The Rock Trading

“Cripto-asset”, 28/10/2022: «L’investimento diretto tramite un Exchange»

https://www.therocktrading.com

CHI SIAMO

ITALIANA
STORICA
AFFIDABILE

3 UFFICI OPERATIVI

70.000+ CLIENTI

10+ ANNI DI ESPERIENZA

TIMELINE

2011 - Prima transazione *bitcoin*: siamo l'*exchange* più longevo in tutta Europa

2013 - Malta

2017 - Società di diritto Italiano

2019 - *Restyling* grafico e di funzionalità

2020 - Campagna di *crowdfunding*

2021 - Integrazione di *lightning network* e piani di accumulo ("PAC"), app per iOS2022

2022 - *Restyling* del sito *web* e *rebranding*

TRT

Bloomberg - PRICE PROVIDER

The Rock Trading SOGGETTO OBBLIGATO

Siamo registrati presso l’OAM e adottiamo le procedure antiriciclaggio previste dalla V Direttiva (AMLD5)

TRT

CHI SIAMO

Il gateway che collega il mondo della finanza tradizionale con quello dei crypto-asset

www.therocktrading.com

THEROCK TRADING

BLOCKCHAIN

Una *blockchain* è un insieme di tecniche, protocolli e strumenti che permettono di avere un archivio digitale non modificabile di transazioni, distribuito tra i nodi di una rete e da essi validato periodicamente.

In termini ancora più semplici:

Una *blockchain* è una sorta di *database* crittografato distribuito. Ogni utente ne ha una copia sul proprio computer / server sempre sincronizzata con le altre. La copia ufficiale attuale è sempre concordata con gli altri utenti. Si possono aggiungere dati non cancellarli.

TRT

BLOCKCHAIN

Esistono due tipologie principali di *blockchain*:

- Pubbliche (*permissionless*), a cui tutti possono accedere. I *bitcoin* e la maggioranza delle altre crittovalute sono implementate su *blockchain* pubbliche.

- Private (*permissioned),* in cui per accedere occorre avere credenziali di accesso. Sono soprattutto *blockchain* create per le aziende, i *business network* o per scopi specifici (es. tracciare l'origine di un prodotto/ provenienza, scambi di un bene (*asset*) digitale o meno (diamanti, opere d'arte, brani musicali ecc.). Molto spesso le *blockchain* private sono solo dei semplici *database* distributi che vengono così rinominate per meri motivi commerciali (ovvero, di puro *marketing*).

TRT

BLOCKCHAIN: IL MECCANISMO DEL CONSENSO

Esistono due tipologie principali di blockchain:

È il meccanismo (regole e procedure) con cui i nodi di una rete *blockchain* validano le transazioni e si accordano sullo «stato del mondo», cioè su quali siano al momento i dati corretti (chi possiede cosa).

Esistono diversi meccanismi, sia per le *blockchain* pubbliche che per quelle private.

TRT

BLOCKCHAIN: CARATTERISTICHE *BLOCKCHAIN* PUBBLICHE

Esistono due tipologie principali di

- ❑ Immutabilità (non vi sono cancellazioni)
- ❑ Pseudoanonimia (gli utenti non sono direttamente identificabili)
- ❑ **Trasparenza (tracciamento delle transazioni)**
- ❑ Decentralizzazione (non esiste un «centro di controllo»)
- ❑ Sicurezza (ogni utente (nodo) possiede copia dell'intera blockchain)
- ❑ Disintermediazione (le transazioni sono validate dalla rete di nodi, non c'è bisogno di terze parti (banche, autorità ecc.)

TRT

BITCOIN: COME FUNZIONA LA SUA *BLOCKCHAIN*?

Esistono due tipologie principali di blockchain:

Ad esempio
Io Andrea ho il controllo di 10 *bitcoin*.
Voglio trasferire 2 *bitcoin* a Giovanni.
Utilizzando un *wallet* di criptovalute, a cui sono associate le mie chiavi crittografiche con cui controllo i miei *bitcoin,* inserisco l'indirizzo pubblico di Giovanni (che lui mi ha precedentemente fornito).
Indico il numero 2 (ovvero il numero di *bitcoin* che voglio trasferire).
Firmo la transazione con le mie chiavi private.

Data la grande trasparenza della *blockchain* pubblica, in qualunque momento, chiunque può controllare su un *blockhain explorer* lo stato della transazione:

https://www.blockchain.com/explorer

TRT

BITCOIN: COME FUNZIONA LA SUA *BLOCKCHAIN*?

Esistono due tipologie principali di
ckchain:

Periodicamente (ogni 10 minuti circa) un certo numero di transazioni in sospeso viene raccolta in un blocco. I blocchi possono essere considerati le «pagine» di un libro mastro (la *blockchain*).

Le transazioni sono controllate per verificare che:

