BLOCKCHAIN E CRIPTOVALUTE

Avv. Daniele Nigro

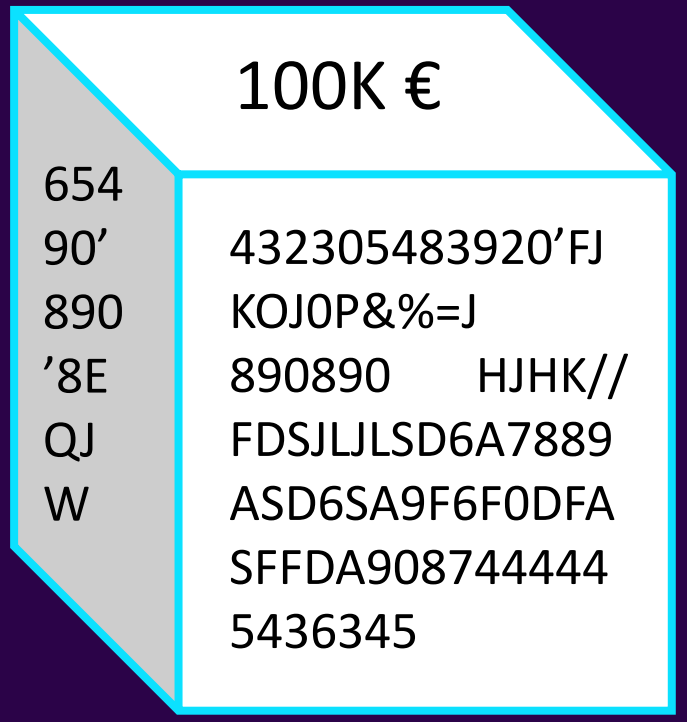
BLOCKCHAIN: DEFINIZIONE

Blockchain significa letteralmente “catena di blocchi”. È una rete informatica di nodi che gestisce in modo univoco e sicuro un registro pubblico composto da una serie di dati e informazioni, come le transazioni, in maniera aperta e distribuita, senza che sia necessario un controllo centrale.

