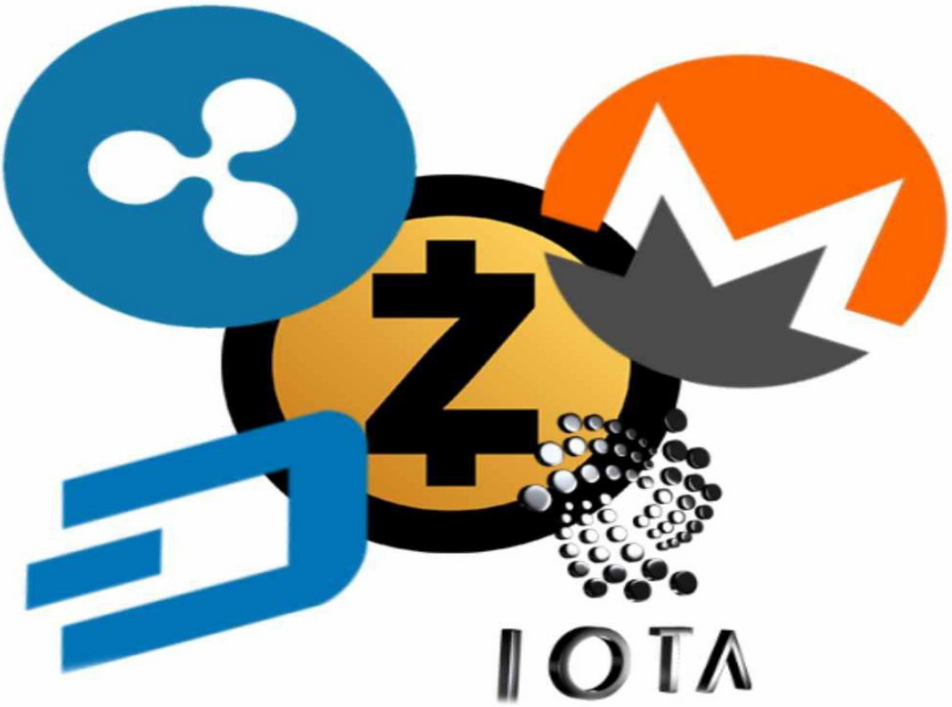

NON SOLO BITCOIN

L'oro si nasconde tra le più insospettabili altcoin

GIUSEPPE OZZIMO

Non solo Bitcoin

L’oro si nasconde tra le più insospettabili altcoin

Giuseppe Ozzimo

08/04/2019

Disamina e valutazione delle più importanti altcoin;

studio dei protocolli di consenso; considerazioni sugli aspetti fiscali riguardanti le criptovalute in Italia.

INDICE

A chi mi ha cambiato i pensieri, le parole, i progetti, la vita;
A chi ha reso il mio mondo splendido ed interessante;
a chi tramite un sorriso sa donarmi amore, pace e spensieratezza;
a chi mi ha reso più ricco, più forte e meno fragile;
a chi mi ha donato nuova linfa;
a chi darei il mondo perché per me lei è l'amore....Vanessa.

PREFAZIONE

Bitcoin è senza dubbio la regina delle

criptovalute, ma tantissime sono le altre valute digitali, definite con il termine di “altcoin”, disponibili sul mercato. Alcune portano avanti dei progetti molto interessanti e hanno davanti un futuro piuttosto roseo, altre invece sembrano destinate a scomparire in quanto rifiutate dal mercato globale. L’intento di questo libro è quello di esaminare molte tra le più importanti criptovalute

“minori”, di delinearne le peculiarità, le prospettive di crescita e i modi per poterle acquistare e conservare. Il discorso non si soffermerà ad analizzare Litecoin ed Ethereum, già oggetto di discussione nel precedente libro dal titolo “Le Criptovalute: parole semplici per definire un mondo complesso”.

Verranno anche esaminati gli aspetti

legali e fiscali delle criptovalute nel nostro Paese. Nonostante la nostra legislazione sia povera di argomenti in tema di valute digitali, esistono comunque delle importanti norme in merito da dover rispettare.

Generalmente tenterò di essere conciso e poco tecnico in modo che quanto scritto sia chiaro non solo a chi è già addentrato in questo mondo ma anche a chi si accinge ad entrarci.

Giuseppe Ozzimo

LE ALTCOIN

Con il termine “altcoin” vengono identificate le criptovalute diverse da Bitcoin. Attualmente è inutile identificarle con un numero esatto poiché sono in continua evoluzione e ogni giorno ne vengono immesse sul mercato a decine, senza considerare le ICO che vengono create giornalmente. Tra le più importanti possiamo annoverare: **Bitcoin Cash, Ripple,**

IOTA, Dash, Monero, Cardano, Zcash, Bytecoin, Neo, Stellar, Tron ed EOS. Sono queste le valute che attualmente stanno scuotendo il mercato (a parte Litecoin ed Ethereum) e che andremo ad esaminare ad una ad una. E' anche vero che non bisogna soltanto focalizzare l'attenzione su pochi e determinati obbiettivi. Quindi, anche se in questo momento ci soffermeremo su queste criptovalute molto interessanti

per il progetto su cui si fondano e per altri svariati motivi, è bene non perdere di vista il resto e fare attenzione su come si muove il mercato globale. Una visione a 360° gradi ci permette di cogliere tutte le opportunità che si presentano giorno dopo giorno, e in un mercato come quello delle criptovalute, noto per la sua estrema “volatilità”, è essenziale essere perennemente attenti

ed informati – per fare un esempio pratico, ho visto, in un paio di ore, monete valutarsi e svalutarsi di centinaia e centinaia di euro -.

Il mondo delle altcoin è molto interessante per molti aspetti: anzitutto la maggior parte di esse presentano dei prezzi accessibilissimi e quindi per acquistarle si richiedono dei capitali piuttosto esigui; e in secondo luogo, molte tra di esse fanno capo a dei

progetti piuttosto interessanti e che in prospettiva potrebbero essere anche migliori di Bitcoin.

Pertanto, come si riconoscono le altcoin che potrebbero essere redditizie nel tempo? La prima cosa da fare è spulciare tra i siti web delle varie altcoin ed esaminare i progetti che propongono i loro creatori. Bisogna poi documentarsi sull'effettivo utilizzo delle

tecnologie proposte per capire se qualcuno applica o abbia intenzione di applicare realmente quanto viene offerto. Solo così è possibile determinare se una criptovaluta sia più o meno diffusa. E' anche vero che bisogna essere dotati di un minimo di fortuna quando si va a puntare su un obbiettivo, perciò è necessario andarci cauti, almeno inizialmente, investire capitali non esagerati e stare attenti a quanto e a

come l’utilizzo di una valuta si espande nel tempo. E’ impossibile stabilire con esattezza il tempo in cui una moneta digitale possa eventualmente “esplodere” e accrescere in modo esponenziale il suo valore. La pazienza molto spesso è l’unica arma da utilizzare. Se si è frenetici e se si ritiene di poter diventare milionari nel breve periodo è meglio cambiare strada e non

entrare affatto all'interno di questo mondo. Anzitutto è giusto precisare che ogni criptovaluta non nasce per fare in modo che l'utente speculi sul suo valore. Piuttosto, queste nascono per far fronte a determinate esigenze dell'economia e più in generale della vita quotidiana. Proprio per questo alla loro base esiste un progetto che contiene delle iniziative che possono far fronte a svariati problemi: la lentezza nei pagamenti da

parte degli istituti bancari, l'inoperatività dei contratti senza l'intervento di intermediari, ecc.. Deriva da questo, quindi, l'importanza dei progetti che vengono promossi dai vari creatori, che possono determinarne la maggiore o minore diffusione della moneta – e tutti sappiamo che il mercato delle criptovalute si basa sulla fiducia che gli utenti hanno nei confronti di esse:

più una moneta viene utilizzata, scambiata e diffusa più il suo valore cresce -. Che si possa poi speculare sul valore delle criptovalute è un altro conto e senza dubbio è un metodo con il quale si possono ottenere dei guadagni, ma chi punta su di esse lo fa principalmente con il fine di ottenere una soluzione ad un determinato problema: ad esempio, chi utilizza Litecoin lo fa per la velocità delle transazioni; chi utilizza la rete

Ethereum lo fa per la semplicità e la praticità con cui vengono eseguiti particolari tipi di contratti (smart-contract).

