

REPUBBLICA ITALIANA
 TRIBUNALE DI FIRENZE
 RF.178/ 2018 e 205/2018

composto dai sig.ri magistrati

Dott. **Silvia Governatori** Presidente est.
 Dott. **Rosa Selvarolo** Giudice
 Dott. **Cristian Soscia** Giudice

riunito in camera di consiglio ha pronunciato la seguente

SENTENZA

In nome del Popolo Italiano

Nel procedimento promosso da:

[REDACTED], elett. dom. per mandato in atti presso prof. avv. Giuseppe Sbisà, avv. Monica Iacoviello e avv. Alessandra Frigerio del foro di Milano e avv. Nicola Pabis Ticci del foro di Firenze ed elett. dom. in Firenze presso quest'ultimo

Creditore Istante proc. [REDACTED]/2018

Pubblico Ministero in persona del dott. [REDACTED]

Istante proc. [REDACTED]/2018

Nei confronti di:

[REDACTED], nato a Firenze l'11.4.1986, quale titolare dell'impresa individuale [REDACTED], CF [REDACTED] con sede in [REDACTED], rappresentato e difeso dall'avv. Francesco Ballati, Marco Della Vedova e Prof. Avv. Francesco D'Angelo, elettivamente domiciliato presso lo stesso per mandato in atti

Debitore

Con l'intervento di:

[REDACTED] elett. dom. per mandato in atti presso prof. avv. Giuseppe Sbisà, avv. Monica Iacoviello e avv. Alessandra Frigerio del foro di Milano e avv. Nicola Pabis Ticci del foro di Firenze ed elett. dom. in Firenze presso quest'ultimo

Fatto e diritto

1.1 Con ricorso depositato in data 26.4.2018 [REDACTED] ha chiesto la pronuncia di fallimento di [REDACTED] quale titolare dell'impresa individuale [REDACTED].

A sostegno della domanda il ricorrente ha esposto che [REDACTED], operando prima attraverso l'impresa individuale [REDACTED] e poi quale amministratore unico e socio di maggioranza di [REDACTED] società appositamente costituita a tale scopo – ha realizzato e gestito il software e sito internet ww [REDACTED].com; che [REDACTED].com è una piattaforma exchange on line che, tra i vari servizi offerti, permette l'acquisto, lo scambio e il deposito di diverse tipologie di

19

19

19



criptovalute, a fronte del pagamento di una commissione; che a partire dall'aprile 2017 era stato possibile ottenere, depositare e fare trading su tale piattaforma anche della criptovaluta Nano, il cui valore unitario alla data di deposito del ricorso era di circa USD 7,12 o € 5,85; che il ricorrente era tra gli utenti che, registrandosi su ██████████, aveva aperto un proprio conto – protetto da una password - su detto exchange, utilizzando la piattaforma per depositare criptovalute, scambiare tra loro criptovalute, in particolare con la possibilità di lasciare le somme così ottenute in deposito sul proprio conto su ██████████.com, scambiarle con altri membri operanti sulla piattaforma, oppure ritirarle, trasferendole così su conti personali o di terzi estranei alla piattaforma, i cui servizi erano offerti a pagamento; che il gestore della piattaforma manteneva il controllo dei singoli conti degli utenti, monitorando le attività e potendo arrivare a bloccare le transazioni, i depositi o i prelievi di criptovaluta, oltre che l'accesso al sito e al conto personale; che era stabilito dalle condizioni generali di ██████████ che in caso di blocco o chiusura del conto da parte del gestore l'utente avesse espressamente diritto alla restituzione delle criptovalute accreditate sul proprio conto, con conversione in Bitcoin e trasferimento all'indirizzo Bitcoin personale dell'utente al di fuori di ██████████.com; che nel mese di gennaio 2018 ██████████ aveva introdotto limiti via via più stringenti al prelievo delle criptovalute dalla piattaforma, e seguito di svariate problematiche riscontrate dagli utenti già dal settembre/ottobre 2017 e successivamente il 12.1.2018 aveva bloccato ogni trasferimento di criptovaluta dai conti su ██████████ a conti esterni, costituendo la società a responsabilità limitata ██████████ con il sig. ██████████; che dopo una temporanea ripresa dei prelievi (limitati per quantitativo massimo giornaliero), il 28 gennaio 2018 il gestore di ██████████ aveva definitivamente bloccato la possibilità per gli utenti di prelevare le proprie criptovalute; che il 9 febbraio 2018 il gestore di ██████████ (nel frattempo divenuto la società ██████████ srl) aveva pubblicato un comunicato in cui aveva dato atto della "sparizione" di 17 milioni di Nano – pari a circa 120 milioni di euro, appartenenti agli utenti dell'exchange e del blocco di tutti i servizi, affermando che l'ammancio di Nano coinvolgeva l'80% dei Nano appartenenti agli utenti, dichiarando di essere nell'impossibilità di restituire tutti i Nano sottratti, e proponendo un "piano di rientro"; che il 14 marzo 2018 BitGrail aveva reso visibili su conti di ciascun utente solo il 20% dei Nano dovuti, offrendo al posto dei Nano sottratti (e quindi al posto dell'80% delle somme iniziali degli utenti) uno "strumento finanziario" creato dalla ██████████, denominato "██████████".