ARCHIVIO DIGITALE CONDIVISO DECENTRALIZZATO CONSULTABILE DA CHIUNQUE

STRUTTURA DI OGNI BLOCCO DELLA CATENA *(AD ESEMPIO TRANSAZIONE IN BITCOIN)*

HASH DEL BLOCCO PRECEDENTE

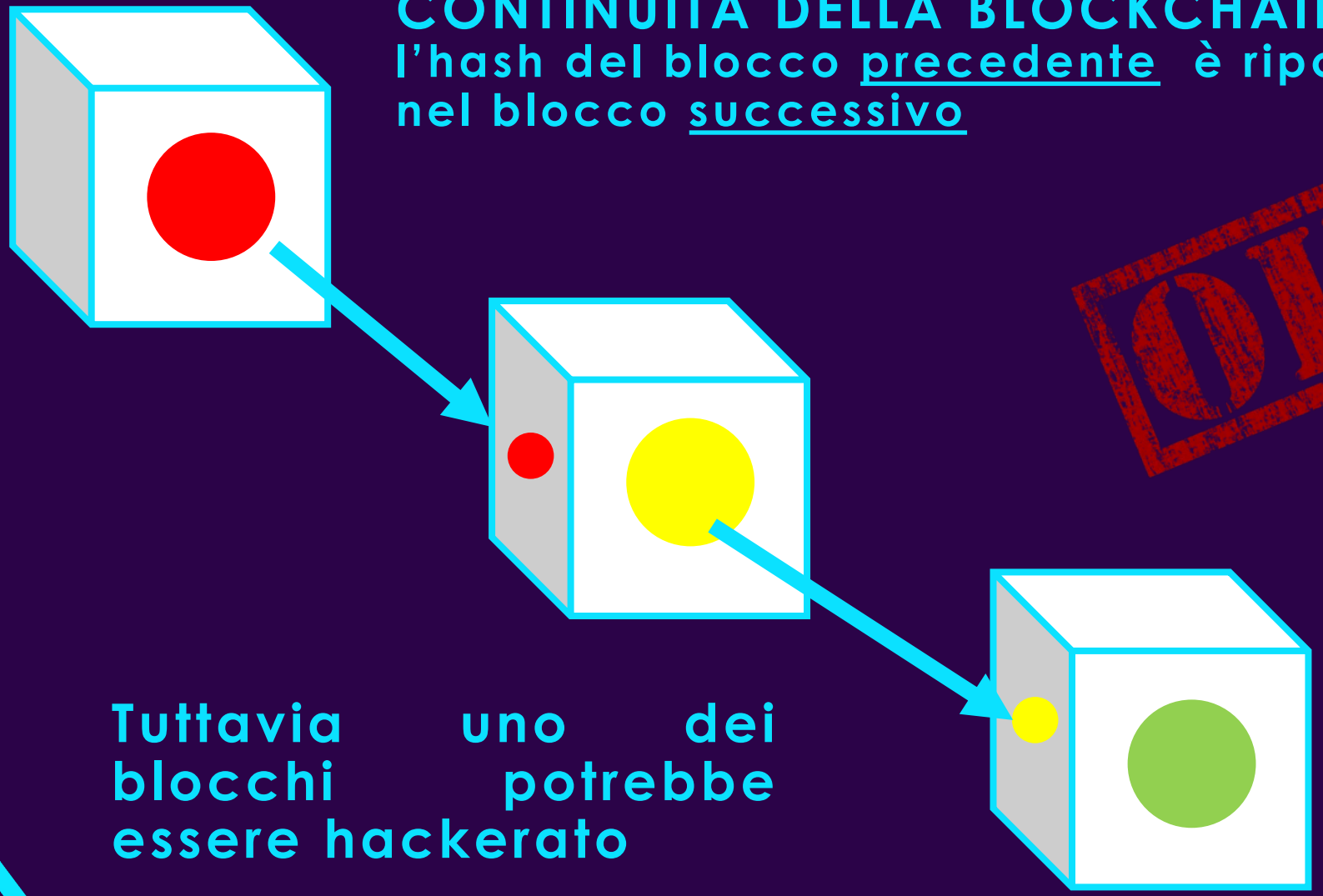


DATO DA TRASMETTERE *(AD ESEMPIO IMPORTO TRANSAZIONE)*

HASH DEL BLOCCO

SI BASA SU STRINGHE DI HASH: sequenze di bit irripetibile ed univoca

CONTINUITÀ DELLA BLOCKCHAIN:
l'hash del blocco precedente è riportato nel blocco successivo



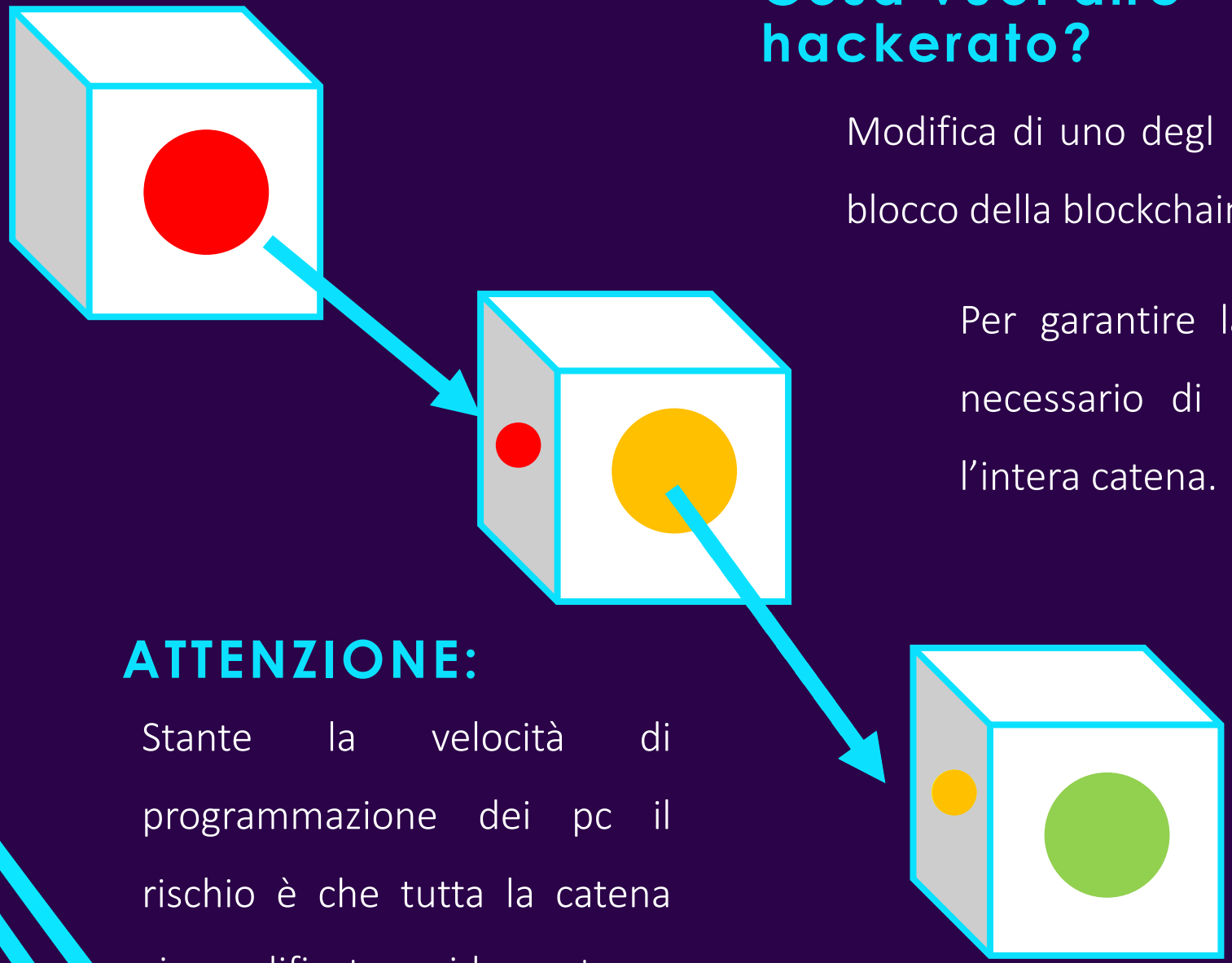
Tuttavia uno dei blocchi potrebbe essere hackerato

Non c'è più continuità nella blockchain.

Cosa vuol dire hackerato?

Modifica di uno degl hash del blocco della blockchain.

Per garantire la continuità è necessario di riprogrammare l'intera catena.



ATTENZIONE:

Stante la velocità di programmazione dei pc il rischio è che tutta la catena sia modificata rapidamente.

COME GARANTIRE LA SICUREZZA?