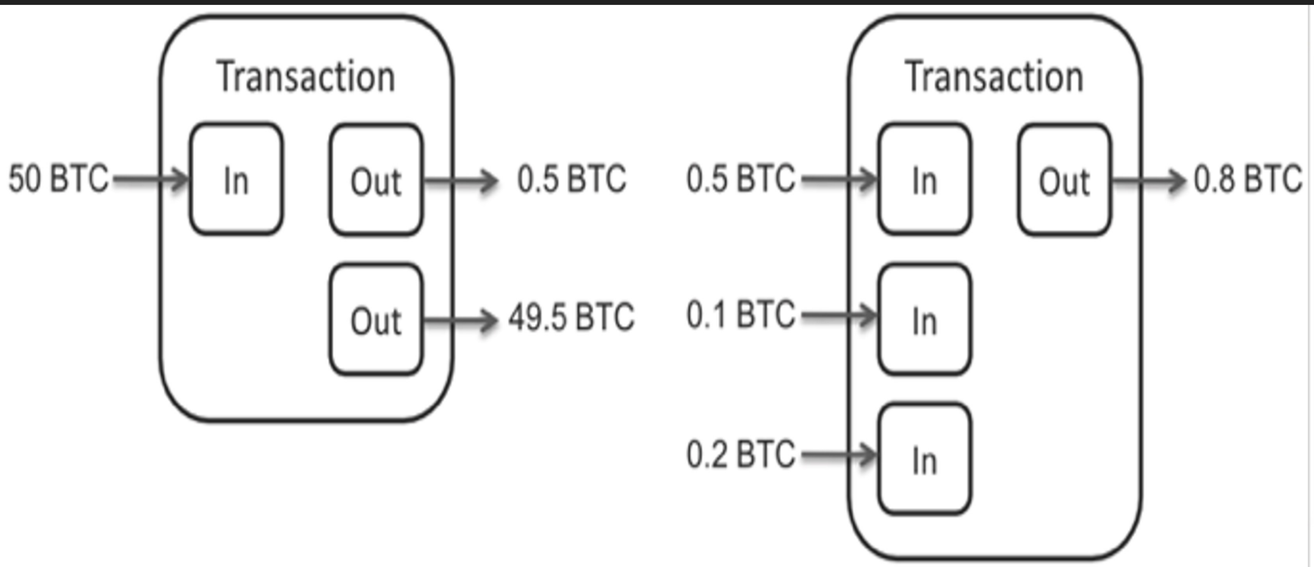
- L'utente che cede il controllo di *bitcoin* abbia effettivamente il controllo di quei *bitcoin*
- Che quei *bitcoin* non siano usati contemporaneamente in altre transazioni (il c.d. «problema della doppia spesa»)

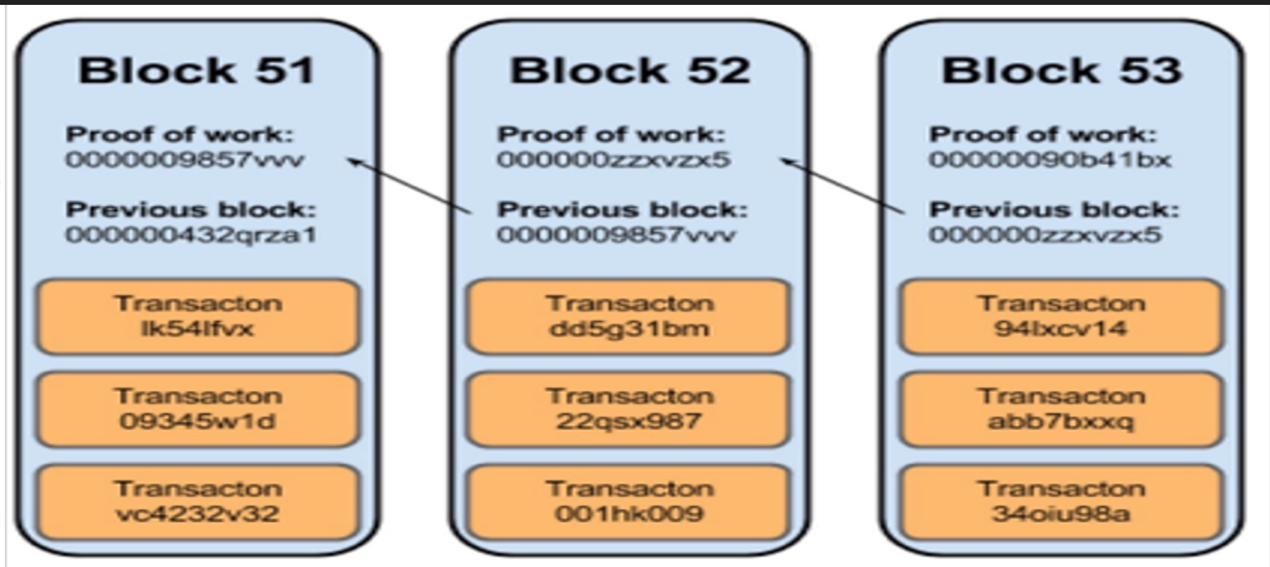
TRT

BITCOIN: COME FUNZIONA LA SUA *BLOCKCHAIN*?

Esistono due tipologie principali di

Le transazioni valide sono accettate (e Giovanni riceve il controllo dei 2 *bitcoin*), le altre respinte.
Il blocco viene «chiuso» e crittografato. Il blocco contiene un riferimento al precedente blocco. Si crea una catena ininterrotta di blocchi, cioè di transazioni registrate.
Si ripete, dunque, il ciclo con altre transazioni.





TRT

BITCOIN: COME FUNZIONA LA SUA *BLOCKCHAIN*?

Esistono due tipologie principali di blockchain:

Come vengono remunerati i validatori delle transazioni? Con il c.d. *mining.*

Chi crea i blocchi e valida le transazioni sono i nodi detti «*miners*»
Competono tra di loro per creare il blocco successivo.
Devono risolvere un «puzzle matematico» computazionalmente molto oneroso (anche in termini di consumo di energia elettrica).
Chi risolve il puzzle valida le transazioni e invia a tutti gli altri nodi il blocco per verifica.
Se tutto è corretto, gli altri nodi accettano implicitamente il nuovo blocco, andando a risolvere il
prossimo puzzle.
Chi crea il blocco viene remunerato con 6,25 *bitcoin* (generati *ex novo*). In più, percepiscono una piccola percentuale dalle transazioni.
Viene creato un blocco ogni 10 minuti. Il totale di *bitcoin* che verrà creato è già stabilito (ci si arriverà tra decenni).

TRT

The Rock Trading

«TENTATIVI DEFINITORI»

www.therocktrading.com

LE FONTI NORMATIVE: MONETA ELETTRONICA?

La definizione di moneta elettronica è stata indicata dalla direttiva Europea 2009/110/CE attuata in Italia con il D.Lgs. 16 aprile 2012 n. 45, quale "*il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso dietro ricevimento di fondi per effettuare operazioni di pagamento […] e che sia accettato da persone fisiche o giuridiche diverse dall'emittente di moneta elettronica*".