Quanto alla propria posizione ██████████ ha esposto che il 9.2.2018 allorchè erano stati bloccati tutti i servizi di ██████████, egli aveva sul proprio conto 412 ██████████ Cash, pari a quella data a circa € 450.000, e 437.905 Nano, pari a quella data a circa 4,23 milioni di Euro, mentre al momento del ricorso risultavano solo 98.763 Nano, pari a circa 869.114 Euro con conversione dei Nano mancanti in ██████████ shares, senza il suo consenso.

Tanto premesso, deducendo la sussistenza di un gravissimo inadempimento nei confronti degli utenti della piattaforma e di una insanabile situazione di illiquidità dell'impresa individuale Webcoin al momento del trasferimento della piattaforma a ██████████ srl, con incapacità di entrambe



di far fronte ai propri obblighi restitutori – per una perdita dichiarata dallo stesso [redacted] esser pari a 17 milioni di Nano, ossia oltre 120 milioni di Euro – il ricorrente ha chiesto la dichiarazione di fallimento di Francesco [redacted], titolare di Webcoin, nonché – con separato ricorso - di [redacted] srl (già [redacted] srl), instando per la riunione dei due procedimenti.

1.2. Con separato ricorso del 10.5.2018 anche il Pubblico Ministero ha chiesto la pronuncia di fallimento di Francesco [redacted] – in virtù della legittimazione derivante dalla pendenza di procedimento penale aperto in relazione alla denuncia di “sparizione” di 17 milioni di Nano presentata dallo stesso [redacted] il 9.2.2018 - e ha chiesto l'adozione di provvedimento di sequestro ai sensi dell'art. 15 comma 8 L.F, essendo emerso nel corso delle investigazioni che “nei giorni tra il 2 e il 5 febbraio 2018, due giorni prima della comunicazione effettuata dalla Nano Foundation dell'avvenuto furto e 3 giorni prima della denuncia presentata...il [redacted] attraverso 9 operazioni sequenziali, ha depositato nel suo portafogli sulla piattaforma [redacted] un totale di 230 Bitcoin, criptomoneta che al cambio nel periodo di riferimento corrispondeva a circa 1.700.000 euro”, essendo emerso “che i versamenti dei Bitcoin, sul wallet del [redacted], provenivano da indirizzi riconducibili a quelli utilizzati dai clienti della [redacted] per effettuare i depositi sulla predetta piattaforma”. Il PM segnalava altresì il tentativo di Francesco Firano di ritirare presso sportelli ATM parte dei bitcoin depositati presso l'exchange italiano [redacted] srl.