1

CONDIVISIONE DEI DATI

Non esiste una banca

dati centralizzata

2

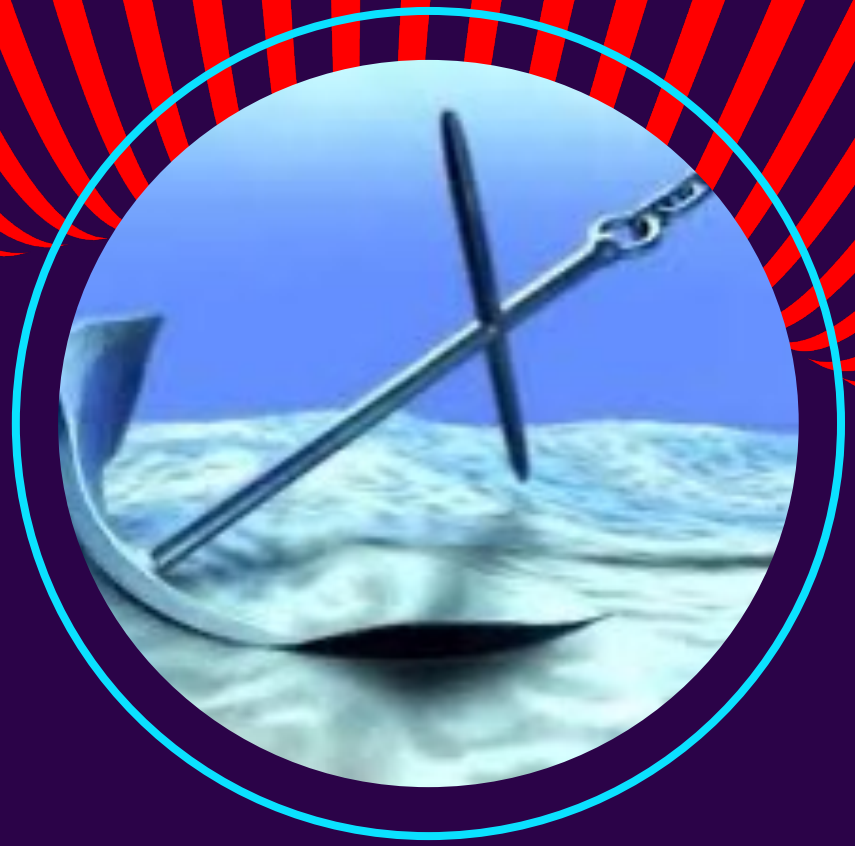
RALLENTARE LE OPERAZIONI DI MODIFICA SEQUENZA DEGLI HASH DEI BLOCCHI

Meccanismo crittografico rappresentano dal

sistema premiale della proof of work

PROOF OF WORK

È una competizione tra programmatori per risolvere algoritmi o equazioni crittografiche e convalidare le transazioni per guadagnare blockchain (meccanismo premiale).



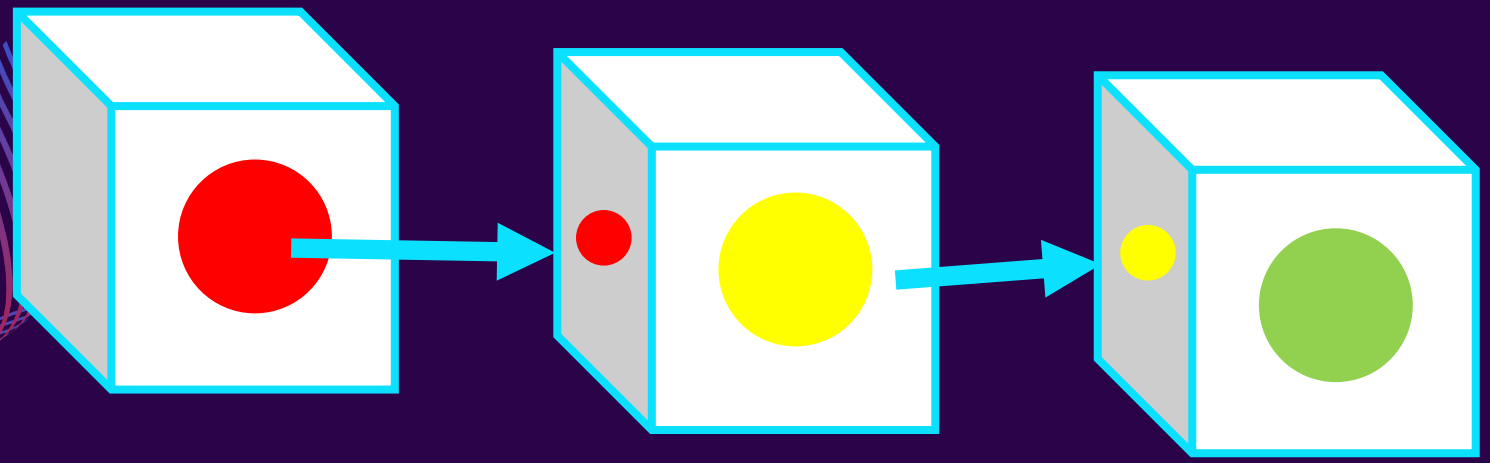
Per aggiungere nuovi dati si richiedono operazioni complesse (aggiunta di un nuovo hash di bitcoin oggi chiede circa 10 minuti).

Come una ancora che cerca di rallentare il sistema di sviluppo.

IL SISTEMA PUÒ ESSERE CONSULTATO DA CHIUNQUE

Una volta che le informazioni sono registrate nella blockchain sono difficili da cambiare perché sono condivise: tutti hanno l'intera blockchain.