Emergono, dunque, delle analogie con la valuta virtuale, ossia il carattere dematerializzato, la presenza di una serie di bit memorizzati su un supporto elettronico, l'utilizzo delle stesse per effettuare acquisti; ma la differenza sostanziale consiste nel fatto che la valuta virtuale non ha corso legale nello Stato, pertanto la sua emissione non avviene da parte di emittenti riconosciuti e controllati dalle banche centrali nazionali.

TRT

LE FONTI NORMATIVE: MONETA ELETTRONICA?

Esistono due tipologie principali di

Sebbene le valute virtuali non siano equiparabili alla moneta elettronica, tale circostanza non impedisce di considerare lecito l'acquisto, l'utilizzo e l'accettazione in pagamento di valute virtuali, in quanto le parti sono libere di obbligarsi come ritengono più opportuno, in a base ad un principio generale dell'ordinamento: il principio consensualistico.

In questa prospettiva la funzione della valuta virtuale è la medesima della moneta, ossia mezzo di scambio, seppur sia emessa e accettata su base consensualistica e non legale; sul punto, si vedano:

- ❑ l'Opinione dell'Autorità Bancaria Europea del luglio 2014[1];
- ❑ la Comunicazione di Banca d'Italia del gennaio 2015[2].

Le Autorità hanno pertanto chiarito che l'acquisto e l'utilizzo delle valute virtuali è considerato una attività lecita, in quanto le parti sono libere di obbligarsi e corrispondere somme non aventi corso legale.

[1] European Banking Autority, EBA, Opinion on "virtual currencies", EBA/Op/2014/08, 4 luglio 2014, in www.eba.europa.eu.
[2] Banca d'Italia, Avvertenze sull'utilizzo delle cosiddette "valute virtuali", 30 gennaio 2015, in www.bancaditalia.it.

TRT

LE FONTI NORMATIVE: MONETA ELETTRONICA?

Esistono due tipologie principali di blockchain:

Al riguardo è opportuno citare una sentenza della Corte Europea circa l'obbligo di versare l'IVA in caso di prestazione di servizi di cambio bitcoin/valuta tradizionale[11]. Tale sentenza ha chiarito che la valuta virtuale non è assimilabile alla moneta legale, seppur abbia la medesima finalità di mezzo di pagamento.

Non da ultimo, è da sottolineare la direttiva UE 2018/243 del Parlamento Europeo e del Consiglio del 30 maggio 2018, di modifica della direttiva UE 2015/849 in materia di antiriciclaggio c.d. V Direttiva AML, la quale ha fornito una definizione di valuta virtuale, ossia "*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*".

TRT

LE FONTI NORMATIVE: PRODOTTO FINANZIARIO?

Esistono due tipologie principali di

Parte della dottrina ritiene che la valuta virtuale sia da includere nel novero dei c.d. strumenti finanziari.

Tuttavia, l'art. 1, comma 2 del D.Lgs. 58/1998 (c.d. T.U.F.) indica con un elenco tassativo gli strumenti finanziari, da cui sono escluse le valute virtuali.

Sembrerebbe, invece, compatibile una associazione con la definizione di prodotto finanziario, di cui all'art. 1, comma 1, lett. u) del T.U.F., che comprende – oltre agli strumenti finanziari – anche l'ampia nozione di "*ogni altra forma di investimento di natura finanziaria*".

Una parte della dottrina, cui si associano alcune comunicazioni della Consob, sostiene che le "altre forme di investimento" ricomprenderebbero "ogni strumento che sia idoneo alla raccolta del risparmio, comunque denominato o rappresentato, purché rappresentativo di un impego di capitale".

La Consob – riassumendo differenti delibere della stessa autorità aventi ad oggetto società offerenti criptovalute – ha chiarito che per definire un'attività quale investimento devono ricorrere l'impiego di capitale, un'aspettativa di rendimento di natura finanziaria, l'assunzione del rischio connesso all'impiego del capitale.

TRT

LE FONTI NORMATIVE: LA V DIRETTIVA AML

Esistono due tipologie principali di blockchain:

Infine, occorre evidenziare che la V Direttiva AML ha sottoposto agli obblighi antiriciclaggio sia i prestatori di cambio valute virtuali che i prestatori di servizi di portafoglio digitale.

Tenuto conto della pseudoanonimizzazione che contrataddistingue le transazioni in cripotovalute, il legisislatore europeo ha ritenuto opportuno procedere alla registrazione degli operatori, al fine di garantire una prima forma di controllo.
A tal riguardo l'Italia ha applicato tali disposizioni con il D.Lgs. 90/2017, il quale ha modificato il D.Lgs. 231/2007 nonché il D.Lgs. 141/2010, in materia di contratti di credito ai consumatori.

TRT

LE FONTI NORMATIVE: LA V DIRETTIVA AML?

Esistono due tipologie principali di blockchain

Occorre evidenziare che l'art. 1, comma 2, lett. ff) del D.Lgs. 231/2007 definisce i prestatori di servizi relativi all'utilizzo di valute virtuali come "*ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale*".

Inoltre, il D.Lgs. 25 maggio 2017, n. 90 ha modificato l'art. 17 bis, del D.Lgs. 141/2010, il quale ha disposto l'istituzione ad opera dell'OAM, Organismo degli agenti in attività finanziaria e dei mediatori creditizi, di un registro dei cambiavalute. (il "Registro").

La modifica introdotta ha visto l'istituzione, da parte dell'OAM, di una sezione speciale del predetto Registro, per il censimento dei prestatori di servizi relativi all'utilizzo di valuta virtuale e i prestatori di servizi di portafoglio digitale.

TRT

LE FONTI NORMATIVE: LA V DIRETTIVA AML

Esistono due tipologie principali di blockchain

Il Ministero dell'economia e delle finanze ha dunque predisposto lo schema di decreto (lo "Schema di Decreto") attuativo del nuovo articolo 17-bis, comma 8-ter del decreto legislativo 13 agosto 2010, n.141, con il quale s'intende predisporre un regime di registrazione obbligatoria dei soggetti che operano in criptovalute.