Molte tra le varie altcoin hanno un funzionamento simile a Bitcoin e generalmente si possono ottenere tramite mining o acquistandole direttamente tramite gli exchange. Tra le monete non minabili e che quindi si possono

solamente acquistare, troviamo ad esempio IOTA (IOT).

BITCOIN CASH

Bitcoin Cash è una criptovaluta nata in seguito all'hard fork del primo Agosto 2017 operato all'interno della blockchain di Bitcoin. Cosa si intende per hard fork? Per capire questo concetto bisogna anzitutto partire dal presupposto che Bitcoin si basa su una blockchain, che è un registro di tutte le operazioni svolte dai vari utenti e che è

regolata da un determinato protocollo deciso in fase di creazione. La blockchain è costituita da una catena blocchi, collegati in modo inscindibile fra di loro, in cui vengono memorizzate tutte le transazioni. Essa è distribuita fra i vari nodi e funziona perché i software che la utilizzano obbediscono allo stesso protocollo di regole per leggere, aggiungere e convalidare le transazioni. Nel momento in cui ha luogo un hard

fork (che si verifica nel momento in cui vi è un accordo fra più miner) viene variato il protocollo di regole e pertanto varia anche la catena di blocchi. Quindi, ciò che cambia, in questo caso, è soltanto il modo in cui si comporta la blockchain, mentre il codice sorgente (in sostanza, il progetto originario) è identico a quello di Bitcoin. Condizione essenziale per il successo dell'hard fork

è che più nodi aderiscano alla nuova blockchain e operino con essa. Alla fine del fork, quando più nodi avranno aggiornato i loro software al nuovo protocollo si verranno a creare due catene di blocchi differenti e incompatibili tra di loro (una che aderisce al protocollo Bitcoin iniziale e una che funziona secondo le nuove regole).

In sostanza, questo fork nasce

dall’esigenza più o meno diffusa di velocizzare le transazioni di Bitcoin. Per ovviare a questo problema Bitcoin Cash ha ampliato la grandezza dei vari blocchi di transazioni a 8 MB, a differenza della blockchain di Bitcoin che contiene blocchi di 1 MB. Così facendo ha creato un sistema capace di elaborare più transazioni contemporaneamente e in modo più

veloce. A tal proposito c'è da sottolineare il fatto che Bitcoin, nonostante sia la criptovaluta più utilizzata del momento e quella che ha acquisito maggior valore, a causa dell'enorme flusso di transazioni faccia fatica ad essere scambiato in un lasso di tempo ragionevole (a volte per validare una transazione sono necessari più giorni).

Seguendo le ultime variazioni del suo

valore (che si attesta stabilmente sopra ai 1200 €), c'è da dire che ha risentito poco delle varie crisi che hanno interessato il campo delle criptovalute e anche la sua capitalizzazione di mercato sembra non accusare troppo l'urto generato dalle ondate negative che hanno interessato l'inizio del 2018 (capitalizzazione che si mantiene sopra i 20miliardi di euro). Ciò, probabilmente,

potrebbe rappresentare una sorta di attestato di stima da parte dei vari investitori che, credendo nel futuro della criptovaluta, preferiscono mantenere la moneta piuttosto che venderla e quindi convertirla in valuta fiat.

IL FUTURO SI CHIAMA

IOTA

IOTA è una criptovaluta creata nel 2015 da David Sønstebø, Sergey Ivancheglo, Dominik Schiener e Dr. Serguei Popov, e resa utilizzabile a partire dal 2017. Nel giro di poco meno di un anno il suo valore ha subito un forte incremento (+ 500 %) e ciò è dovuto al fatto che la rete IOTA è entrata nel giro di colossi come Samsung e altri produttori di attrezzature tecnologiche. I vari token sono stati

predistribuiti sul mercato e non ne possono essere prodotti degli altri, pertanto non esiste un'attività di mining riferibile alla moneta. Il numero di IOTA distribuiti è quasi inscrivibile e impronunciabile ed ammonta approssimativamente a 2 triliardi.

Il "libro mastro" su cui si basa non è la comune blockchain che caratterizza le altre criptovalute ma prende il nome di "Tangle". Questa tecnologia è

sicuramente molto vicina a quella blockchain, in quanto è decentralizzata e quindi distribuita fra i vari nodi (cioè i vari utenti che scaricano il software IOTA sui propri dispositivi) che hanno il compito di approvare e di eseguire le transazioni risolvendo determinati algoritmi ed è consultabile liberamente da tutti gli utenti. La differenza sostanziale tra la comune blockchain e

Tangle sta nel fatto che quest'ultima non si basa su blocchi limitati che possono contenere un numero prestabilito di transazioni ma è stata progettata per associare ad ogni transazione un singolo blocco: ne consegue che sono infinite le transazioni che possono essere eseguite e validate nel medesimo istante. Tra l'altro non esistendo i miner, che hanno il compito di validare le transazioni tramite la loro attività in cambio di

commissioni più o meno alte, la rete IOTA impone un vincolo a tutti gli utenti che scambiano la moneta, per far si che ogni transazione sia del tutto gratuita: in particolare, l'utente, per poter inviare un pagamento deve necessariamente approvare due transazioni presenti sulla rete, verificando che non siano in conflitto tra di loro. Ovviamente la verifica non viene svolta fisicamente

dall'utente, ma dal nodo su cui è installato il suo wallet, che segue le regole peculiari imposte dal protocollo su cui si basa la criptovaluta.

Attualmente il wallet ufficiale di IOTA è un software che prende il nome di IRI, e una volta installato funzionerà anche da nodo.

Ma come viene utilizzata la rete IOTA e perché? Partiamo dal presupposto che il suo nome deriva da IoT, che è un

acronimo che sta ad indicare “Internet of Things”. IOTA rappresenta pertanto l’*internet delle cose*, pertanto la rete costruita attorno ad essa è stata progettata per connettervi dei dispositivi tecnologici e per consentire l’elaborazione dei dati da loro prodotti, che poi possono essere scambiati in modo semplice e veloce. In termini pratici la rete IOTA potrebbe dare voce

ai dispositivi elettronici ed elaborare, ad esempio, i dati derivanti da una semplice macchinetta distributrice di snack, permettendole di inviare nuovi ordini al suo fornitore automaticamente e quando ce n'è bisogno, di contattare in modo automatico l'assistenza in caso di guasto, ecc. Ovviamente l'acquisizione e l'elaborazione di tali dati e le operazioni che ne derivano hanno un costo che viene pagato tramite la moneta

circolante all'interno della rete che per l'appunto è IOTA.

Ciò che, quindi, potremmo acquistare tramite essa non è un bene qualsiasi ma soltanto l'uso delle apparecchiature elettroniche connesse alla sua rete, come ad esempio un quantitativo di spazio su un hard disk condiviso su di essa.

Grazie alla sua enorme funzionalità, IOTA sta raccogliendo sempre più

consensi da parte delle grandi aziende produttrici di materiali tecnologici. E' un progetto ancora in via di sperimentazione e in via di ottimizzazione, ma le buone premesse per una crescita futura ci sono tutte, anche perché gli scambi di valuta sono del tutto gratuiti tanto da rendere possibili anche micro-transazioni che hanno ad oggetto piccole somme (non dimentichiamoci che per scambiare

piccole somme di critptovalute come Bitcoin è quasi impossibile a causa delle fee elevate e dei tempi di approvazione molto elevati).

DASH: VELOCE E PERFETTAMENTE ANONIMO

Dash è una criptovaluta nata nel 2014 e prima di essere così denominata ha assunto l'appellativo di XCoin e poi di Darkcoin.