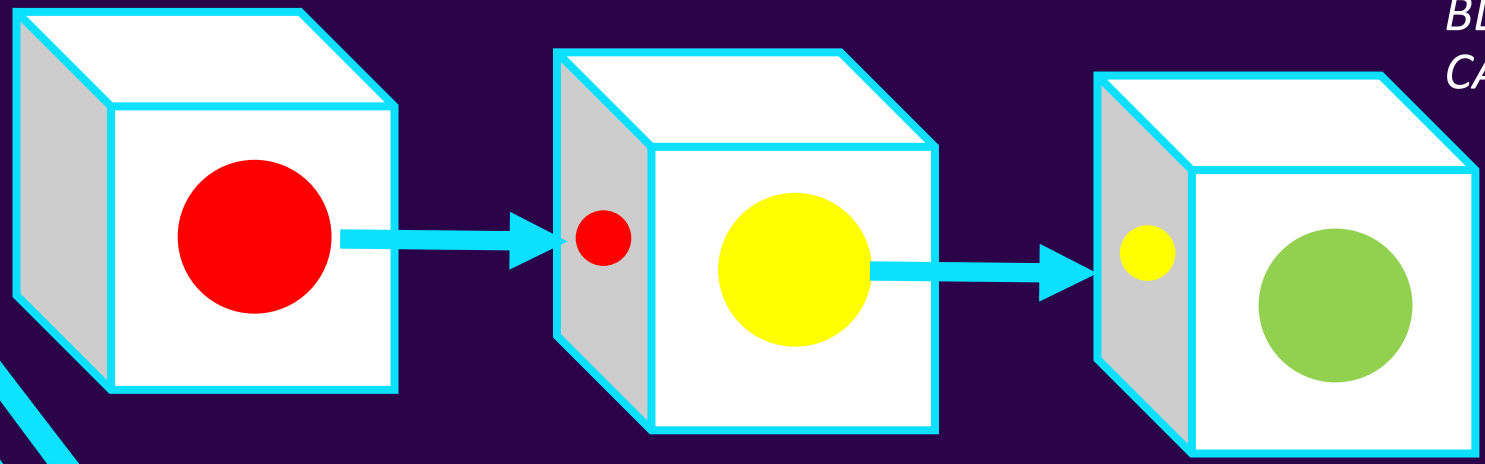
BLOCKCHAIN DI TIZIO



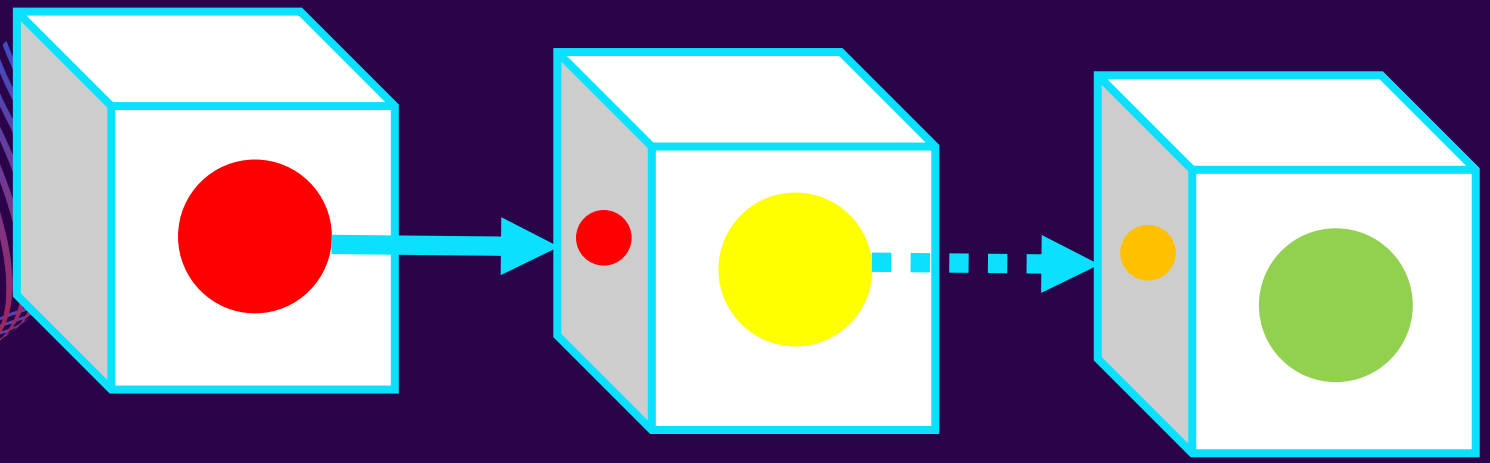
Se Tizio aggiunge un blocco alla blockchain lo stesso viene inviato a Caio il quale aggiunge il medesimo blocco.

Caio verifica coincidenza e valida la catena.

