

Incontro a cura Gruppo di Lavoro

VALUTE VIRTUALI, TECNOLOGIA BLOCKCHAIN E SISTEMI INNOVATIVI DI PAGAMENTO

- *Glossario e presentazione dei principali termini utilizzati nel mondo delle criptovalute.*
- *Analisi della recente risposta ad interpello dell'Agenzia delle Entrate in tema di tassazione e monitoraggio fiscale.*
- *Sintesi della normativa adottata in altri Paesi.*
- *Programmazione dell'attività del Gruppo: raccolta di suggerimenti e spunti.*

Relatore

Dott. Luca Piovano

Referenti e coordinatori

Dott. Stefano Branca

Dott. Federico Moine

GLOSSARIO

Per introdurre al mondo delle valute virtuali, è necessario conoscere almeno i seguenti termini di uso corrente:

Alternative currencies/Alt Coins

Esistono centinaia di altre monete alternativa al Bitcoin (e in continuo aumento), si usa questo termine per riferirsi a questo folto gruppo alternativo.

Arbitraggio

L'arbitraggio si riferisce alla pratica di acquistare bitcoin o qualsiasi altra criptovaluta, rivendendola immediatamente su un altro exchange per trarre vantaggio dalla differenza di prezzo

ASIC mining

L'Asic è un sistema di elaborazione per il mining che ha il vantaggio di impiegare meno energia rispetto a CPU o GPU e ottenere prestazioni nettamente superiori.

Il termine "ASIC" è spesso usato genericamente per riferirsi all'intero sistema, e non solo al chip da cui prende il nome.
(Application Specific Integrated Circuit)

Ask price

Nel trading, l'Ask (domanda) si riferisce al prezzo al quale è possibile acquistare un bene da un venditore. Può essere definito come la domanda o il prezzo richiesto. È l'opposto di bid (offerta)

AT

Acronimo di Analisi Tecnica

ATH

Un all-time high è il prezzo più alto che ogni crypto o alt coin abbia mai raggiunto dal momento in cui è stata quotata su un exchange

GLOSSARIO

Balance

Ammontare del totale delle criptovalute presenti sul proprio account

Bid price

Cifra offerta da chi acquista criptomonete

Blocco

Un blocco è una parte della blockchain, contiene le transazioni in attesa. E' su ogni singolo blocco che compone la Blockchain (dall'inglese "catena di blocchi") che vengono impresse e registrate le transazioni tra due o più utenti. Questi blocchi sono collegati tra loro in una successione temporale e soltanto quando un blocco viene chiuso in seguito al calcolo di un complesso algoritmo, attraverso il mining, la transazione può essere considerata chiusa e controfirmata.

Blockchain

La blockchain, o catena di blocchi, è il libro contabile in cui sono registrate tutte le transazioni fatte -nel caso del Bitcoin- dal 2009 ad oggi. Si tratta di un database distribuito, ovvero non presente su un solo server o computer, ma condiviso da tutti i pc che supportano il progetto (nodi)

Chiave Privata

Una chiave privata è una parte di dati segreti che provano che sei tu ad utilizzare bitcoin o altre monete da un determinato portafoglio attraverso una firma crittografata. La tua chiave privata (o chiavi private) è conservata nel tuo computer se utilizzi un portafoglio software; invece è conservata nei server se utilizzi un portafoglio web. La chiave privata non deve essere rivelata ad altri in quanto permette di utilizzare i fondi dal tuo portafoglio (wallet)

Conferma

La conferma indica che una transazione è stata processata dalla rete ed è altamente improbabile che sia respinta. La transazioni ricevono una conferma quando sono incluse in un blocco e per ogni blocco successivo. Anche una singola conferma può essere considerata sicura per le transazioni di basso valore, è consigliabile attendere più conferme. Ogni conferma esponenzialmente diminuisce il rischio di una transazione respinta.

GLOSSARIO

dApps

Le applicazioni decentralizzate (dApps) sono strumenti creati impiegando la tecnologia blockchain di Ethereum ed in particolare sfruttando gli smart contracts, elemento caratterizzante il network Ethereum.

La protezione assoluta della privacy e l'indipendenza da un unico server centrale rendono le applicazioni decentralizzate molto più efficienti e sicure rispetto agli applicativi che siamo abituati ad utilizzare.