La rete che sta intorno a questa criptovaluta ha un funzionamento molto particolare, ma comunque molto efficiente in termini di velocità e di anonimità delle transazioni. In particolare si sviluppa su due livelli: uno costituito dai miner, l'altro

costituito dai cosiddetti “master nodes”. Il compito dei miner è quello di approvare le transazioni e di riportarle all’interno della blockchain; i “nodi master”, invece, possono eseguire, oltre alle normali funzioni di supervisione dell’intero sistema, delle funzioni avanzate della rete: “InstantSend” e “PrivateSend”. Si tratta, rispettivamente, delle funzioni di invio istantaneo e di

invio anonimo. Per quanto riguarda il primo servizio, gli utenti possono spedire Dash, pagando delle commissioni più elevate, in una frazione di tempo che si aggira intorno a un secondo (utilizzando il metodo standard per inviare transazioni il tempo medio di approvazione è di 2,5 minuti, nonché il tempo che la blockchain impiega per generare un nuovo blocco): non saranno quindi i miner ad approvare la

transazione, bensì i vari nodi master; per quel che riguarda il secondo servizio, innanzitutto è usufruibile solo se riguarda transazioni che hanno ad oggetto non più di 1000 Dash e consiste nell'incorporare in altre transazioni una singola transazione, rendendola difficilmente tracciabile. Anche in questo caso l'operazione viene svolta dai nodi ed è fruibile pagando una

percentuale più alta di fee.

In generale, quindi, il sistema di funzionamento di Dash può essere considerato decentralizzato, in quanto, come per tutte le altre criptomonete, non è controllato da alcun ente specifico, seppur presenta delle particolarità: anzitutto, i cosiddetti “master nodes” (per essere approvati come tali, gli utenti devono avere, prima di tutto, una risorsa di 1000 Dash a loro

disposizione, per evitare che si tratti di operatori che abbiano il solo scopo di compromettere il sistema) hanno un ruolo centrale nel funzionamento della rete poiché possono proporre sistemi di sviluppo e di modifica di quest'ultima; poi, alla base della criptovaluta risiede un gruppo di fondatori che prende il nome di "Dash Core Team", che è responsabile della diffusione e dello

sviluppo effettivo di essa. Ciò che permette a questo team di lavorare sono dei finanziamenti che derivano direttamente dalla rete. Infatti per ogni blocco che viene approvato, il 10 % del premio è riservato allo sviluppo della moneta, e saranno i vari nodi master a stabilire, tramite dei voti, a quale attività saranno destinati tali guadagni. Rimanendo in tema di premi per l'approvazione dei vari blocchi di

transazioni, il 45 % va ai nodi master e il restante 45 % va ai miner che hanno contribuito all'approvazione. E' interessante anche il modo in cui i nodi vengono scelti per approvare le varie transazioni: esiste una lista in cui essi sono trascritti in un ordine casualmente prestabilito. Per l'approvazione di una transazione particolare (come, ad esempio, una transazione privata) è

necessario il consenso del 10% dei nodi. Questa percentuale verrà scelta seguendo l'ordine riportato nella lista e una volta che avranno svolto il loro compito, questi nodi, verranno collocati in fondo ad essa.

La crescita di questa criptovaluta sembra inarrestabile, tanto che in un anno ha avuto un aumento di valore del 6000% e grazie alla sua enorme affidabilità e al continuo sviluppo

sembra destinata ad ottenere ancora maggiore diffusione. Si tratta di un valuta digitale molto versatile in quanto può essere utilizzata in ogni ambito, anche per effettuare micro-transazioni poiché ha delle fee standard molto basse. I grafici che attestano la sua enorme crescita parlano da soli, quindi c'è poco da dire circa la serietà del progetto su cui si basa, che tra l'altro è

sempre in via di sviluppo per essere reso più efficiente.

Il numero massimo di Dash che possono essere coniati è pari ad una cifra che si aggira intorno ai 18 milioni e attualmente non sono previste modifiche a tale soglia. Si tratta di un quantitativo relativamente contenuto e ciò non ha fatto altro che rendere maggiormente ricercata e appetibile la moneta sui mercati.

TRANSAZIONI SEMPRE PIU' SICURE E ANONIME CON MONERO.

Monero (XMR) è una criptovaluta nata e distribuita sul mercato a partire dal 2014 e rappresenta il risultato del primo fork di Bytecoin. Si tratta di una valuta decentralizzata e che garantisce un alto livello di privacy delle transazioni. A differenza di altre criptomonete, Monero è stata

progettata per essere minata servendosi anche delle prestazioni della propria CPU o GPU, riducendo così il rischio che si possano creare delle enormi pool di miner che influenzino le funzionalità della rete. Anche Monero si basa su una blockchain, sulla quale vengono registrate le varie transazioni: essa è distribuita tra i vari nodi della rete, che funzionano seguendo il protocollo

I2P. La rete I2P garantisce perfetta anonimità ai nodi Monero, tanto che risulta impossibile tracciare anche l'indirizzo IP degli utenti che svolgono questa funzione. Anche la blockchain si basa su un protocollo diverso rispetto a quello di altre criptovalute, che prende il nome di "CryptoNight": se all'interno della blockchain Bitcoin possiamo tracciare i vari indirizzi di

chi ha spedito una certa somma di valute, di chi ha ricevuto questa somma e anche l'importo, all'interno della blockchain Monero è possibile solo venire a conoscenza del fatto che esiste una transazione e non possiamo risalire agli indirizzi di invio e ricezione, né tantomeno all'importo di essa. Pertanto i vari blocchi che compongono questa blockchain non saranno concatenati e gli unici in grado di accedere alle

informazioni private di una transazione sono soltanto chi ha inviato e chi ha ricevuto la transazione.

La privacy delle transazioni all'interno della blockchain di Monero viene garantita da tra elementi fondamentali:

- *Ring signatur;*
- *Ring CT;*
- *Stealth address.*

Per quanto riguarda il primo elemento,

consente di rendere anonimo il mittente di una transazione, mescolando all'interno di un gruppo di altre transazioni simili il suo indirizzo pubblico; per ciò che attiene alla seconda funzione, permette l'offuscamento degli importi relativi ad una transazione; lo "stealth address", invece, serve a garantire l'anonimato di chi riceve la transazione: chi emette la transazione

dovrà creare anche un indirizzo casuale a favore del ricevente, che avrà validità solo per una specifica operazione (pertanto solo mittente e destinatario potranno conoscere i dettagli di una singola transazione). La rete Monero risulta, nel complesso, parecchio reattiva e un nuovo blocco viene aggiunto alla blockchain in media ogni due minuti. Ogni blocco

porta con se, oltre alle varie transazioni fra gli utenti, anche le cosiddette “coinbase transactions”, ovvero il totale delle commissioni da corrispondere a favore dei miner che hanno partecipato ad approvare le transazioni all’interno del blocco. Generalmente le fee per ogni transazione sono parecchio basse e i tempi di approvazione si aggirano intorno ai due minuti.

Ultimamente questa criptovaluta è finita sotto la lente di ingrandimento di vari organi di vigilanza, in quanto il suo sistema di funzionamento, perfettamente anonimo e che non lascia speranze di rintracciamento delle varie transazioni, è finito nel giro di affari che riguardano il “dark web”. A proposito, si è ipotizzato l’utilizzo di Monero per l’acquisto di armi, droga e

altre risorse illegali. Generalmente, la criptovaluta non sembra aver subito gli effetti negativi di questi avvenimenti e anzi nell'anno 2017 ha avuto una crescita del 6000%, circa, arrivando a sfiorare i 400 € di valore.

A mio modesto parere il progetto Monero non sembra proporre delle novità molto allettanti, anche perché rappresenta, per molti aspetti, una sovrapposizione del progetto Dash,

seppur con delle sfaccettature diverse. Penso, piuttosto, che il fatto di voler rendere a tutti i costi completamente anonimi sia i vari nodi sia le varie transazioni, possa essere un modo per favorire scambi di denaro occulti e per fini illegali. Comunque la sua capitalizzazione di mercato si aggira intorno ai 3miliardi e in confronto ad altre criptovalute che hanno raggiunto

livelli di capitalizzazione più alti, Monero possiede un valore di mercato maggiore. La quantità totale di monete coniabili è di 18milioni, pertanto, sulla base di questi due ultimi dati, il suo valore ha dei margini di crescita nel caso in cui attraesse nuovi investimenti.

CARDANO: LA CRIPTOVALUTA IN CONTINUO SVILUPPO

Il progetto definito dagli sviluppatori della rete Cardano è sicuramente uno fra i più interessanti dell'interno mondo delle criptovalute. Anzitutto, il progetto è stato distribuito sulla rete mondiale a partire da settembre 2017 e nel giro di pochi mesi ha avuto una crescita del 6000%, circa.