BLOCKCHAIN DI CAIO



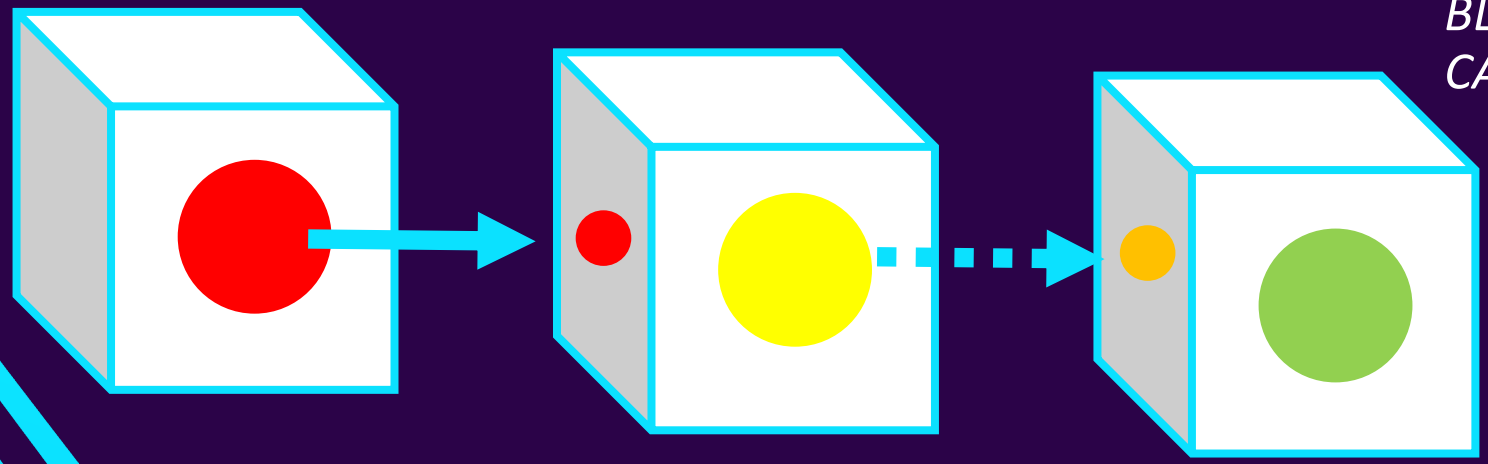
BLOCKCHAIN DI TIZIO



Se Tizio aggiunge un blocco alla blockchian che è stato alterato.

Viene respinto dagli altri blocchi e la catena non è validata.

BLOCKCHAIN DI CAIO

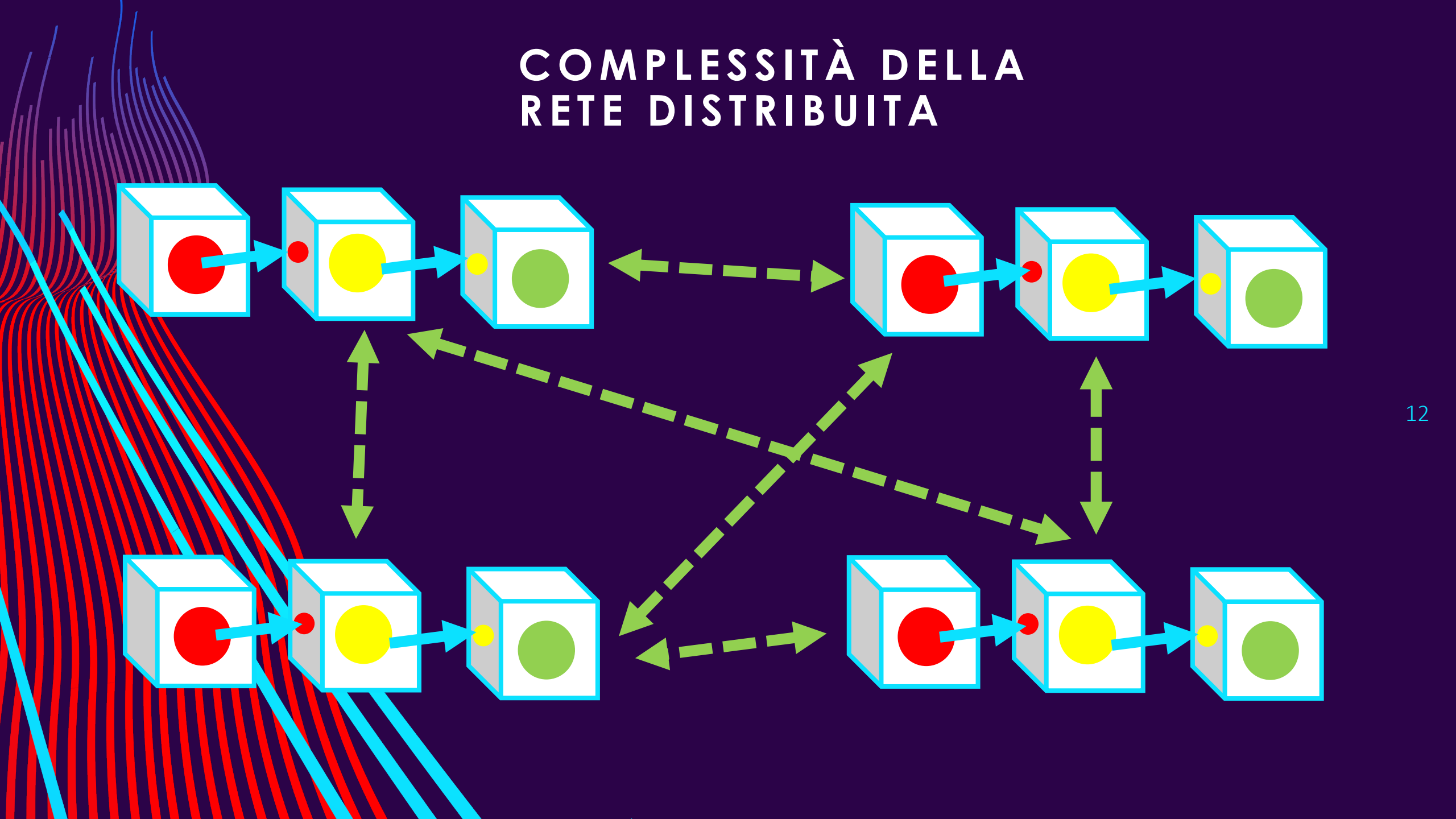


COME HACKERARE LA RETE?