1.3. Con decreto inaudita altera parte ex art. 15 comma 8 L.F. del 10.5.2018 (confermato il 25.5.2018 a seguito di radicamento del contraddittorio) il Tribunale emetteva decreto di sequestro delle disponibilità finanziarie e/o in moneta virtuale appartenenti a Francesco [redacted] ed in specie di quelle da quest'ultimo detenute attraverso [redacted] srl presso [redacted] e/o altri intermediari finanziari, fino al controvalore di € 120.000.000.

Per l'udienza fissata ex art. 15 LF si costituiva Francesco [redacted] ed esponeva che la piattaforma [redacted] che era stata ceduta alla BG solutions srl nel gennaio 2018, era una piattaforma exchange on line qualificabile come “un prestatore di servizi relativo all'utilizzo di valuta virtuale ai sensi dell'art. 1 del D.L. n. 231/2007 (come da ultimo modificato con il D.lgs.n. 90/2017); che il contratto stipulato tra l'exchanger e i suoi utenti è un contratto di servizi con il quale il professionista garantisce alcune prestazioni funzionali a consentire lo scambio, la compravendita e la conservazione, tramite account, di diverse tipologie di valute virtuali, fra le quali, la criptovaluta denominata “Nano” ; che non era riconosciuta all'exchanger alcuna facoltà di utilizzo delle somme depositate dagli utenti sui propri account; che era stata data agli utenti ampia informativa sui rischi legati alla volatilità della moneta virtuale e sui rischi anche di natura tecnica che possono interessare il loro corretto funzionamento, con una clausola di limitazione di responsabilità; che l'attività principale era ed è proprio la fornitura di servizi finalizzati allo scambio di valute virtuali, mentre le attività di deposito erano residuali e strumentali al solo fine di permetterne lo scambio; che difatti non vi era alcuna remunerazione collegata al deposito, ma unicamente una commissione sui prelievi e scambi di criptovalute; che gli utenti non potevano



cambiare euro o altre divise legali in criptovalute e viceversa; che la piattaforma, per sua natura rivolta ad utenti esperti, aveva avuto un notevole successo anche per l'opera svolta dagli sviluppatori della valuta Nano, che avevano promosso detta piattaforma, per la sua maggiore affidabilità rispetto all'alternativa esistente; che il valore della criptovaluta Nano al momento della sua introduzione nell'aprile del 2017 era di circa 0,01 \$, ed era salito vertiginosamente per arrivare a \$ 36 (dunque con un incremento di 3.600 volte del valore iniziale); che in ragione della conseguente aumentata importanza degli scambi il [REDACTED] aveva deciso di costituire una società di capitali per gestire la piattaforma; che nel febbraio del 2018 il [REDACTED] aveva preso contezza di una serie di ammanchi a seguito di alcuni prelievi indebiti effettuati da alcuni utenti, per circa 17 milioni di Nano, i quali avevano sfruttato, probabilmente, la vulnerabilità del software Nano sviluppato dal team che lo aveva ideato; che la [REDACTED] aveva presentato prontamente denuncia querela per l'ammancio, comunicandolo anche sul web, procedendo altresì nel tentativo di trovare una soluzione condivisa con gli utenti derubati; che al fine di agevolare una soluzione la [REDACTED] aveva annunciato che dal 2 maggio la piattaforma avrebbe ripreso la propria operatività; che aveva tuttavia sospeso la stessa appena appreso del sequestro della piattaforma disposta dal Tribunale su istanza del Pubblico Ministero.