Al momento del lancio sono state

distribuite circa 31miliardi di monete fra i vari exchange e i vari finanziatori del progetto e rimangono da coniare 14miliardi di monete, per un totale di 45 miliardi. Si tratta quindi di un'emissione limitata token e il numero prestabilito in fase di rilascio non potrà essere modificato.

La differenza sostanziale tra Cardano e altre criptovalute sta nel fatto che la sua blockchain si basa su un sistema

definito con il nome di “Proof of stake” (Pos), mentre ad esempio Bitcoin si basa sul sistema di “Proof of work” (PoW). Ciò significa che all’interno della rete Bitcoin, perché vengano approvati i vari blocchi di transazioni e perché vengano coniate nuove monete, è necessaria l’attività di mining che comporta delle enormi spese di energia, tra le altre cose.

Invece, ciò che accade all'interno della rete Cardano è del tutto differente e assomiglia, in maniera molto blanda, alla rete IOTA: i vari blocchi vengono creati da particolari nodi che prendono il nome di "slot leader"(che hanno anche il compito di firmare i vari blocchi mediante le loro chiavi private e di scriverli all'interno della blockchain), anche se al processo di approvazione delle varie transazioni

partecipano anche i nodi semplici, o per essere precisi, quei nodi che abbiano un saldo positivo sul loro wallet (definiti nodi “stakeholder”). Ciò che conta al fine di essere scelto come slot leader è il saldo presente sul proprio wallet della moneta nativa delle rete Cardano, che viene definita “ADA”: maggiore è il saldo, maggiore è la probabilità di essere incluso nella

lista dei prescelti a svolgere questa funzione. Esiste, quindi, una lista elaborata sulla base di un algoritmo (ancora da definire) dei potenziali slot leader e a scegliere colui il quale sarà preposto alla creazione di un determinato blocco saranno i vari stakeholder che avranno un saldo sul proprio wallet pari, almeno, al 2% della quantità totale di monete. La scelta, però, non potrà avvenire in

modo del tutto arbitrario, in quanto è prevista una componente casuale: il sistema, probabilmente, prevede che ogni stakeholder effettui un ipotetico lancio di una moneta per scegliere il nodo predisposto alla funzione appena descritta, in modo che il risultato sia, da un lato, il frutto di un voto ma dall'altro, connotato anche da un certo grado di casualità.

La rete Cardano è stata anche concepita per supportare al suo interno l'esecuzione di smart-contract, come Ethereum. Pertanto si sviluppa su due livelli (o *layers*): il primo dove circola la moneta nativa della rete che è ADA; il secondo, invece, predisposto ad ospitare il funzionamento degli smart-contract. Altro elemento importante da

sottolineare è l'economicità delle transazioni, in quanto sono previste delle fee più basse rispetto alle criptovalute di punta, seppur potrebbero subire delle variazioni al rialzo nel caso in cui il numero delle transazioni sulla rete aumenti. Queste commissioni saranno corrisposte a favore dei nodi che hanno partecipato all'attività di creazione dei blocchi e di approvazione delle varie

transazioni.

Il discorso fatto fin quà su cardano è solo introduttivo, in quanto si tratta di una tecnologia in via di sviluppo. Effettivamente, ad oggi, i vari nodi sono rappresentati dalle varie aziende fondatrici della moneta essendo che, ancora, i vari protocolli sono in via di aggiornamento. Per evitare di creare attività sospette, i guadagni generati

dalle commissioni sulle varie transazioni, da corrispondere ai nodi slot leader, sono stati raccolti e distrutti.

Per onore di cronaca è giusto sottolineare che la rete Cardano è decentralizzata, pertanto nessuna entità ne esercita direttamente il controllo e la blockchain della rete è pubblica e distribuita fra i vari nodi. Attualmente l'unico wallet per raccogliere i propri

ADA è Daedalus e funziona anche come nodo.

Nel complesso, il progetto portato avanti si basa su un lavoro solido, che ha riscosso ampia approvazione nel giro di pochi mesi, facendo decollare il valore della criptovaluta. Bisogna capire, però, in che modo verrà ultimato e quali vantaggi offrirà sul piano concreto l'utilizzo di questa rete.

I dati sul suo funzionamento effettivo, attualmente, sono in parte basate su ipotesi in quanto il reale protocollo di rete ancora non risulta attivo al cento per cento.

Il consenso riscosso è veramente tanto, considerando che ancora il tutto è in via di sviluppo, ma il destino di Cardano sarà definibile solo quando la rete sarà funzionante in tutte le sue parti.

ZCASH, IL CUGINO “ANONIMO” DI BITCOIN

Zcash è una criptovaluta distribuita sul mercato a partire dall’ottobre 2016 ed

è nata, inizialmente, come un fork di Bitcoin. L'intento degli sviluppatori era quello di creare un sistema totalmente anonimo di pagamenti, ancor più di Bitcoin. Zcash funziona, a grandi line come tutte le altre criptovalute, pur presentano delle particolarità: si basa su una blockchain consultabile da tutti gli utenti e distribuita fra i vari nodi della rete; le

transazioni sono raccolte all'interno di blocchi e vengono approvate dall'attività dei miner.

In particolare, per ciò che attiene alle transazioni, è possibile inviarle in forma pubblica o privata: nel momento in cui si sceglie di inviare una transazione in forma privata, le varie informazioni riguardanti i dati del mittente, del destinatario e l'importo di essa saranno offuscati, seppur

registrati all'interno della blockchain tramite un codice univoco e visibile ai vari utenti (quindi è possibile risalire al fatto che è avvenuto uno scambio di monete ma non è dato sapere gli indirizzi che hanno presto parte allo scambio, né tantomeno l'importo); se invece il mittente sceglie di inviare monete in forma pubblica dalla blockchain sarà possibile accedere

solo ai dati riguardanti il valore della transazione.

Il protocollo tramite il quale le transazioni vengono verificate dai vari miner prende il nome di “Zero knowledge Proof” (che tradotto, significa “dimostrazione a conoscenza zero”) e permette la registrazione dei vari movimenti all’interno della blockchain con un livello di privacy del cento per cento. In parole povere,

anche i miner che validano le transazioni non possono risalire ai dati di esse pertanto dovranno controllare soltanto che la singola transazione aderisca a determinati parametri protocollari della rete: l'unico elemento che in mano ai verificatori della transazione, è una "stringa di riferimento", che dovrà essere esaminata e confrontata con le regole

che stanno alla base delle rete.

Per quel che riguarda il mining della criptovaluta, è importante notare che la componente hardware che lavora a tale scopo è la RAM e non più la CPU o la GPU come per altre criptovalute. Ciò permette, quindi, di rendere la moneta facilmente estraibile anche tramite un modesto pc domestico, senza troppi sprechi di energia elettrica.

Un elemento molto interessante della

rete Zcash è il protocollo di pagamento rapido BOLT, che rappresenta l'acronimo di "Blind Off-chain Lightweight Transactions" (tradotto assume il significato di "transazioni oscurate e leggere fuori catena). Questo sistema permette a due o più soggetti di accordarsi per aprire un canale privato di pagamenti, in cui le transazioni si muovono velocemente in

modo anonimo senza attendere che vengano incluse all'interno dei blocchi. All'interno di questi canali circoleranno, alla stregua della rete che si basa su Ripple, dei crediti IOU che permetteranno di muovere grandi quantità di denaro senza spostare fisicamente i capitali. Il sistema elaborato dagli sviluppatori di Zcash è molto più snello rispetto a quello previsto da Ripple. Portando un

esempio pratico, potremmo immaginare che vi siano due soggetti che acquistano l'uno dall'altro, periodicamente, dei beni e quindi devono spostare spesso delle somme di denaro. Identifichiamo questi soggetti con "A" e "B": Al momento dell'apertura del canale l'utente A deve a B 50 IOU € e l'utente B deve a quest'ultimo anche 50 IOU €.