DAO (Decentralized Autonomous Organization)

E'una struttura in cui la proprietà, la gestione e il controllo sono automatizzati, in quanto basati su regole predeterminate con un intervento umano pressoché assente.

DEX Decentralized Exchange (Exchange Decentralizzato)

Un DEX è un mercato per criptovalute totalmente open source. Nessuno ha il controllo su un DEX, e compratori e venditori trattano reciprocamente su base uno a uno tramite applicazioni di trading peer-peer (P2P)

ERC20

Lo standard Ethereum token(ERC20) viene utilizzato per gli smart contract di Ethereum. ERC20 definisce un elenco comune di regole che un token Ethereum deve implementare, dando agli sviluppatori la possibilità di definire come i nuovi token funzioneranno all'interno dell'ecosistema Ethereum. Questo protocollo token è il più usato per quanto riguarda le ICO. ERC è l'acronimo di Ethereum Request for Comments.

Escrow

Una terza parte fidata che svolge la funzione di arbitro all'interno di una transazione.

Exchange

Mercato dove è possibile acquistare e vendere sia Bitcoin che le altre criptovalute, come un in mercato azionario. L'exchange è solito trattenere una parte degli scambi come fee (tassa di transazione)

Fee

E' il costo da sostenere per far si che avvenga la transazione

GLOSSARIO

Fiat

Valuta con corso legale (ci si riferisce tipicamente a valuta cartacea). USD, EURO, GBP, etc., sono valute fiat.

GAS price Ethereum

Ethereum Gas Price, ovvero il prezzo interno per far eseguire una transazione o un contratto sulla blockchain di Ethereum.

Il funzionamento dell'Ethereum Gas Price non è differente dall'uso dei Kw per misurare il consumo di elettricità.

Ethereum ha un limite di dimensione del blocco – quindi tu paghi per avere spazio premium nel blocco successivo, proprio come succede con i bitcoin.

Con Bitcoin i miner danno priorità alla transazione con le commissioni più alte. Lo stesso discorso vale per Ethereum, poiché i minatori sono liberi di scegliere di ignorare le operazioni il cui gas limite è troppo basso.

Più complessi sono i comandi che vuoi eseguire, più gas (ed Ether) dovrai pagare.

Hard fork

Modifica del protocollo della moneta. Divisione di una blockchain, con la formazione di un nuovo protocollo, di conseguenza una seconda blockchain, che non è retrocompatibile con le versioni precedenti.

Hash

Hash è un algoritmo che serve per fornire un riassunto di alcune informazioni per determinarne la correttezza in maniera univoca. L'elaborazione di un singolo blocco richiede milioni di operazioni di Hash.

Hash Rate

Per hash rate si intende l'unità di misura della potenza di elaborazione della rete Bitcoin. Per fini di sicurezza la rete Bitcoin deve eseguire delle operazioni matematiche intensive. Quando la rete raggiunge un hash rate di 10 Th/s, significa che può realizzare un trillione di calcoli al secondo.

Hashing

L'hashing è l'unità di misura della potenza del mining

GLOSSARIO

Indirizzo

Un indirizzo Bitcoin è equivalente ad un indirizzo fisico o ad una e-mail.

ICO

Abbreviazione per Initial Coin Offering. Analogamente a quanto accade durante una IPO (Initial Public Offer) per le società che si quotano in Borsa, la ICO è il momento in cui per la prima volta vengono offerte agli investitori unità di nuove criptovalute o crypto-tokens. Gli investitori normalmente possono acquistare i nuovi tokens utilizzando altre criptovalute (Bitcoin, Ethereum o altre) oppure possono conferire valute fiat.

Le ICO possono essere considerate una sorta di crowdfunding, infatti ormai da anni sono utilizzate dalle "cripto startup" per finanziare lo sviluppo e l'implementazione di nuovi progetti in ambito blockchain e relative applicazioni.

Per pubblicizzare la ICO e per far conoscere il progetto a quanti più investitori possibili, i promotori redigono il cosiddetto white paper, una sorta di documento di "trasparenza" in cui sono descritte una serie di informazioni di dettaglio, tra cui le finalità del progetto, i suoi utilizzi, l'ammontare di token che verranno allocati, l'obiettivo minimo di raccolta di fondi, le tempistiche della ICO e così via.