Operazione difficile (o impossibile) in termine di tempo

Poco conveniente in termini economici

COMPLESSITÀ DELLA RETE DISTRIBUITA



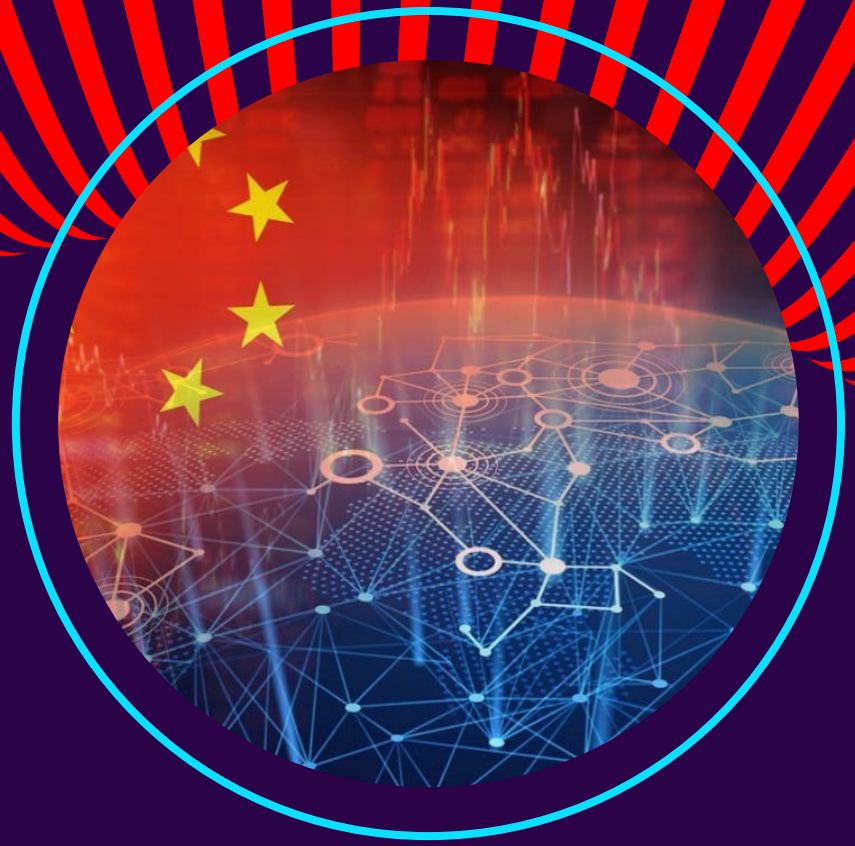
VANTAGGI DELLA BLOCKCHAIN

TRASPARENTE E DIFFUSI

Tutti possono accedere al sistema.

LIBERA

Tutti la possono usare.



RESISTENTE ALLA CENSURA

Nessuno può fermare il sistema.

USO DELLE BLOCKCHAIN

1. BITCOIN
2. SMART CONTRACT
3. CARTELLE SANITARIE
4. NFT


The
Economist

BITCOIN

IL BITCOIN È SOLO UNA DELLE CRIPTOVALUTE

DEFINIZIONE

Il Bitcoin è una moneta virtuale, ovvero che non viene stampata come la normale cartamoneta, ma che viene creata, distribuita e scambiata in maniera completamente virtuale, attraverso i computer, e con una tecnologia peer to peer.

CREATORE

(ANONIMO)

CREATO NEL 2008 DA SATOSHI NAKAMOTO:

- «Satoshi» significa «un pensiero chiaro, veloce e saggio»;
- «Naka» può significare «medium», «dentro» o «relazione»;
- «Moto» può significare «origine» o «fondamento».

CRIPTOVALUTE

- Bitcoin - BTC
- Ethereum - ETH
- Tether - USDT
- BNB - BNB
- USD Coin - USDC
- XRP - XRP
- Solana - SOL
- Cardano - ADA
- Terra - LUNA
- TerraUSD - UST
- Binance USD - BUSD
- Dogecoin - DOGE
- Avalanche - AVAX
- Polkadot - DOT
- Wrapped Bitcoin - WBTC
- SHIBA INU - SHIB
- Dai - DAI
- TRON - TRX
- NEAR Protocol - NEAR
- Polygon - MATIC
- Litecoin - LTC
- Cronos - CRO
- UNUS SED LEO - LEO
- Uniswap -UNI
- Bitcoin Cash - BCH
- FTX Token -FTT
- Algorand - ALGO
- Chainlink - LINK
- Cosmos - ATOM
- Stellar - XLM
- Monero - XMR
- Bitcoin BEP2 - BTCB
- Ethereum Classic - ETC
- ApeCoin - APE
- VeChain - VET
- Internet Computer - ICP
- Hedera - HBAR
- Filecoin - FIL
- Decentraland - MANA
- Axie Infinity - AXS

ONECOIN

LA CRIPTOVALUTA CHE HA INGANNATO IL MONDO

L'imprenditrice bulgara Ruja Ignatova voleva «sotterrare BitCoin» e ha creato una nuova criptovaluta che doveva cambiare il mondo: «OneCoin».

Dietro il suo sogno scintillante, però, si nascondeva una truffa da quattro miliardi di dollari, spariti insieme alla stessa Ignatova.