Ammettiamo che B compri da A dei beni per un valore di 50 €, ciò che succede a questo punto è che i vecchi IOU che erano stati firmati da entrambi crittograficamente, debbano essere distrutti tramite l'assenso di entrambi che andranno ad apporre una nuova firma per dei nuovi IOU. Quindi la situazione a questo punto sarà la seguente: A avrà 100 IOU € e B 50 IOU €. Gli IOU continueranno a

muoversi all'interno del canale finchè le parti non decideranno di chiudere il canale e di liquidare il pagamento tramite qualsiasi moneta. Comunque, tutti i movimenti di IOU e tutte le operazioni di apertura e chiusura del canale dovranno essere stabilite di comune accordo e tramite l'apposizione delle firme crittografate degli utenti. Nessuna azione può essere

svolta unilateralmente e tutto avviene in completo anonimato.

Come già detto, Zcash è stato immesso sul mercato a partire dall'ottobre 2016 e al momento del lancio il suo valore si aggirava intorno ai 3000 €. Il numero massimo di monete coniabili è di 21 milioni, proprio come Bitcoin. Nei primi mesi del 2017, il suo valore ha subito una forte discesa, fino a toccare quota 20 €, per poi risalire e

attestarsi stabilmente intorno ai 300 €. Ciò che il progetto propone è, senza dubbio, qualcosa che abbiamo già visto con altre criptovalute, seppur con qualche sfaccettatura: il punto cardine è l'anonimità delle transazioni. Da non sottovalutare, però, è il protocollo di pagamento BOLT, che sarebbe molto utile da utilizzare nel campo del commercio. Molto spesso, infatti,

molte aziende che vendono prodotti di qualsiasi genere si riforniscono da altre aziende sparse in tutto il mondo, e non è facile per loro inviare e ricevere i vari pagamenti della merce in tempi brevi e senza affrontare dei cambi di valuta. In questo ambito potrebbe essere molto funzionale l'utilizzo della criptovaluta, anche se c'è molta diffidenza attorno a Zcash. L'anonimità "perfetta" non ha fatto altro che

incrementare la vigilanza dei vari governi mondiali, i quali ritengono ragionevolmente che questa valuta possa essere utilizzata per la compravendita di armi, sostanze stupefacenti, ecc.. Pertanto, è incerto il modo in cui il suo valore si rapporterà a queste continue ingerenze dei governi. E' necessario anche capire chi investe all'interno di Zcash, perché

se i maggiori investitori fossero soggetti con intenti criminali, probabilmente se venisse messa alle strette dalla legge, probabilmente si avvicinerà ad azzerare il suo valore. Pertanto prima di speculare o di acquistare importanti somme di Zcash è necessario capire se effettivamente vi sono delle aziende o dei privati che operano all'interno del mercato utilizzando questa rete, sfruttando la

sua praticità.

BYTECOIN COME MONERO

Bytecoin è una criptovaluta distribuita sui mercati a partire dal 2014 e nonostante le buone premesse con cui è

stata lanciata, ancora oggi non è riuscita a fare il salto di qualità. Questo, probabilmente, dipende dal fatto che nel tempo sono state proposte molte criptovalute con livelli di tecnologia più avanzata e affidabile che, essenzialmente, ricalcano lo schema progettuale di Bytecoin rendendolo, però, più efficiente e funzionale. Altro elemento da non

trascurare è il fatto che non possediamo un elenco esaustivo di informazioni sulla criptovaluta in questione e ciò che riusciamo a recepire, tramite la documentazione ufficiale e altre fonti presenti sul web, è solo una serie di dati abbastanza generici e poco tecnici. Questo sarà anche dovuto al fatto che il progetto è estremamente lineare, poco complesso e senza alcuna particolarità di fondo.

Ritengo inutile soffermare l'attenzione sul funzionamento della blockchain, dei nodi, ecc. perché si tratta del medesimo sistema di funzionamento delle più comuni criptovalute, ma ritengo sia più interessante sottolineare gli aspetti peculiari di questo progetto. Ciò che gli sviluppatori di Bytecoin si sono proposti di creare, è una criptovaluta veloce e dinamica, capace

di spostarsi rapidamente a livello internazionale. Mediamente per trasferire Bytecoin da un utente all'altro si impiegano due minuti scarsi; le transazioni sono gratuite e sono i miner ad elaborarle. Tutti i miner che partecipano all'approvazione delle transazioni ricevono una ricompensa che va diminuendo nel corso degli anni. La blockchain di Bytecoin si basa sulla

tecnologia *CriptoNight*, la stessa che utilizza Monero, che consente di creare delle transazioni difficilmente rintracciabili e quindi anonime.

Per rendere l'idea di quanto è grande il numero massimo di Bytecoin coniabili nel tempo, dobbiamo misurarlo in Bitcoin (BTC) per evitare di riportare cifre impronunciabili, pertanto esso ammonta a 184, 47 miliardi di BTC. Il

numero è molto elevato ed è anche elevata la possibilità che nel tempo Bytecoin si riveli soltanto un “flop”. D’altronde sistemi simili più sviluppati come Dash e Monero (derivato dal fork di Bytecoin) hanno avuto una rapida crescita. Il progetto non risulta essere originale e anzi va a ricalcare, grosso modo, quello di altre criptovalute che sono, tra l’altro, maggiormente note in termini di

efficienza. Ciò si è riflesso anche sul suo valore che ormai da anni viaggia al di sotto del centesimo di Euro. L'unico aspetto positivo è che il mining risulta essere abbastanza produttivo anche utilizzando un pc con una scheda grafica e una cpu di ultima generazione.

Per il resto è difficile cogliere degli aspetti positivi anche perché dubito del

fatto che il suo progetto possa essere puntato da grandi aziende, in quanto esistono tecnologie simili nettamente migliori.

Tra l'altro, è vero che il numero di Bytecoin è limitato, ma è come se non lo fosse, in quanto per generare un numero così alto di token sono necessari svariati anni di mining e il fatto che la data in cui l'emissione cesserà sia lontana, è un altro elemento

che non rende preziosa e appetibile

questa criptovaluta.

L’ETHEREUM CINESE: NEO

Neo è una criptovaluta sviluppata in Cina e lanciata nel giugno del 2017, anche se era già operante a partire dal

2014 sotto il nome di Antshares.

L'elemento chiave che accomuna Neo a Ethereum è la possibilità di eseguire all'interno della sua blockchain degli smart-contract, seppur in modo più semplice e funzionale rispetto alla sua diretta concorrente più conosciuta e più valutata sul mercato. Infatti, mentre gli smart-contract della rete Ethereum sono sviluppabili solo sulla

piattaforma Solidity, quelli Neo possono essere creati sfruttando il linguaggio Java, GO e Python.

Per capire come funziona la rete NEO bisogna anzitutto conoscere il protocollo che regola la creazione e l'approvazione dei vari blocchi di transazioni, che nella fattispecie prende il nome di *Delegated Byzantine Fault Tolerance* (DBFT) *algorithm* (in una traduzione

molto approssimativa assume il significato di “delegata tolleranza al problema dei bizantini”). Il nome di questo protocollo è del tutto particolare ma prende spunto dal già noto problema informatico dei generali bizantini ideato nel 1982 da Leslie Lamport, il quale spiega come raggiungere un consenso in particolari situazioni in cui esiste la possibilità

che vi siano degli errori. Andando ad esaminare il modo in cui funziona questo particolare protocollo, bisogna ammettere l'esistenza, all'interno della rete NEO, di due categorie di nodi: nodi di contabilità e nodi semplici.
I nodi di contabilità sono rappresentati o da persone fisiche o anche da aziende, il cui nome viene reso pubblico, ed hanno il compito di creare ed approvare i vari blocchi di

transazioni; i nodi semplici sono costituiti dagli utenti che detengono almeno 1 NEO ed hanno il diritto di votare l'istituzione di nuovi nodi di contabilità e il nodo preposto a creare ed approvare un nuovo blocco. Quando un nodo contabile viene nominato per approvare un blocco, esso al termine dell'operazione trasmette la sua versione della blockchain agli altri

nodi e soltanto se il 66% degli altri nodi si dimostra d'accordo con le informazioni trasmesse, allora raggiungerà un consenso. Nel caso contrario verrà nominato un altro nodo contabile per trasmettere la sua versione della blockchain, fin quando non verrà raggiunto un consenso. La scelta di ammettere due categorie diverse di nodi ha un significato molto importante: i nodi cosiddetti contabili,

preposti all'approvazione dei vari blocchi, non sono soggetti anonimi ma noti e facilmente determinabili, in modo che venga scongiurato qualsiasi tentativo di attacco illecito all'intera rete e nel caso in cui un nodo operi in maniera contraria alle norme prestabilite, esso è facilmente identificabile ed escludibile. Da ciò possiamo intuire come Neo sia

difficilmente vulnerabile al cosiddetto *51% attack* e ad altre attività hacker.

