione Proof-of-Work (PoW), ossia la prova del lavoro di calcolo effettuato. Per assicurare questa prova, la stringa viene pubblicata sulla rete con una *timestamp* o marca temporale, ossia con una registrazione in formato cartaceo o digitale che mostri l'ora in cui qualcosa è accaduto o è stato fatto[15]. Alice aggiunge la stringa di sfida iniziale e la stringa di PoW con la marca temporale su di un Registro distribuito tra tutti i partecipanti alla rete, chiamato *distributed property title registry* o Registro titoli di proprietà bit-gold. In questo modo si eviterà di fare affidamento su di un singolo soggetto detentore del registro. L'ultima stringa creata costituirà, poi, la nuova stringa di sfida. Per chiunque è possibile verificare la proprietà di una particolare stringa di bit-gold consultando sul Registro la catena infalsificabile, in quanto condivisa e dotata di marca temporale della PoW, dei titoli di proprietà. Il possesso effettivo del singolo bit-gold non dipende dalla sola detenzione dei *bits*, ma piuttosto dalla posizione

[14] Da tradursi letteralmente con "prova di sforzo" e conosciuto anche come funzione di costo della CPU, puzzle computazione o funzione di pricing della CPU. Si tratta di un protocollo informatico che funziona secondo il concetto di richiedere un lavoro al cliente di un servizio. Normalmente il lavoro richiesto consiste nell'eseguire complesse operazioni di calcolo, comunque controllabili dal fornitore del servizio (service provider). Queste operazioni vengono poi verificate dalla rete e, una volta approvate, al cliente viene concesso l'accesso per utilizzare le risorse della rete. Si cerca, così, di impedire ai client dannosi di consumare tutte le risorse in modo incontrollato. Nasce come una misura economica per scoraggiare attacchi *denial of service* (negazione di servizio) e altri abusi di servizio, come spam sulla rete. Il primo fu creato da Adam Black nel 1997, sotto il nome di *hashcash*. Esistono due tipologie di PoW: *Challenge response* (Risposta di sfida) e *Solution-verification* (Soluzione-Verifica). Il primo sistema La maggior parte di tali schemi sono procedure iterative probabilistiche illimitate [https://academy.bit2me.com/it/que-es-proof-of-work-pow/].

[15] https://dictionary.cambridge.org/it/dizionario/inglese/timestamp

di Alice al primo posto della catena infalsificabile dei titoli di proprietà presente sul Registro condiviso. In particolare, tale catena può essere intesa come una catena di firme digitali personali, che attestano la volontà di trasferire la propria moneta. Tuttavia, la maggior parte dei tentativi di creare una criptovaluta funzionante non hanno dato esito positivo. Si è dovuto aspettare sino al gennaio 2009,[16] quando venne effettuata la prima transazione su Bitcoin ad opera di Satoshi Nakamoto.

1.1.2. Bitcoin

Bitcoin è la criptovaluta più famosa in assoluto, nonché quella con la più alta capitalizzazione di mercato. Il 31 ottobre 2008, un informatico conosciuto con lo pseudonimo di **Satoshi Nakamoto** pubblicò, sulla mailing list[17] *cypherpunk*, un messaggio con il quale sosteneva di aver lavorato ad un sistema di contanti elettronico completamente **peer-to-peer,**[18] che non necessitava della presenza di una terza parte fiduciaria. Qualche giorno più tardi pubblicò un *white paper* in cui analizzò nel dettaglio il funzionamento di questo sistema informatico. Nasce, così, il progetto Bitcoin. All'interno del *white paper,* l'autore descrive un sistema di denaro elettronico in grado di effettuare pagamenti *online* in maniera autonoma, senza alcun bisogno della presenza obbligatoria di istituzioni finanziarie. La soluzione è parzialmente fornita dal sistema delle **firme digitali**[19]**.** Tuttavia, la maggior parte dei benefici forniti dalle firme digitali risulterebbe inutile senza prima risolvere il problema della doppia spesa, ossia il rischio che un soggetto possa trasferire due volte la medesima moneta in assenza del controllo di

[16] BUNJAKU, Flamur; GJORGIEVA-TRAJKOVSKA, Olivera; MITEVA-KACARSKI, Emilija. Cryptocurrencies–advantages and disadvantages. *Journal of Economics*, 2017, 2.1: 31-39.

[17] Uno speciale indirizzo di posta elettronica, corrispondente ad un elenco di persone che dialogano tra loro su un argomento di interesse comune scrivendo messaggi che vengono poi inviati a tutti gli altri mediante tale indirizzo. [oxford Languages]

[18] Peer-to-peer (espressione della lingua inglese, abbreviato anche P2P ovvero rete paritaria/paritetica) nelle telecomunicazioni. Si tratta di una rete informatica in cui i nodi non sono gerarchizzati tra client e server fissi. Ogni nodo è equivalente e paritetico, potendo fungere sia da client che da server.

[19] Il sistema delle firme digitali si basa sull'applicazione invertita delle chiavi asimmetriche; infatti, l'utente cifra il messaggio utilizzando la propria chiave privata, mentre il destinatario utilizza la chiave pubblica del mittente per decifrarlo. Lo scopo delle firme digitali è garantire l'origine e l'integrità del messaggio, dunque che risulti autentico.

un’autorità, che faccia, così, da garante su tutte le transazioni. La soluzione proposta da Satoshi consiste in un network P2P che, grazie alla pubblicazione sulla rete dei dati di una transazione, marcati temporalmente e sottoposti a funzione di hash, crea una catena immodificabile di blocchi legati tra loro.