LO SCHEMA PONZI ADOTTATO DALLA «CRYPTOQUEEN»

- **FASE A.** Al potenziale cliente viene promesso un investimento con rendimenti superiori ai tassi di mercato, in tempi ravvicinati.
- **FASE B.** Dopo poco tempo viene restituita parte della somma investita, facendo credere che il sistema funzioni veramente.
- **Fase C.** Si sparge la voce dell'investimento molto redditizio; altri clienti cadono nella rete. Si continuano a pagare gli interessi con i soldi via via incassati.
- **Fase D.** Lo schema si interrompe quando le richieste di rimborso superano i nuovi versamenti.

SISTEMA CRITTOGRAFICO BITCOIN *(COME DI QUALUNQUE BLOCKCHAIN)*

CHIAVE PUBBLICA

La chiave pubblica (che funziona come una sorta di indirizzo mail) e deve essere comunicata alle altre persone per l'invio delle bitcoin.

CHIAVE PRIVATA

Codice di sicurezza noto solo al destinatario.

QUANDO VENGONO ASSEGNATE?

Sono attribuiti dal sistema al momento dell'acquisto ella bitcoin.

CRITTOGRAFIA

Lorem ipsum dolor sit amet, consectetur adipisci elit, sed do eiusmod tempor incidunt ut labore …….

CHIAVE PUBBLICA

Utente A cifra con chiave pubblica di B e trasmette.

fdsfssdadpd@~‹ ´©©©©‘¥“«qw 456u68qdjsakla òsadjkòl@≠`´‹ 21390890 fdjko 5609’ZZ>>>123

CHIAVE PRIVATA

Utente B decifra con propria chiave privata

Lorem ipsum dolor sit amet, consectetur adipisci elit, sed do eiusmod tempor incidunt ut labore …….

TRASFERIMENTO BITCOIN

CHIAVE PUBBLICA

Utente A cifra con chiave pubblica di B e trasmette dal proprio wallet le bitcoin.

CHIAVE PRIVATA

Utente B decifra con propria chiave privata e ricevere bitcoin

ESECUZIONE SU CRIPTOVALUTE: DOVE SONO CONTENUTE LE CHIAVI?

1

HARDWARE WALLET

Dispostivo che archivia off line chiavi.

2

SOFTWARE WALLET

Le chiavi sono installate su un pc

3

WEB WALLET

Contenute in un salvadanaio virtuale e remoto

PROBLEMA PRINCIPALE ESECUZIONE

REPERIBILITÀ

Le criptovalute sono all'interno della blockchain la cui caratteristica principale è l'anonimato del titolare.

COERCIBILITÀ DELLA CONSEGNA

In assenza di collaborazione da parte del debitore che consegna la chiave pubblica e privata è sostanzialmente impossibile individuare il proprietario.

REPERIBILITÀ

In assenza di collaborazione da parte del debitore che consegna la chiave pubblica e privata è sostanzialmente impossibile individuare il proprietario

MODALITÀ DI RICERCA

Richiesta al debitore al momento del pignoramento negativo

492 bis c.p.c. ma non vi è certezza dell'esistenza di una traccia nelle banche dati

L'UFFICIALE GIUDIZIARIO TROVA L'HARDWARE WALLET

Viene effettuato un pignoramento mobiliare.

Richiede competenze informatiche avanzate da parte dell'Ufficiale Giudiziario e comunque difficilmente verrebbe lasciata sulla «scrivania».

L'UFFICIALE GIUDIZIARIO TROVA IL SOFTWARE WALLET

Il software wallet è installato su un personal computer.

Potrebbe essere un bene impignorabile in quanto strumentale all'attività.

FORMA DEL PIGNORAMENTO: PIGNORAMENTO MOBILIARE

1

DEVICE CON PSW PUBBLICA E PRIVATA (NELL'IPOTESI DI HARDWARE WALLET E SOFTWARE WALLET)

2

CRIPTOVALUTA ALL'INTERNO DEL DEVICE

3

ENTRAMBI

SI HA LA CERTEZZA DELL'ESISTENZA DI UN WEB WALLET

Pignoramento presso terzi con dichiarazione del terzo.

Anche il provider non può fare nulla senza le chiavi in possesso e note solo al debitore (e nello specifico chiave privata).

FORMA DEL PIGNORAMENTO: PIGNORAMENTO PRESSO TERZI

PIGNORAMENTO

FORMALMENTE VALIDO

PIGNORAMENTO SOSTANZIALMENTE INSEGIBILE CON RISCHIO ESTINZIONE DELLA PROCEDURA

MANCANO I CODICI IDENTIFICATIVI

CHIAVE PUBBLICA E CHIAVE PRIVATA

SE È REPERITO IL WALLET (HARDWARE, SOFTWARE O REMOTO) LA BITCOIN COME DEVE ESSERE CONSIDERATA?

1. MONETA
2. STRUMENTO FINANZIARIO
3. BENE MOBILE

LIQUIDAZIONE FORZATA: MODALITÀ

1

MONETA / STRUMENTO FINANZIARIO

È sufficiente chiedere l'assegnazione del bene avendo la bitcoin un valore di mercato

2

BENE MOBILE

È necessaria la vendita e successiva assegnazione del ricavato

DEFINIZIONE DI VALUTA VIRTUALE

1

DIRETTIVA DEL 20.5.2015 N. 849 ART. 3

18) «valute virtuali»: 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

AGGIUNTA RISPETTO NORMATIVA EUROPEA: FINALITÀ DI INVESTIMENTO

2

D.LGS. 231/2007 ART. 1 LETT. QQ

qq) valuta virtuale: la rappresentazione digitale di valore, non emessa nè garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o **per finalità di investimento** e trasferita, archiviata e negoziata elettronicamente

DFINIZIONE DI EXCHANGER

EXCHANGE: piattaforma tecnologica che permette di scambiare il prodotto finanziario per acquisto e vendita criptovalute