Lo Schema di Decreto - frutto della nuova disciplina antiriciclaggio introdotta dal decreto legislativo 25 maggio 2017, n. 90 e dall'ultimo aggiornamento di cui al decreto legislativo 4 ottobre 2019, n. 125, in recepimento della V direttiva EU - è stato oggetto di una consultazione pubblica, i cui esiti sono disponibili sul sito internet del MEF, e rappresenta un'opportunità per iniziare a costruire un'infrastruttura regolamentare per il mondo delle valute virtuali in Italia, con il più ampio coinvolgimento delle istituzioni pubbliche e private.

TRT

FUTURI SCENARI NORMATIVI PER GLI *EXCHANGE*

Esistono due tipologie principali di blockchain:

“MiCAR” - Proposta di regolamento sui mercati dei cripto-asset che mira a creare un quadro normativo armonizzato per gli emittenti di cripto-asset e i fornitori di servizi di cripto-asset che operano nell'UE.

“Pilot Regime” - Proposta di regolamento su un regime pilota per le infrastrutture di mercato basato su DLT che introduce una sandbox normativa a livello europeo all'interno della quale le entità che intendono gestire infrastrutture di mercato DLT possono essere esentate da alcuni requisiti che impediscono la diffusione della DLT nella negoziazione di titoli.

“Travel Rule”- Trasfer funds regulation che seguendo le linee guida del FATF/GAFI per il settore delle criptovalute, attraverso la revisione dell'attuale regolamento sui dati informativi che accompagnano i trasferimenti di fondi (regolamento 2015/847/UE) – che, ad oggi, si applica ai soli prestatori di servizi di pagamento –, applicherà la “travel rule”- anche ai trasferimenti di cripto-asset.

TRT

MiCAR: QUESITI CHE COINVOLGO GLI *EXCHANGE*

- "*Cripto-attività: una rappresentazione digitale di valore o di diritti che possono essere trasferiti e memorizzati elettronicamente, utilizzando la tecnologia di registro distribuito o una tecnologia analoga*".
- Definizione ampia che comprende vari tipi token: valute virtuali, di pagamento, di utilità e token ibridi.

- MiCAR riuscirà a creare parità di condizioni per l'eservizio dell'attività di "crypto exchange"?

- MiCAR riuscirà a prevenire le pratiche di manipolazione di mercato ed una maggiore trasparenza dei dati al mercato?

TRT

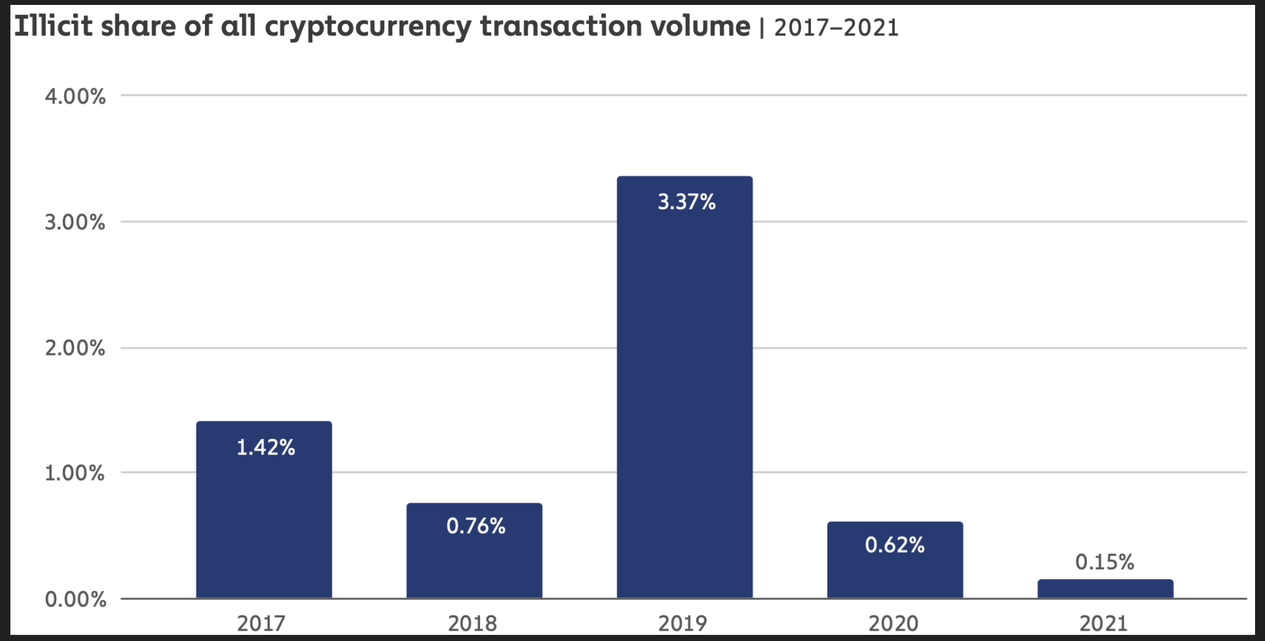
The Rock Trading

«ALCUNI DATI»

www.therocktrading.com

I DATI

Le transazioni che coinvolgono indirizzi illeciti rappresentano solo lo 0,15% del volume di transazioni di criptovalute nel 2021, nonostante il valore del volume delle transazioni illecite abbia raggiunto il livello più alto di sempre (essendo correlato alla crescita generale dei volumi).