Tra l'altro questo sistema rende la rete Neo particolarmente reattiva, in quanto può arrivare a confermare fino a 10000 transazioni al secondo, a differenza della rete Ethereum che può arrivare ad approvare solo 15 transazioni al secondo.

Altra peculiarità è rappresentata dal token operativo della rete Neo che

prende il nome di GAS. Tramite di esso è possibile pagare le varie operazioni svolte all'interno della rete e tra l'altro rappresenta un "interesse" che viene corrisposto a tutti coloro che posseggono almeno 1 Neo nel proprio wallet, proporzionalmente alla quantità di Neo posseduti. Pertanto ogni qualvolta verrà approvato un nuovo blocco tutti i possessori di Neo

riceveranno dalla rete un ricompensa in GAS, che diminuirà nel tempo fino ad esaurirsi, in quanto il numero massimo di GAS coniabile è fissato a 100 milioni. Proprio come avviene per Neo, anche GAS viene quotato sul mercato ed è acquistabile (nel gennaio del 2018 ha addirittura sforato la valutazione dei 60 Dollari).

Neo può essere anche definito un progetto molto dinamico, in quanto

sono in via di sviluppo alcune implementazioni della rete, come:

- NeoX, che si propone di offrire l'interoperabilità tra più blockchain, anche tra blockchain pubbliche e private;
- NeoFS, che rappresenta un sistema semplificato di archiviazione e condivisione di file sulla blockchain;
- NeoQS, che è un sistema di

protezione per difendersi contro gli attacchi provenienti dai computer quantistici.

E’ inutile dire che questo progetto è sicuramente dotato di un altissimo potenziale di crescita, anche perché le varie migliorie che il team di sviluppo ha intenzione di apportare nel corso del tempo sono a dir poco fenomenali. Già il fatto di avere in mente di creare un sistema di interoperabilità tra

blockchain diverse è estremamente rivoluzionario e il giorno in cui ciò sarà possibile non sembra essere nemmeno molto lontano, poiché gli esperti di Onchain (azienda che lavora in stretta collaborazione con il team di sviluppo di Neo e che crea soluzioni personalizzate per multinazionali e startup basate sulla blockchain) sono già a lavoro da parecchi mesi.

Per quanto riguarda il numero di Neo in circolazione, al momento della sua creazione ne sono stati immessi 100 milioni e non sarà possibile coniarne degli altri o effettuare attività di mining. Altra preziosa opportunità di investimento è rappresentata dal GAS della rete Neo. D'altronde detenere delle considerevoli quantità di GAS, che rappresenta ciò che fa muovere e

funzionare l'intera rete, può essere economicamente vantaggioso in quanto man mano che la produzione andrà esaurendosi è pronosticabile un considerevole aumento del suo valore. Questo può avvenire perché rappresenta un bene indispensabile per il funzionamento della rete Neo e chiunque voglia operarci al suo interno deve necessariamente possederne una determinata quantità in relazione alle

operazioni che intende fare. Ad oggi per ottenerlo in quantità più o meno discrete basta possedere dei Neo sul proprio wallet, ma immaginiamo tra un paio di anni quando sarà minore la quantità dispensata ai vari possessori di Neo: sicuramente ci saranno operatori costretti ad acquistarlo da terzi a prezzi sicuramente più alti rispetto ad oggi, in quanto

rappresenterà un bene più prezioso, se vorranno avere la possibilità di far eseguire degli smart-contract o di compiere altre operazioni. Il tutto sarà, ovviamente, subordinato al modo in cui Neo saprà crescere e svilupparsi. Sicuramente, ad oggi, la strada che sta percorrendo è quella giusta.

Acquistare e possedere Neo o GAS è del tutto semplice in quanto sono resi disponibili da moltissimi exchange

presenti in rete. Bisogna prestare, però, attenzione al fatto che molti tra gli exchange non danno la possibilità di riscattare il GAS corrispondente ai Neo che si posseggono. Se si vuole essere sicuri di conservare al riparo da facili attacchi i propri Neo e di ricevere puntualmente il GAS spettante basta scaricare il wallet-software *NEO-GUI,* che funzionerà anche da

nodo della rete.

10. E’ STELLAR IL DEGNO RIVALE DI RIPPLE

Se il progetto di Ripple, che ci permette di scambiare valute da una

parte all'altra del mondo in modo rapido e quasi a costo zero, ci sembra del tutto eccezionale, quello che propone Stellar è un sistema di pagamento a dir poco geniale.
L'obbiettivo perseguito sia da Ripple che da Stellar è quello di rendere più semplici e veloci gli scambi transfrontalieri e di favorire gli scambi multi-valuta.

Tutti gli utenti possono utilizzare i sistemi di pagamento offerti dalla rete di Stellar e tutti possono contribuire alla sua diffusione diventando dei nodi della rete stessa.

Il protocollo che regola la creazione dei blocchi e l'approvazione delle varie transazioni è il seguente: *Federated Byzantine agreement* (FBA). Si tratta di un algoritmo molto

simile a quello già visto per la criptovaluta NEO. La sua peculiarità è costituita dal fatto che tutti i nodi della rete possono creare ed approvare blocchi di transazioni e tramite un sistema di votazione sono loro a scegliere il nodo delegato a svolgere questa funzione. Le transazioni che avvengono sulla rete Stellar vengono confermate in pochissimi secondi (in media dai 2 ai 5). Questa estrema

velocità è dovuta al fatto che all'approvazione di una transazione non partecipano tutti i nodi ma soltanto una parte di essi. Altra importante considerazione che vi è da fare è che ogni nodo della rete deve possedere una riserva di 20 Lumen e ciò è molto importante perché generalmente garantisce la presenza di nodi "affidabili". L'aspetto fondamentale di

questa crypto è la possibilità di effettuare delle transazioni con delle commissioni praticamente nulle: la fee che viene applicata ad ogni singola transazione è di 0,00001 XLM. Considerare questa crypto alla pari di Ripple è corretto ma non bisogna dimenticare che rappresenta anche una valida concorrente di altre criptovalute più importanti come ad esempio Ethereum. Infatti sulla rete Stellar è

possibile far eseguire anche degli smart-contract o creare determinate tipologie di app.

Non bisogna dimenticare, tra le altre cose, che Stellar è un progetto creato da un ente no profit – la Stellar Development Foundation – che si prefigge di sconfiggere la povertà nei Paesi in via di sviluppo. Infatti, una percentuale (il 25%) di tutte le fee

raccolte dalle varie transazioni è destinata appunto ad essere devoluta in beneficenza.

L'ente creatore di Stellar ha stabilito che la massima quantità producibile di XML è fissata a 100 miliardi.

Questo interessante progetto è stato accolto da tantissime aziende nel mondo. Infatti Stellar può vantare la collaborazione con importanti marchi internazionali come IBM, Stripe e

Swipe.

Il processo di sviluppo di questa crypto è molto interessante e può vantare una capitalizzazione di mercato che supera il 2 miliardi di Euro.

E’ molto difficile stabilire fino a che punto riuscirà arrivare questa interessantissima criptovaluta, anche perché la concorrenza sul mercato è veramente molto elevata. Di certo le

collaborazioni con importanti aziende a livello mondiale hanno contribuito ad aumentare il suo appeal, ma ciò per ora non basta.

11. CENNI SU EOS E TRON

Due criptovalute ancora in piena fase di sviluppo sono EOS e TRON.

Negli ultimi mesi del 2018 entrambe le

criptovalute facevano registrare i più alti volumi di scambi e raggiungevano i primi posti nel ranking per capitalizzazione di mercato.

Entrambi i progetti sono molto interessanti. In particolare, EOS rappresenta una sorta di integrazione più articolata di Ethereum mentre Tron è una piattaforma di condivisione di contenuti di intrattenimento (file,

media, musica, videogiochi, ecc.).