Analizziamo, nel dettaglio, quanto detto da Satoshi Nakamoto[20] per comprendere meglio come funziona Bitcoin. Tuttavia, prima di descrivere questo grande progetto, è doveroso fare una premessa. Nel *paper* viene usato il termine ***electronic coin,*** la cui corretta traduzione è “moneta elettronica”. Tuttavia, si rischierebbe di fare confusione con il denaro elettronico, il quale consiste in *“un valore monetario rappresentato da un credito nei confronti dell'emittente che sia memorizzato su un dispositivo elettronico, emesso previa ricezione di fondi di valore non inferiore al valore monetario emesso e accettato come mezzo di pagamento da soggetti diversi dall'emittente"*[21]. Per questi motivi, nella seguente trattazione, utilizzeremo il termine valuta virtuale. Come già accennato, una valuta virtuale consiste in una catena di firme digitali, pertanto, non si può toccare e scambiare con mano come avviene con le monete tradizionali. Più nello specifico, sono costituite da linee di codice informatico protette, dunque, per essere trasferite, è sufficiente firmare digitalmente - utilizzando la propria chiave privata - l’*hash*[22] della transazione precedente e la chiave pubblica del destinatario della transazione. Qui potrebbe emergere il problema della doppia spesa, che viene risolto, nel mondo dei pagamenti tradizionali, da un’autorità centrale con il compito di controllare ogni transazione. Al contrario, con Bitcoin, il beneficiario della transazione può verificare le firme per controllare la catena di proprietà. Il sistema funziona perché è sufficiente verificare la transazione avvenuta prima per ordine temporale; infatti, tutti i tentativi successivi di seconda spesa non vengono considerati dalla rete. Per fare ciò senza l’ausilio

[20] https://bitcoin.org/files/bitcoin-paper/bitcoin_it.pdf

[21] Testo dell’art. 55, lett. h ter della Legge n. 39 del 1° marzo 2002, attuativa della Direttiva 2000/46/CE.

[22] L' impronta hash di un testo o di un file informatico è una sequenza di lettere (a,b,c,d,e,f) e cifre (da zero a 9), lunga solitamente 64 caratteri, ottenuta applicando un particolare algoritmo di calcolo alla sequenza di bit che formano il testo o il file. Ne abbiamo già parlato nel paragrafo precedente.

di un'autorità di fiducia, è necessario annunciare pubblicamente tutte le transazioni, così che possano essere registrate nell'ordine in cui sono state effettuate. Su tale ordine di convalida deve, tuttavia, essere concorde l'intera comunità della rete. Infatti, il destinatario della transazione dovrebbe avere la prova che, all'epoca della transazione, la maggioranza dei nodi era concorde che l'operazione conservata nella catena fosse stata la prima ad essere ricevuta. Nakamoto propone, come soluzione a questo problema, un *"timestamp server"*[23], ossia un nodo della rete che si occupi di creare una sequenza di caratteri aventi lo scopo di dimostrare in quale ordine siano state generate le transazioni, associando, così, una sorta di marca temporale[24] ad ogni transazione. Sistema molto simile a quello ideato da Szabo in Bit-gol. Il server, effettuando l'*hash* di un blocco di informazioni, crea una sorta di fotografia dei dati contenuti nel blocco e, successivamente, la pubblica sulla rete *peer-to-peer* secondo le modalità di una rete Usenet. In questo modo la transazione viene marchiata temporalmente, dimostrando, così, che i dati contenuti nell'hash esistevano necessariamente al momento dell'*hashing*. Ogni *timestamp*, inoltre, include, nel calcolo del proprio *hash*, la marcatura temporale della precedente transazione, creando una catena immodificabile. Tuttavia, risulta necessario introdurre un sistema di Proof-of-Work (PoW) simile a quello che era stato creato con **Hashcash**[25] da Adam Back ma, anziché tramite posts, attraverso una rete Usenet. In senso lato, per "Proof-of-Work" si intende la risoluzione di un compito intrinsecamente difficile da eseguire ad opera di un utente appartenente alla rete. Sulla rete Bitcoin, questo compito consiste nella risoluzione di un puzzle crittografico e, in particolare, nell'aggiunta di un numero, chiamato ***nonce,*** ai dati del blocco da sottoporre ad *hash*. Si tratta del "***n****umber that can only be used on****ce***", ossia un *"*numero che può essere usato una volta sola*"*, puramente arbitrario e utilizzato in crittografia nei protocolli di autentificazione. Nella

[23] NAKAMOTO, Satoshi. Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review*, 2008, 21260.

[24] NAKAMOTO, Satoshi. Bitcoin: un sistema di moneta elettronica peer-to-peer. *Bitcoin.org*, 2008.

[25] Hashcash è un algoritmo di proof-of-work che è stato utilizzato come tecnica di contromisura denial-of-service in numerosi sistemi. Un timbro hashcash costituisce una proof-of-work che richiede una quantità di lavoro parametrizzabile da calcolare per il mittente. Il destinatario (e in effetti chiunque in quanto è pubblicamente verificabile) può verificare in modo efficiente i timbri hashcash ricevuti. Fu ideato da Adam Back come funzione antispam delle e-mail. Oggi è più ampiamente utilizzato come funzione di mining di bitcoin. (http://www.hashcash.org/)