D.LGS. 231/2007 ART. 1 (DEFINIZIONI):

FF) PRESTATORI DI SERVIZI RELATIVI ALL'UTILIZZO DI VALUTA VIRTUALE:

ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, anche online, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale o in rappresentazioni digitali di valore, ivi comprese quelle convertibili in altre valute virtuali nonchè i servizi di emissione, offerta, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio delle medesime valute

FF-BIS) PRESTATORI DI SERVIZI DI PORTAFOGLIO DIGITALE:

ogni persona fisica o giuridica che fornisce, a terzi, a titolo professionale, anche online, servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali

SOTTOPOSTI OBBLIGO ANTIRICICLAGGIO (ART. 3 – SOGGETTI OBBLIGATI)

1

D.LGS. 231/2007 ART 3 COMMA 5 – LETT. I

Rientrano nella categoria di altri operatori finanziari: […] i) i prestatori di servizi relativi all'utilizzo di valuta virtuale

2

D.LGS. 231/2007 ART 3 COMMA 5 – LETT. I BIS

Rientrano nella categoria di altri operatori finanziari: […] i-bis) i prestatori di servizi di portafoglio digitale

SOTTOPOSTI OBBLIGHI D.LGS. 58/1998 (T.U.F.)

→ **GIURISPRUDENZA**

OBBLIGHI T.U.F.

TRIB. VERONA 24 GENNAIO 2017

«La compravendita di valute virtuali (ad es. di bitcoin), qualificabili alla stregua degli strumenti finanziari, è un'operazione definibile ad alto rischio per il risparmiatore, il che obbliga colui il quale ne pubblicizzi la vendita, in proprio o per conto terzi, ad informare preliminarmente l'utente interessato all'acquisto sui rischi connessi all'investimento (c.d. informativa precontrattuale), così come stabilito dagli artt. 67 e ss. del codice del consumo in tema di commercializzazione a distanza di servizi finanziari ai consumatori; in particolar modo, il promotore dell'operazione di vendita è tenuto all'applicazione delle disposizioni più rigorose previste dalla normativa di settore che disciplina l'offerta del servizio o del prodotto interessato.»

OBBLIGHI ANTI RICICLAGGIO

CASSAZIONE PENALE SEZ. II - 17/09/2020, N. 26807

«In tema di intermediazione finanziaria, la vendita "on line" di moneta virtuale "bitcoin" pubblicizzata quale forma di investimento per i risparmiatori - ai quali vengano offerte informazioni sulla redditività dell'iniziativa - è attività soggetta agli adempimenti previsti dalla normativa in materia di strumenti finanziari, di cui agli artt. 91 e ss. t.u.f., la cui omissione integra il reato di cui all'art. 166, comma 1, lett. c), t.u.f»

SEQUESTRO PREVENTIVO WALLET

CASSAZIONE PENALE SEZ. II - 26/10/2022, N. 44378

«La valuta virtuale deve essere considerata uno "strumento di investimento" perché consiste in un "prodotto finanziario" e deve dunque essere disciplinata dalle norme in materia di intermediazione finanziaria (articolo 94 e seguenti del Tuf).

La II sezione penale, accogliendo il ricorso del Pg, ha disposto un nuovo giudizio in merito al mancato sequestro preventivo di un wallet contenente 30 bitcoin relativamente ai reati, ipotizzati, di esercizio abusivo dell'attività finanziaria e autoriciclaggio.

Nel caso specifico all'imputato era stata contestata la raccolta di fondi che "aveva avuto come scopo la creazione di una piattaforma decentralizzata di servizi logistici", e il fatto che "a chi aveva contribuito erano stati corrisposti in cambio LWF Coin, che costituivano titoli per l'utilizzo dei servizi della piattaforma". [...].»

CASSAZIONE PENALE SEZ. II - 26/10/2022, N. 44378

«[...] Per la Corte ricorrono tutti gli elementi distintivi dell'investimento finanziario, poiché i soggetti interessati all'investimento per ottenerlo:

"a) hanno erogato capitali (sotto la forma di bitcoin);

b) con l'aspettativa di ottenere un rendimento, costituito dalla corresponsione di altre monete virtuali che avrebbero permesso la partecipazione alla piattaforma, dal valore variabile a seconda del momento dell'acquisto e che avrebbe acquistato maggior valore se il progetto relativo alla piattaforma avesse avuto successo;

c) hanno assunto su di sé un rischio connesso al capitale investito.»

IN OGNI CASO: PROBLEMA PRINCIPALE ESECUZIONE CIVILE E PENALI CRIPTOVALUTE

CHIAVE PUBBLICA

Difficile individuare la chiave pubblica data la segretezza della struttura della blockchain.

CHIAVE PRIVATA

Obbligo infungibile che richiede la collaborazione del debitore.

POSSIBILI CONSEGUENZE MANCATA CONSEGNA

Pignoramento inesegibile con estinzione della procedura.

CONCLUSIONE:

Nell'ambito dell'attività di pignoramento delle criptovalute il problema principale consiste nell'individuazione delle chiavi pubbliche e private per le quali è necessaria la collaborazione del debitore sostanzialmente impossibile.

PIGNORAMENTO SOSTANZIALMENTE INSEGIBILE CON RISCHIO ESTINZIONE DELLA PROCEDURA

METAVERSO CONSULTING ®

GRAZIE PER L'ATTENZIONE

AVV. DANIELE NIGRO

Via Magenta, 27

26900 – Lodi

info@studionigro.eu

http://www.studionigro.eu