Le criptovalute concorrenti di Ethereum sono parecchie, eppure EOS sembra aver battuto tutta la concorrenza, raggiungendo in poco tempo il secondo posto nel ranking delle cripto per capitalizzazione di mercato (scavalcando anche Ethereum). Il motivo per il quale questa criptovaluta ha attirato l'attenzione di tantissimi investitori è

molto semplice: rappresenta una tecnologia che permette di sviluppare smart-contract ed app in modo del tutto innovativo. Essa funziona appunto come se fosse un vero e proprio sistema operativo tramite il quale è possibile sviluppare far funzionare e distribuire svariate applicazioni. Tron invece può essere considerata come una piattaforma ideata per la

condivisione di contenuti di intrattenimento come videogames, media, musica, ecc. Questa crypto è stata concepita per favorire lo sviluppo e il lancio di applicazioni senza passare da enti intermediari. Ad esempio, i creatori di applicazioni per smartphone per distribuire le proprie idee sono costretti ad utilizzare servizi intermediari come Google Play o Apple Store incorrendo tra l'altro nel

pagamento di svariate commissioni. Grazie a Tron ciò non avverrà più e ognuno sarà libero di distribuire sulla sua blockchain la propria creazione e di essere retribuito tramite il token nativo della sua piattaforma. In più sarà anche possibile lanciare delle ICO e renderle quindi disponibili in modo semplice sul mercato.

Per ciò che riguarda queste

criptovalute è inutile fare dei discorsi molto tecnici in quanto si tratta ancora di progetti in via di perfezionamento. Quello che è sicuro è che il loro potenziale di crescita è enorme ed ancora sul mercato la concorrenza è quasi nulla. Si tratta di due progetti che portano un vento di novità nel campo delle criptovalute e che non rappresentano dei “copia e incolla” di altre crypto.

Sono tra l’altro delle criptovalute molto funzionali alle esigenze della società moderna e non per niente la loro capitalizzazione aumenta di giorno in giorno.

2. RIPPLE: SI TRATTA DI UNA CRIPTOVALUTA?

Vista l'enorme crescita che negli ultimi anni ha interessato Ripple), si è acceso un animato dibattito intorno ad un argomento delicato: può essere considerata o meno una criptovaluta? Anzitutto bisogna dire che i fondatori della moneta hanno costituito nel 2012 un'omonima società che ha il compito di gestire il protocollo di essa. Il dibattito nasce proprio a partire dal fatto che il

funzionamento di Ripple (noto con il simbolo XRP) sia gestito direttamente da un ente centrale. Pertanto può entrare nel novero delle criptovalute una moneta digitale che ha come riferimento un entità privata? La risposta è no, almeno a mio parere. Se il sistema che sta alla base di Ripple è gestito direttamente da un entità centrale individuabile, è scontato sostenere che si tratta di un qualcosa di diverso rispetto ad una

criptovaluta. Come quest'ultima, anche Ripple utilizza la crittografia per validare le transazioni e si basa su una blockchain pubblica decentralizzata. L'unico elemento difforme rispetto alle classiche criptovalute è rappresentato dal fatto che per poter entrare a far parte della rete di Ripple è necessario ottenere il nulla osta della società che la gestisce. Ciò non esclude il fatto che

chiunque può possedere XRP e può scambiarli liberamente con altri utenti, ma non tutti possono utilizzare i servizi avanzati e diventare nodi della rete. Quindi il sistema Ripple è “chiuso” e la sua gestione è affidata ad un ente ben preciso che in qualsiasi momento può sentirsi libero di modificarne il funzionamento e l’emissione (a sue spese). Altro elemento da non trascurare è che la società emittente possiede il

55% dei 100miliardi di token immessi sul mercato (ciò consentirebbe di manipolare in modo non indifferente il mercato).

Il suo funzionamento è senza dubbio molto efficiente, soprattutto in tema di trasferimento di fondi da una parte all'altra del mondo: infatti tramite la rete Ripple è possibile scambiare quasi a costo zero e in pochi secondi anche

grandi capitali di denaro. Proprio per questo essa si propone in primo luogo di sostituire il sistema tradizionale di pagamento tramite SWIFT, che è quello attualmente utilizzato per gli scambi di valute tra istituti di credito, in quanto risulta essere lento e costoso, soprattutto in tema di scambi di denaro a livello internazionale. Per i vari operatori della rete Ripple scambiarsi denaro è piuttosto semplice anche se mittente e

destinatario di una transazione posseggono valute differenti e il tutto avviene in maniera pressoché istantanea. Lo schema di operatività del sistema di pagamento adottato da Ripple prevede che:

- Il mittente di una transazione versa il suo denaro liquido ad un ente accreditato della rete;
- L'ente converte in XRP il denaro

versato al tasso corrente e invia la quantità di XRP ad un altro ente accreditato che si trova in un'altra parte del mondo;

- L’ente che riceve questa quantità di XRP la incassa e provvede a recapitare il corrispondente valore di denaro liquido (in valuta avente corso legale in quel luogo) al destinatario del pagamento.

Sostanzialmente questo sistema non

richiede grandi movimentazioni di valuta liquida e soprattutto non prevede nessun iter burocratico complesso da dover seguire come avviene nel caso di un bonifico internazionale. Tra l'altro il trasferimento è del tutto istantaneo e servono al massimo 5-6 secondi per vedere il denaro accreditato direttamente sul conto del cliente di un istituto di credito.

All’interno della rete Ripple è tra l’altro possibile scambiarsi anche valute diverse da XRP o anche dei beni fisici sotto forma di crediti IOU - *I owe you*, che tradotto significa “ti pagherò” -. Questi crediti posseggono una valutazione in XRP, anche se comunque possono essere scambiati tra di loro senza ricorrere al pagamento nella valuta nativa della rete. I cosiddetti IOU

sono generati dai *gateway*, i quali non sono altro che probabili attività commerciali, istituti di credito o altre entità che offrono dei servizi ai propri clienti. Potrebbero esistere degli IOU Bitcoin, IOU in oro, IOU dollari, ecc.. Ma in realtà quale logica segue questo sistema di emissione e di scambio di crediti IOU? Lo schema di funzionamento è il seguente:

1. Un cliente, perché ha necessità di

effettuare un pagamento ad un altro soggetto, si affida ad un gateway che rilascia, ad esempio, crediti IOU Euro e paga una data quantità di Euro a quest'ultimo al dì fuori della rete Ripple, in cambio dell'emissione all'interno di essa della corrispondente quantità di IOU Euro.

2. Perché il cliente possa effettuare una transazione con un altro soggetto

operante all'interno della rete Ripple è necessario abbia un rapporto di fiducia con il soggetto che riceverà il pagamento, poiché quest'ultimo deve essere sicuro che nel momento in cui andrà a reclamare la quantità di Euro (liquidi) corrispondente agli IOU che gli verranno ipoteticamente inviati, il gateway che li ha emessi abbia la riserva necessaria di Euro per poter liquidare il debito. Proprio a tale

scopo Ripple prevede la costituzione di “linee di fiducia” tra utenti che hanno fiducia reciproca.

3. Nel momento in cui il soggetto riceve gli IOU Euro tramite una transazione validata e registrata all’interno della blockchain di Ripple, può decidere di rivolgersi al gateway emittente per ricevere liquidità in Euro. Pertanto gli IOU

Euro potranno essere convertiti direttamente in valuta fiat, in cambio di una commissione pagata in Ripple.

L'efficienza della rete Ripple non si limita soltanto a questo ma permette anche di effettuare delle conversioni di valuta (ad esempio da Euro a Dollaro) o di pagare un utente in Dollari pur possedendo solo degli Euro. Il tutto avviene molto rapidamente nonostante la

complessità dei passaggi da eseguire, seppur si tratta ancora di sistemi in via di sviluppo e di definizione.

Qualsiasi tipo di illegalità commessa dai gateway o comunque dai vari operatori della rete è suscettibile di denuncia di fronte alle autorità giudiziarie, oltre ad essere punita dal regolamento interno della rete.