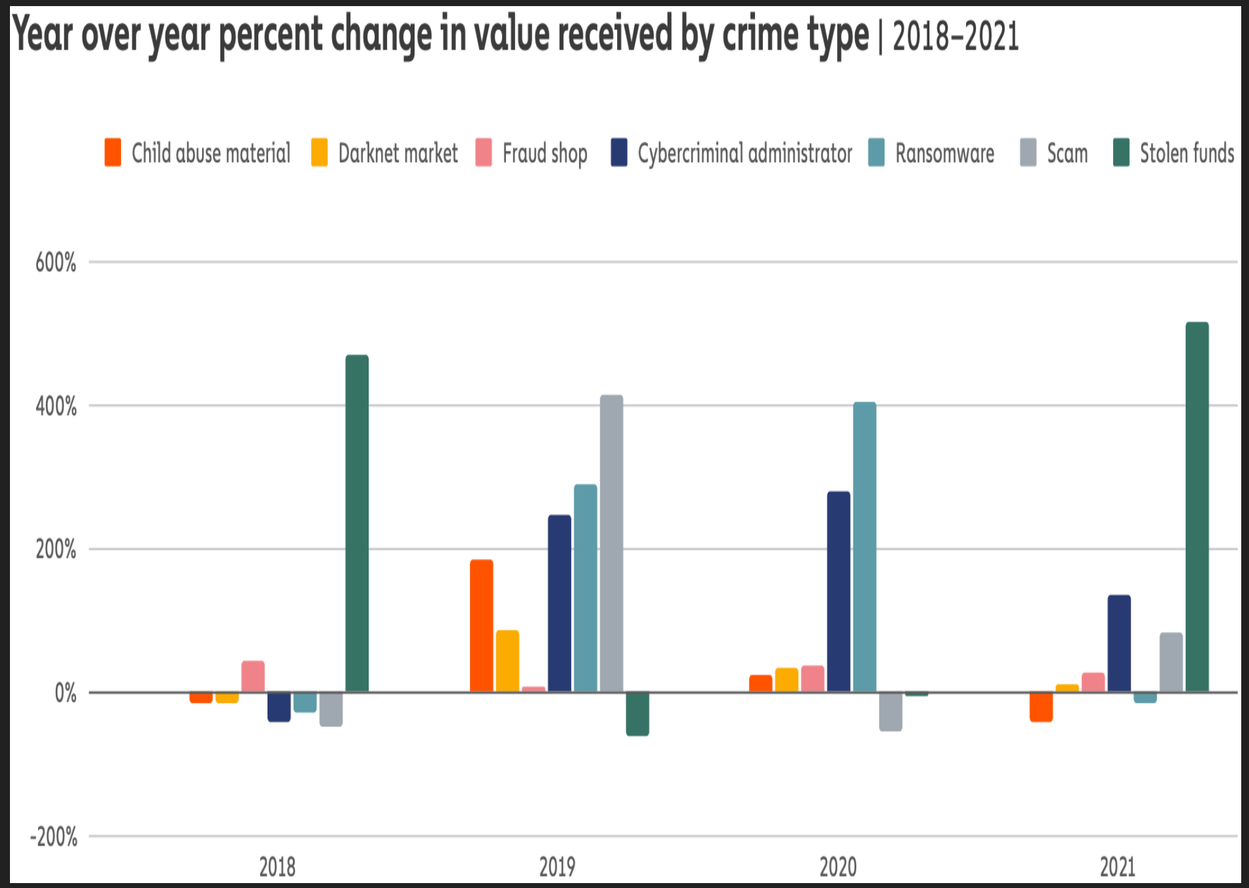


Fonte: Chainalysis,'The 2022 Crypto Crime Report'

TRT

I DATI

Due categorie spiccano per la loro crescita: i fondi rubati e, in misura minore, le truffe. Nel 2020, poco meno di 162 milioni di dollari di criptovalute sono stati rubati dalle piattaforme DeFi, che ha rappresentato il 31% dell'importo totale rubato nell'anno. Questo dato rappresenta un aumento del 335% rispetto al totale rubato dalle piattaforme DeFi nel 2019. Nel 2021, questa cifra aumenterà di un altro 1.330%. In altre parole, con la crescita della DeFi è cresciuto anche il problema dei fondi rubati e delle rug pull.