Al termine del periodo di durata (prefissato) della ICO, se sarà stato raggiunto l'obiettivo della raccolta, il token diverrà disponibile per lo scambio su uno o più exchange. Se il progetto sottostante avrà successo, verosimilmente si verificherà un aumento del valore di mercato del token, permettendo ai primi investitori (ovvero coloro che hanno partecipato all'ICO), di avere i maggiori rendimenti. Qualora invece il progetto non avesse i successi sperati (o peggio, se la ICO si rivelasse uno scam), gli investitori potrebbero perdere quanto conferito, ritrovandosi a possedere token inutili. E' anche possibile che l'ICO non raccolga sufficienti adesioni, in tal caso normalmente il white paper prevede la restituzione dei conferimenti ricevuti.

KYC

Know Your Customer, procedura di riconoscimento dei clienti obbligatoria per ICO.

Miner

Risorsa hardware o software che consente l'operazione di mining. L'hardware utilizzato può essere la CPU, la GPU o hardware dedicato. L'hardware si interfaccia con del software che consente di specificare dove effettuare l'operazione di mining e con quali parametri.

GLOSSARIO

Mining

Per mining si intende il processo che fa eseguire all'hardware del computer calcoli matematici al fine di confermare le transazioni ed aumentare la sicurezza della blockchain. Come ricompensa per il loro servizio, i miner (minatori) possono incassare delle commissioni sulle transazioni che confermano insieme ai nuovi bitcoin appena creati.

Nodi

Ogni singolo utente rappresenta un nodo di questo ecosistema ed è il controllore e il garante della correttezza della Blockchain. I nodi quindi si possono controllare a vicenda e tutto viene fatto alla luce del sole: ogni utente può analizzare le transazioni di chiunque altro.

Satoshi/bit

Si riferisce alla minima parte divisibile dei bitcoin, ovvero a 0,00000001 BTC. Il nome viene da Satoshi Nakamoto, pseudonimo dell'inventore di Bitcoin.

100.000.000 di Satoshi = 1 bitcoin (BTC)

100 Satoshi = 1 bit

1.000.000 di bit = 1 bitcoin

Scam/Scammer

Si riferisce a truffe e truffatori e questo genere di attività illecite.

Segwit Segregate Witness

È il processo mediante il quale il limite della dimensione del blocco su una blockchain viene aumentato rimuovendo i dati delle firme dalle transazioni. Quando alcune parti di una transazione vengono rimosse, questo libera spazio o capacità per aggiungere più transazioni alla catena.

Segregate Witness in breve, significa separare le firme delle transazioni.



GLOSSARIO

Smart contracts

Gli smart contracts sono “protocolli informatici che facilitano, verificano o fanno rispettare la negoziazione o l’esecuzione di un contratto”

Lo smart contract funziona con logiche “se A allora B” (A implica B), ciò significa che il protocollo verifica in automatico l’avverarsi delle condizioni di esecuzione del contratto e si auto-esegue se e solo se tutte le condizioni sono verificate, applicando in automatico le clausole concordate dalle parti. Questo automatismo permette di stipulare ed eseguire contratti in modo sicuro ed economico, in quanto non è necessaria la fiducia tra le parti contraenti, né l’intervento di terze parti neutrali (intermediari). E’ il protocollo che funge da intermediario indipendente, “decidendo” in modo intelligente (smart) se eseguire o no il contratto e applicando autonomamente le condizioni prestabilite. Un altro di elemento di sicurezza è l’impossibilità di annullare lo smart contract (esso è immutabile). Infine, gli smart contracts sono decentrati, cioè si trovano su una rete distribuita e quindi la loro esecuzione deve essere “validata” da molti nodi all’interno del network. Un tentativo di forzatura del contratto da parte di un nodo porterebbe gli altri nodi a invalidare il contratto.

Script

Metodo crittografico successivo ed alternativo a SHA256. In questa categoria troviamo quasi tutte le criptovalute secondarie più importanti come Litecoin e Dogecoin.

SHA256

Metodo crittografico alla base di Bitcoin e di alcune criptovalute secondarie conosciute come Namecoin e Devcoin.

Stop loss (Ordine)

Letteralmente blocco delle perdite, è un ordine effettuato su una posizione aperta che impone la chiusura della stessa ad un prezzo predefinito, che risulta meno favorevole rispetto al prezzo di mercato corrente. l’ordine di stop loss viene utilizzato per definire un limite massimo di perdite possibili per una data posizione aperta.