Nel complesso, il sistema portato avanti

da Ripple è molto funzionale agli interessi degli istituti bancari che hanno modo di ridurre tempi e costi legati agli scambi di denaro, soprattutto a livello internazionale. Bisogna precisare che il modello appena descritto si presta ancora a miglioramenti in quanto sono ancora in via di sviluppo dei sistemi di conversione di valute pressoché istantanei e che rilevano automaticamente le condizioni più

vantaggiose per il cliente che deve inviare denaro in una valuta differente rispetto a quella che possiede, o più semplicemente per quell'operatore che intende semplicemente convertire, ad esempio, Dollari in Yen.

Ad oggi, Ripple, sembra essere riuscito ad ovviare in modo egregio a parecchi inconvenienti legati all'ambiente bancario, tanto che sempre più aziende

si affidano ad esso per fornire un servizio efficiente ai propri utenti.

Per ciò che attiene all'aspetto meramente speculativo bisogna anzitutto pensare al numero elevatissimo di XRP che sono stati immessi in circolazione, che indubbiamente ci induce a sostenere che siano necessari miliardi e miliardi di investimenti in questa valuta per assistere ad un incremento della sua valutazione sul mercato. Non chiara è

anche la posizione di chi sta dietro e gestisce questo progetto che, pur avendo dichiarato di non voler intervenire in futuro per aumentare il numero di XRP in circolazione, potrebbe comunque decidere di intraprendere qualsiasi tipo di azione per evitare ad esempio sconsiderati apprezzamenti o deprezzamenti. D'altronde una moneta che viene utilizzata nei termini appena

descritti ha bisogno di possedere un valore stabile nel tempo e di non essere fin troppo volatile. Senza dubbio, allo stato attuale, se si scongiurassero interventi mirati ad intervenire sul valore di mercato, è pensabile che il consenso che sta ottenendo tra aziende ed istituti di credito, possa portare nel lungo periodo un considerevole apprezzamento. E', a mio parere, inutile detenere direttamente delle somme di

XRP per i semplici utenti, sia per il fatto che è necessario un deposito minimo di 20 XRP (non utilizzabili) per aprire un wallet online, sia perché è impossibile utilizzare i servizi avanzati offerti dalla rete Ripple se non si è un ente accreditato dalla società che ne sta a capo. Piuttosto sarebbe più sensato operare tramite CFD e aprire una posizione long a lunga scadenza, se si

crede nel progetto. I presupposti per una ascesa vincente ci sono tutti ma bisogna rimanere vigili sul modo in cui potrebbe essere eventualmente manipolato il suo valore.

13. ASPETTI LEGALI E FISCALI DELLE CRIPTOVALUTE IN ITALIA

Attualmente la legislazione italiana non possiede alcuna legge che definisce in maniera chiara ed esaustiva le criptovalute e tutti i profili che ruotano attorno a questo argomento.

Attualmente esistono soltanto due riferimenti normativi ai quali attenersi: la IV Direttiva Europea Antiriciclaggio

(Luglio 2017) e la Risoluzione dell'Agenzia delle Entrate n°72 del 02/09/2016.

- IV DIRETTIVA EUROPEA ANTIRICICLAGGIO

La Direttiva Europea in questione si preoccupa anzitutto di definire le criptovalute e i prestatori di servizi del settore. In particolare dal testo emerge l'assimilazione degli exchange ai tradizionali cambiavalute e li definisce

come degli operatori non finanziari (differenti da banche, società di investimenti o consulenti finanziari che sono, invece, degli operatori finanziari). Questa direttiva ha imposto anche l'obbligo a tutti gli exchange di registrare l'identità degli utenti tramite l'esibizione di documenti validi, per evitare l'agevolazione di operazioni di riciclaggio del denaro.

E’ chiaro però che le Direttive Europee debbano essere attuate dai singoli stati membri tramite una legge. Ad oggi ci risulta che è stata soltanto presentata una bozza di legge nel 2018 e che fin’ora non esiste un serio dibattito in merito.

- RISOLUZIONE N°72 DELL’AGENZIA DELLE ENTRATE

Dal punto di vista fiscale questa

Risoluzione dell'Agenzia delle Entrate risulta del tutto illuminante per ciò che riguarda l'aspetto della tassazione sulle criptovalute.

Partiamo dal presupposto che una Risoluzione dell'Agenzie delle entrate non è una legge ma soltanto un atto amministrativo interno che serve ad indirizzare e a disciplinare in modo uniforme l'attività degli organi inferiori.

In questo caso un'azienda ha interrogato

l'Agenzia delle Entrate in merito alla possibilità di ricevere pagamenti tramite criptovalute e alla tassazione a cui esse sono soggette. L'Agenzia delle Entrate ha risposto considerando anzitutto le criptovalute alla stregua delle valute estere. Pertanto un'azienda può utilizzare Bitcoin e altre criptovalute come se fossero degli Euro, dei Dollari, ecc. senza dover far fronte a particolari

iter burocratici e senza che esse siano soggetti a speciali regimi di tassazione. L'impresa sarebbe soggetta a pagare ulteriori tasse soltanto se ricavasse una plusvalenza dalla vendita di criptovalute. Quindi fin quando le criptovalute vengono conservate sull'apposito wallet l'azienda non sarebbe soggetta a pagare tasse extra. Nel momento in cui converte le criptovalute in un'altra valuta e genera

una plusvalenza allora quest'ultima è soggetta a tassazione.

Sulla base dell'assimilazione delle crypto alle valute estere, il discorso cambia per i privati cittadini.

Generalmente un privato cittadino non è soggetto a pagare alcuna imposta nel momento in cui realizza una plusvalenza derivante dal cambio di valuta. Però nel caso in cui nel corso di un anno un

soggetto privato per almeno sette giorni consecutivi detiene Bitcoin che hanno un valore in Euro pari o superiore 51.000, allora l'attività viene considerata speculativa e soggetta a tassazione. Bisogna anche citare il caso in cui si acquistano e si detengono criptovalute su wallet la cui sede risulta all'estero (come ad esempio nel caso di Coinbase). Nella fattispecie in questione, probabilmente, l'ammontare

detenuto andrebbe indicato nel quadro RW della dichiarazione dei redditi, che è riservato al monitoraggio dei capitali detenuti all'estero.

Quelle appena fatte sono delle considerazioni che è possibile dedurre da ciò che l'Agenzia delle Entrate ha dettato nella sua Risoluzione. Ma comunque se sussistono dei casi particolarmente complessi è sempre

meglio rivolgersi a degli esperti del settore per poter determinare con più chiarezza se si è soggetti a particolari regimi di tassazione.

Come è possibile notare, il nostro sistema legislativo è povero di norme che regolano il settore delle criptovalute e anzi quel poco che si può dedurre è del tutto inadeguato e alimenta solo incertezze. Pertanto, attualmente, è difficile soprattutto per le imprese

aprire totalmente le porte a questo mondo in quanto è molto facile, vista l'incertezza, incorrere in sanzioni o cadere in preda a problemi di difficile soluzione.

RINGRAZIAMENTI

Sarebbero tante le persone da ringraziare ma ci tenevo particolarmente a citare quegli amici che giorno dopo

giorno non hanno mai smesso di supportarmi e sopportarmi in tutte le mie “avventure”. In particolare, il mio “grazie” va a Giuseppe C., Fiorenzo S., Anna L. e Gioela C. e Francesco G..
Il mio ringraziamento è dovuto al fatto che la loro presenza nella mia vita rappresenta una fonte di cultura, valori e sentimenti positivi. Un autore trova spesso la sua ispirazione, oltre che nelle

conoscenze tecniche della materia che tratta, anche nelle esperienze di vita che si trova ad affrontare: e le mie esperienze possono senza dubbio considerarsi positive alla luce della costante e preziosa presenza di queste persone. Sembra banale ma sentirsi incoraggiati a perseguire determinati obbiettivi, sentirsi ascoltati, avere qualcuno con cui confrontarsi a 360° significa ottenere una spinta maggiore

verso il raggiungimento di un traguardo prestabilito.

Pertanto grazie a tutti voi che avete reso più semplice e più ricco il mio cammino.

CONTATTI AUTORE

- Sito web: https://cryptouniverse.it
- Facebook: Giuseppe Ozzimo
- E-mail:

giuseppe.ozzimo1108@gmail.com