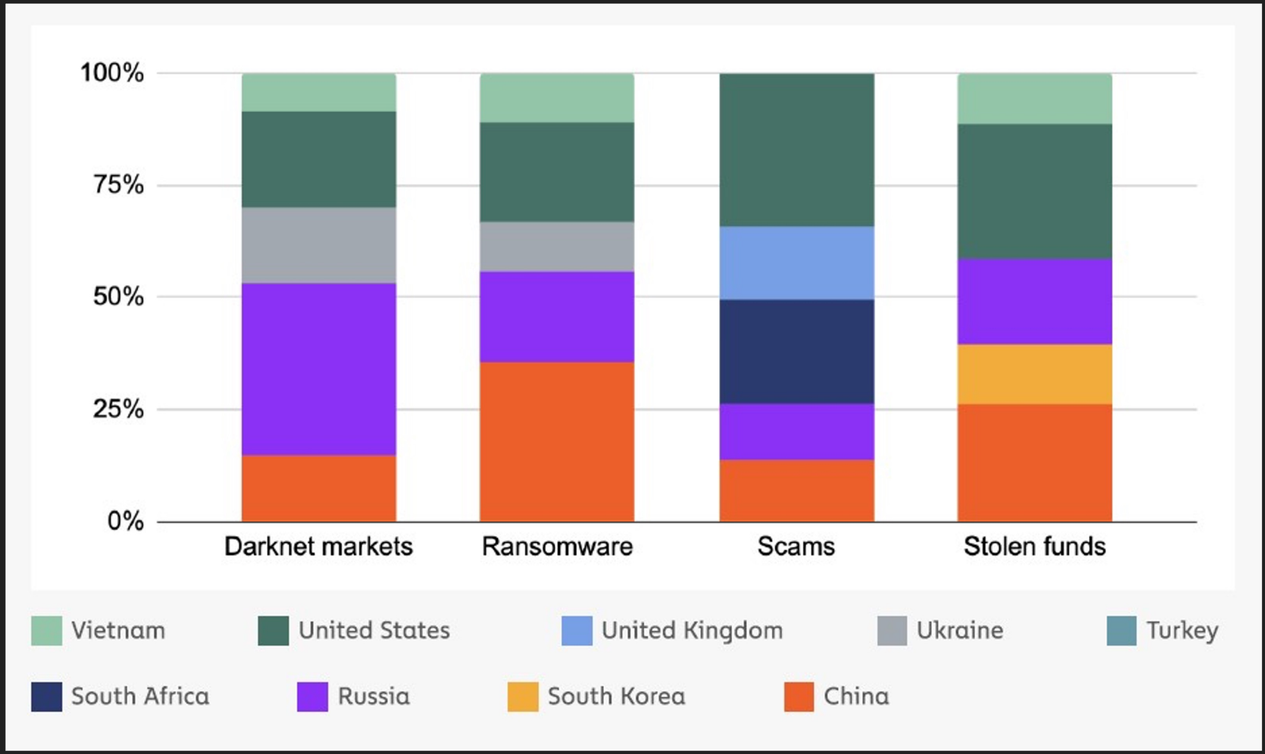


Fonte: Chainalysis 'The 2022 Crypto Crime Report'

TRT

I DATI

Nel corso del 2020, le truffe e le transazioni nel dark web, che insieme comprendono circa l'80% delle attività illecite che interessano le criptovalute, trovano maggiore spazio rispettivamente negli USA e Russia.
Rilevante anche l'alta incidenza di Ransomware in Cina e il furto di fondi sempre negli USA.

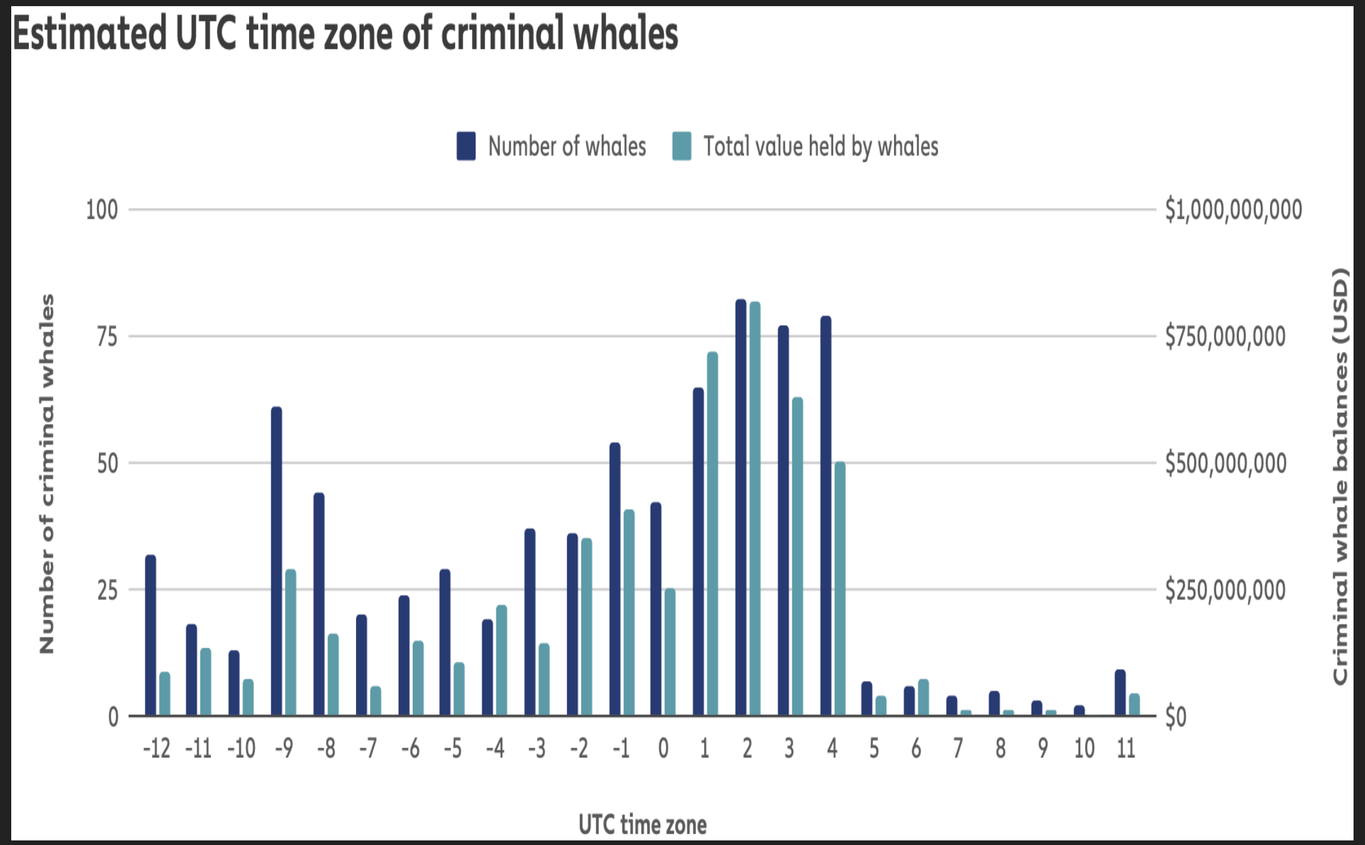


Fonte: Chainalysis 'The 2021 Crypto Crime Report'

TRT

I DATI

Si stima che le zone orarie UTC 2, 3 e 4 contengano il maggior numero di balene criminali, mentre fusi orari 1 e -9 ne hanno un gran numero. I fusi orari UTC 2, 3 e 4 comprendono gran parte della Russia, compresi i grandi centri abitati come Mosca e San Pietroburgo. della Russia, compresi i principali centri abitati come Mosca e San Pietroburgo. Tuttavia, i fusi orari ci permettono solo di stimare la posizione longitudinale (Sudafrica, l'Arabia Saudita o l'Iran?).