GLOSSARIO

Supply

Circulating supply: è la migliore approssimazione del numero di coins che circolano nel mercato e nelle mani del pubblico in generale.

Total supply: è la quantità totale di coins esistenti al momento (meno quelli che sono stati bruciati in modo verificabile)

Max Supply: è la migliore approssimazione della quantità massima di coins che esisterà mai nella vita della criptovaluta

Wallet/Portafoglio

portamonete virtuale per ricevere, custodire e spendere criptovalute e tokens. Contiene la chiave privata per apporre la firma digitale necessaria all'esecuzione di una transazione in uscita (pagamento) ed un indirizzo "di deposito" (assimilabile all'Iban bancario) per le transazioni in entrata (depositi e ricezione pagamenti) E' un file che potete tenere sul vostro computer, in un drive a parte come una pendrive usb, o in hardware specifico (Hardware Wallet). Può anche essere conservato in forma cartacea (Paper Wallet)

Take profit (Ordine Limite)

L'ordine limite è un ordine effettuato su una posizione aperta che impone la chiusura della stessa ad un prezzo predefinito, in modo da garantire al trader un profitto.

White paper è un documento in cui viene spiegato il funzionamento di un progetto nascente, sia dal punto di vista informatico che concettuale. I white paper sono reperibili sui siti ufficiali delle varie alt coins o criptovalute.

Withdrawal

Prelievo di una somma

LINK A VARI SITI DI INTERESSE

SITO che riepiloga i dati delle «Top 100 Cryptocurrencies by Market Capitalization»:

<https://coinmarketcap.com/>

SITI di exchange:

<https://www.therocktrading.com/>

<https://www.binance.com/>

<https://bittrex.com/>

<https://www.coinbase.com/>

SITO per calcolo rendiconto fiscale:

<https://cointracking.info/>

L'INTERPELLO ALL'AGENZIA DELLE ENTRATE DI GENNAIO 2018

Nell'interpello in oggetto si trovano alcune importanti risposte ai tanti quesiti aperti. Fra i punti trattati, si segnalano i seguenti.

*...si ritiene che, ai fini delle imposte sul reddito, delle persone fisiche che detengono bitcoin (o altre valute virtuali) al di fuori dell'attività d'impresa, alle operazioni di conversione di valuta virtuale si applicano i principi generali che regolano le operazioni aventi ad oggetto **valute tradizionali**.*

*Conseguentemente, le cessioni a pronti di valuta virtuale non danno origine a redditi imponibili mancando la finalità speculativa salvo generare un **reddito diverso** qualora la valuta ceduta derivi da prelievi da portafogli elettronici (wallet), per i quali la **giacenza media superi un controvalore di euro 51.645,69 per almeno sette giorni lavorativi continui nel periodo d'imposta**, ai sensi dell'articolo 67, comma 1, lettera c-ter), del testo unico delle imposte sui redditi approvato con d.P.R. 22 dicembre 1986, n. 917 (TUIR), e del comma 1-ter del medesimo articolo. Per cessione a pronti si intende una transazione in cui si ha lo scambio immediato di una valuta contro una valuta differente.*

*Il valore in euro della giacenza media in valuta virtuale va calcolato secondo il cambio di riferimento all'inizio del periodo di imposta, e cioè al 1 gennaio dell'anno in cui si verifica il presupposto di tassazione (cfr. circolare 24 giugno 1998, n. 165). Resta inteso che, qualora non risulti integrata la condizione precedentemente individuata, **non si rendono deducibili neppure le minusvalenze eventualmente realizzate**.*

L'INTERPELLO ALL'AGENZIA DELLE ENTRATE DI GENNAIO 2018

Tenuto conto che manca un prezzo ufficiale giornaliero cui fare riferimento per il rapporto di cambio tra la valuta virtuale e l'euro all'inizio del periodo di imposta, il contribuente può utilizzare il **rapporto di cambio al 1 gennaio rilevato sul sito dove ha acquistato la valuta virtuale o, in mancanza, quello rilevato sul sito dove effettua la maggior parte delle operazioni.**

Detta giacenza media va **verificata rispetto all'insieme dei wallet detenuti** dal contribuente indipendentemente dalla tipologia dei wallet (paper, hardware, desktop, mobile, web).