Fonte: Chainalysis 'The 2021 Crypto Crime Report'

TRT

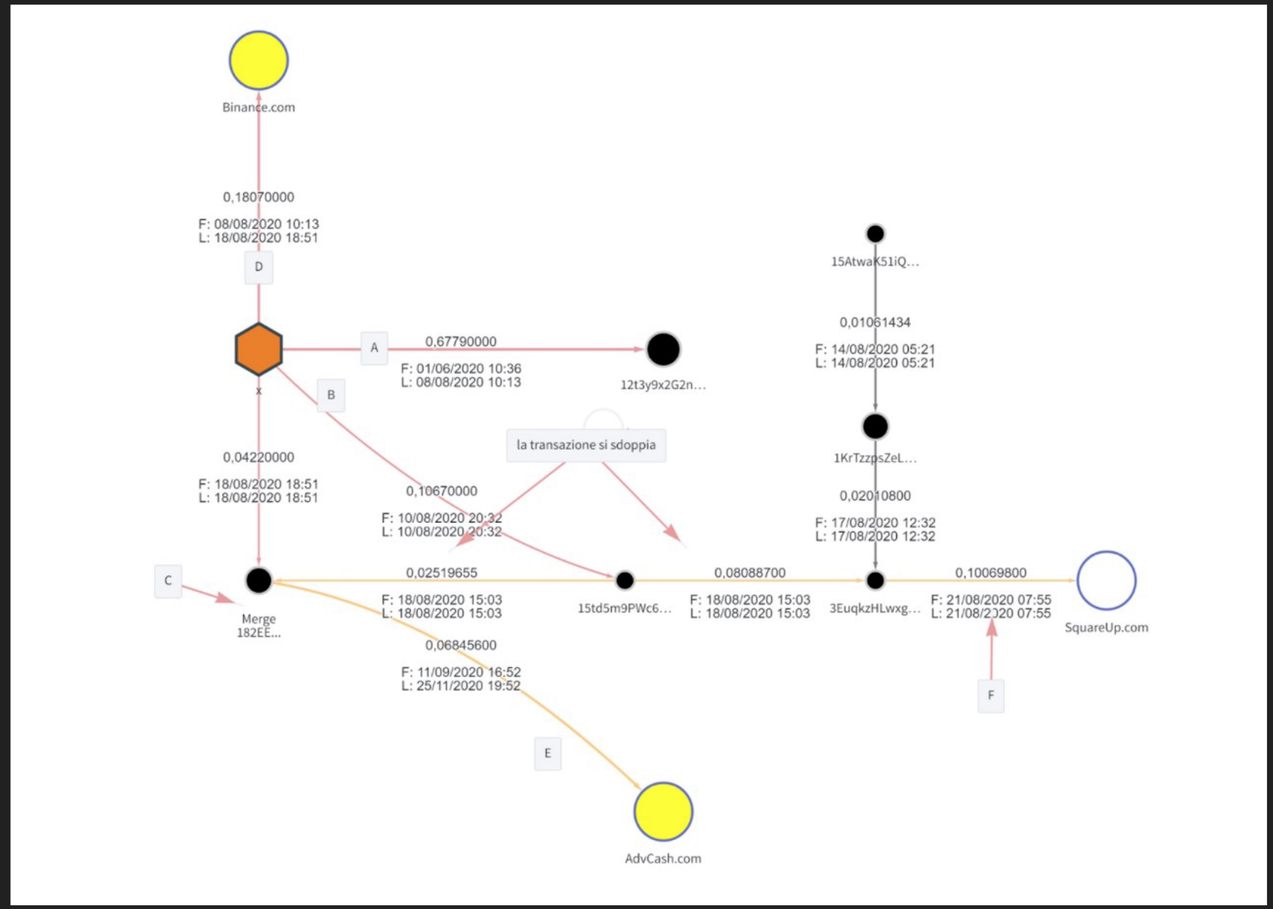
The Rock Trading

«*Blockchain forensics*»

www.therocktrading.com

ANALISI KYT

Tramite l'evoluzione dei sistemi di analisi forense delle transazioni, uniti alla trasparenza della *blockchain*, è possibile ripercorrere e ricostruire lo storico di ogni movimentazione, potendo così segnalare e individuare potenziali criticità.



Esempio di analisi KYT

TRT

INTRODUZIONE

“KYT” è l’acronimo di “Know Your Transaction”, la prima soluzione di compliance automatizzata offerta da Chainalysis e poi, con altri nomi, da altri fornitori.

La finalità del KYT è quella di esporre all’utente le informazioni rilevati in modo chiaro e immediato.

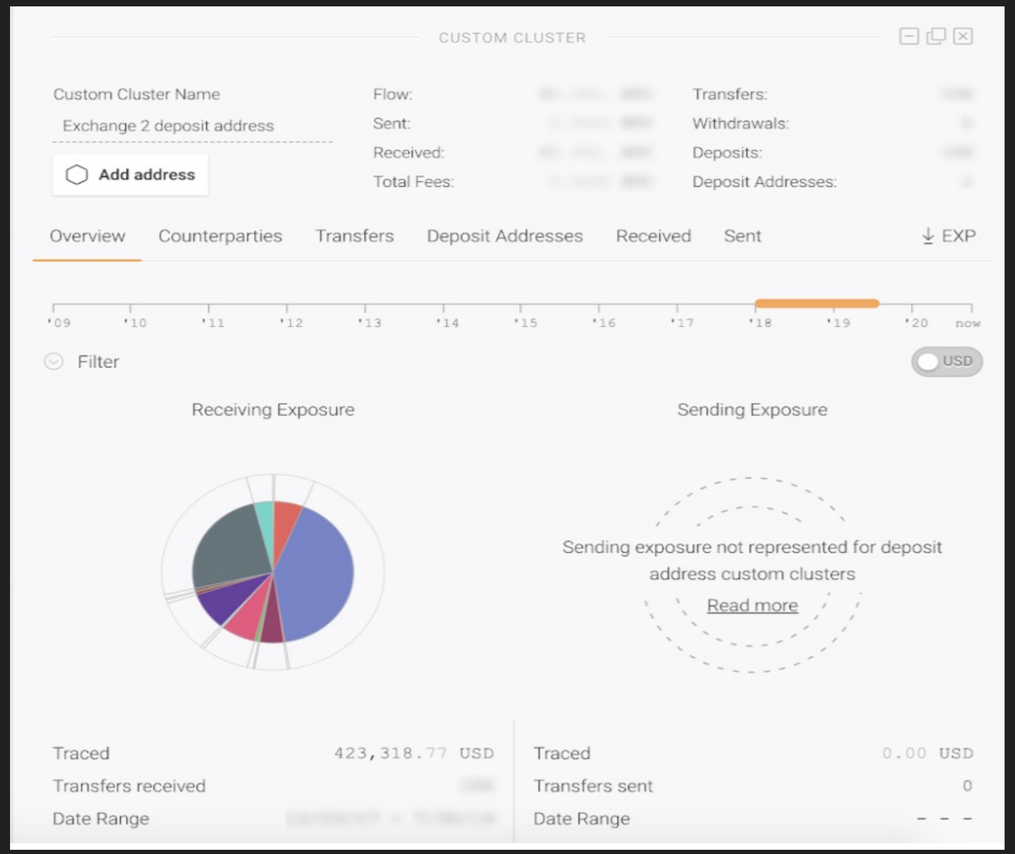
L’utente deve però sempre compiere una *enhanced due diligence* con altri strumenti.