Ai fini della eventuale tassazione del reddito diverso occorre, dunque, verificare se la conversione di bitcoin con altra valuta virtuale (oppure da valute virtuali in euro) avviene per effetto di una cessione a termine oppure se la giacenza media del wallet abbia superato il controvalore in euro di 51.645,69 per almeno sette giorni lavorativi continui nel periodo d'imposta.

Si fa presente, inoltre, che ai fini della determinazione di un'eventuale plusvalenza derivante dal prelievo dal wallet, che abbia superato la predetta giacenza media, si deve utilizzare il costo di acquisto e che agli effetti della determinazione delle plusvalenze/minusvalenze **si considerano cedute per prime le valute acquisite in data più recente** (cfr. articolo 67, comma 1-bis, del TUIR).

...

L'INTERPELLO ALL'AGENZIA DELLE ENTRATE DI GENNAIO 2018

...

Per quanto riguarda gli **obblighi di monitoraggio fiscale**, si fa presente che il citato decreto legislativo n. 90 del 2017, oltre a definire la valuta virtuale, ha tra l'altro modificato alcune disposizioni relative al monitoraggio fiscale di cui al decreto legge 28 giugno 1990, n. 167 (convertito, con modificazioni, dalla legge 4 agosto 1990, n. 227 e successive modificazioni).

In particolare, sono stati estesi gli obblighi di monitoraggio fiscale, ordinariamente previsti per gli intermediari bancari e finanziari, altresì ai soggetti (c.d. "operatori non finanziari") che intervengono, anche attraverso movimentazione di "conti", nei trasferimenti da o verso l'estero di mezzi di pagamento effettuate anche in valuta virtuale, di importo pari o superiore a 15.000 euro.

...

Poiché alle valute virtuali si rendono applicabili i principi generali che regolano le operazioni aventi ad oggetto valute tradizionali nonché le disposizioni in materia di antiriciclaggio, **si ritiene che anche le valute virtuali devono essere oggetto di comunicazione attraverso il citato quadro RW, indicando alla colonna 3 ("codice individuazione bene") il codice 14 – "Altre attività estere di natura finanziaria"**.

Il controvalore in euro della valuta virtuale detenuta al 31 dicembre del periodo di riferimento deve essere determinato **al cambio indicato a tale data sul sito dove il contribuente ha acquistato la valuta virtuale**. Negli anni successivi, il contribuente dovrà indicare il controvalore detenuto alla fine di ciascun anno o alla data di vendita nel caso di valuta virtuale vendute in corso d'anno.



L'INTERPELLO ALL'AGENZIA DELLE ENTRATE DI GENNAIO 2018

Da ultimo, si precisa che **le valute virtuali non sono soggette all'imposta sul valore dei prodotti finanziari**, dei conti correnti e dei libretti di risparmio detenuti all'estero dalle persone fisiche residenti nel territorio dello Stato (c.d. IVAFE, istituita dall'articolo 19 del decreto legge 6 dicembre 2011, n. 201, convertito, con modificazioni, dalla legge 22 dicembre 2011, n. 214, e successive modificazioni), in quanto tale imposta si applica ai depositi e conti correnti esclusivamente di natura "bancaria" (cfr. circolare 2 luglio 2012, n. 28/E).

COSA SUCCEDDE NEL MONDO

La regolamentazione del mondo delle criptovalute è molto diversa da Paese a Paese. Nei due documenti scaricabili ai link sottoriportati è sintetizzata la disciplina fiscale applicabile alle criptovalute e quella applicabile alle ICO nei diversi Paesi.

[SCARICA IL DOCUMENTO «Crypto Taxes regulation worldwide»](#)

[SCARICA IL DOCUMENTO «ICO Regulations Worldwide 2018»](#)

L'Autorità Finanziaria Svizzera (FINMA) ha recentemente emanato le linee guida applicabili alle ICO. Sono reperibili al link sottostante:

<https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/>

L'IRS, l'autorità fiscale degli Stati Uniti d'America, ha pubblicato le linee guida per la tassazione dei proventi derivanti da criptovalute. Le linee guida sono scaricabili al link sottoriportato:

<https://www.irs.gov/newsroom/irs-reminds-taxpayers-to-report-virtual-currency-transactions>