TRT

DASHBOARD

La *dashboard* è costituita dalle seguenti sezioni:

- *Overview* della distribuzione delle categorie di rischio dei clienti;
- Grafico del volume dell'esposizione diretta complessiva degli utenti dell'*exchange*;
- Exposure complessiva dell'*exchange*.



USER RISK PROFILE

Il *risk assessment* di un utente è basato sull'aggregato di tutte le transazioni.

Tre sono i profili di rischio:

Alto rischio Medio Rischio Basso Rischio

THEROCK TRADING

ESEMPIO DI DETERMINAZIONE DEL PROFILO DI RISCHIO NELLA *BLOCKCHAIN FORENSICS*

1. Eliminazione delle exposure con valore inferiore a $5;
2. Analisi relativa, ovvero quanto valore percentuale del totale delle transazioni è collegata a controparti rischiose (se tale percentuale è maggiore del 10% si ha un incremento del fattore di rischio);
3. Analisi assoluta, ovvero quanto valore assoluto del totale delle transazioni è collegata a controparti rischiose (se tale valore è maggiore di $500 si ha un incremento del fattore di rischio);
4. Se l'attività rischiosa dell'utente è maggiore del 10% e ha un controvalore maggiore di $500 allora il profilo di rischio dell'utente è alto.

TRT

ESPOSIZIONI DIRETTE E INDIRETTE

Il *risk profile* è ricalcolato:

- ad ogni transazione;
- settimanalmente, se non ci sono nuove transazioni.

Vengono individuati i seguenti indirizzi a rischio:

- Darknet markets, Gioco d’azzardo, Exchange ad alto rischio, Mixers, Servizi P2P, Ramsomware, Siti Scam (truffe),
- Pedopornografia, terrorismo, sanzioni
- ed in generale indirizzi identificabili

TRT

STRATEGIE DI *CLUSTERING*

Un *cluster* è un aggregato di indirizzi che si ritiene esser controllati da una singola entità.

La *blockchain* contiene la storia di tutte le transazioni e quindi informazioni sugli indirizzi utilizzati.

Come fanno i *provider* di *blockchain forensics tool* a (ri-)collegare a un’entità reale l’indirizzo o l’insieme di indirizzi che essa controlla?

TRT

STRATEGIE DI *CLUSTERING*

I *provider* di *blockchain forensics tool* analizzano la/le *blockchain* usando specifiche tecniche di *clustering* ed euristiche, per esempio:

- *Co-spend*: questa euristica raggruppa indirizzi che contribuiscono input in una transazione. L'inferenza è che questi indirizzi di contribuzione siano controllati dalla stessa entità;

- *Behavioural*: identificazione di *pattern* temporali e strutturali;

- *Intelligence*: investigazione manuale, *data leak*, *data partenership*, ecc.

TRT

STRATEGIE DI *CLUSTERING* (UN ESEMPIO)

Ad esempio, un investigatore, che collabora con tali *provider*, si iscrive presso un marketplace nel dark web ed effettua una serie di depositi e prelievi.

Con gli indirizzi ottenuti, una volta analizzati dagli algoritmi di *clustering*, è in grado di ottenere l'intero cluster di quel marketplace.

Attenzione: dato che il *clustering* è una stima, raramente si ottiene una copertura completa di tutti gli indirizzi che appartengono ad una specifica entità.

TRT

EXPOSURE

Esposizione diretta: connessione diretta tra il *cluster* oggetto di analisi e un *cluster* identificato.

Esposizione indiretta: connessione indiretta tra il *cluster* oggetto di analisi e un *cluster* identificato; questa connessione è individuata passando per cluster non identificati fino a raggiungere un *cluster* identificato.

Attraverso questo metodo si stima l'origine e la destinazione dei fondi.

TRT

REAZIONE

- TRT analizza in tempo reale tutte le transazioni in entrata ed uscita sulla propria piattaforma
- I *tool* di *blockchain forensics* forniscono una indicazione di rischio dell'operatività del cliente che puo mutare nel tempo anche retroattivamente.
- Se TRT riceve una segnalazione sospetta di anomalia, verifica manualmente se esistono i presupposti per ulteriori azioni.
- In caso affermativo, viene coinvolto un/a analista interno/a per una valutazione approfondita
- Se il riscontro dell'anomalia risulta essere di rilevanza, si procede con le relative azioni a secondo della gravità (segnalazione SOS, coinvolgimento della Cyber Crime Financial Unit, ecc.).

TRT

ESEMPI PRATICI

1. Richiesta d’informazioni da parte della Polizia Postale di Milano a fronte di una indagine della Procura di Brindisi.

2. Richiesta di analisi forense da parte della UIF a fronte di una nostra SOS.

TRT

The Rock Trading

Grazie!

www.therocktrading.com

TRT