Tanto premesso contestava che la [REDACTED] o il [REDACTED] potessero ritenersi responsabili del furto e/o ammanco, e che pertanto l'asserito controvalore non costituiva in alcun modo un debito della [REDACTED] e ancor meno del [REDACTED]; contestava l'esistenza dei presupposti per l'adozione del sequestro, sia in punto di periculum, perché il tentativo di prelievo di denaro era stato fatto senza alcun intento sottrattivo, e peraltro con movimentazione esclusivamente di somme proprie, sia in punto di fumus boni juris. Sotto tale ultimo profilo la difesa del [REDACTED] ha esposto che le criptovalute oggetto dei depositi non sono di proprietà del gestore della piattaforma, ma dei depositanti, e che pertanto si applicherebbe il principio *res perit domino*; che di conseguenza non vi sarebbe alcun debito del [REDACTED] nei confronti degli utenti della piattaforma, in specie considerata l'assenza nei Terms of Use di specifici obblighi di custodia in capo al gestore e, al contrario la previsione dell'assunzione dei rischi connessi all'utilizzo della piattaforma in capo agli utenti, che lascerebbe intendere che le conseguenze di eventi non direttamente riferibili alla condotta di [REDACTED] e connessi ai servizi, che essa si è limitata a garantire, non potrebbero che gravare sugli utilizzatori; che ove si volesse ricondurre la fattispecie al contratto di deposito, nella specie si sarebbe in presenza di un furto, suscettibile di integrare quell'evento imprevedibile e inevitabile non imputabile al depositario, che ne determina la liberazione dall'obbligo di restituzione, ai sensi dell'art. 1780 comma 1 c.c.; che comunque non sarebbe provato il diritto alla restituzione delle somme, o al risarcimento del danno per la mancata restituzione delle somme, dovendosi escludere qualsiasi riconoscimento di debito nell'offerta di soluzioni amichevoli effettuata dal [REDACTED] al precipuo fine di evitare possibili controversie legali, con danno reputazionale; che comunque l'ammancio sarebbe stato successivo al trasferimento della piattaforma alla [REDACTED] Services con conseguente esclusione di responsabilità del



Il [redacted] ha altresì contestato la sussistenza dei presupposti di fallibilità di cui all'art. 1 L.f. deducendo che Webcoin non risulta avere o avere avuto un attivo patrimoniale superiore a 300.000 euro o un volume di ricavi lordi superiore ad € 200.000, in specie considerato che le provvigioni incassate durante l'esercizio 2017 in criptovalute non risultavano convertite in euro, e non potendo ritenersi sussistenti debiti superiori ad € 500.000 per le medesime ragioni per cui ha contestato la sussistenza di responsabilità degli ammanchi di criptovaluta. In ogni caso, secondo la difesa del convenuto, in nessun modo detta responsabilità sarebbe ascrivibile al [redacted], ma, semmai, alla [redacted] essendo gli eventi riferiti ad un periodo successivo al subentro nella gestione della piattaforma. Peraltro si tratterebbe di crediti contestati, non portati da alcun titolo, e non assistiti da alcun previo accertamento, del tutto inidonei a supportare una pronuncia di fallimento. Ha inoltre dedotto che l'ammancio – derivato da furto – era stato reso possibile da una fallacità del sistema Nano, imputabile al Nano Team, mentre il [redacted] e la [redacted] avevano adottato le cautele opportune per quelli che erano gli aspetti di competenza della piattaforma da loro gestita.

1.4. Nel procedimento sono intervenuti [redacted], [redacted] e [redacted], aderendo alla richiesta di fallimento deducendo di essere creditori dell'exchange [redacted].com, precisando che [redacted] si era iscritto alla piattaforma il 25.12.2017 allorchè era gestita dall'impresa individuale Webcoin, con transazioni eseguite nel periodo 26-28 dicembre, con un deposito di 26.000,98 Nano per un controvalore di € 236.114; [redacted] di essersi iscritto alla piattaforma il 31.12.2017 eseguendo trading fino all'8 gennaio 2018, con un deposito di 7.964,49 Nano per un controvalore di € 72.317 e [redacted] di essersi iscritto il 28.12.2017 e che aveva in deposito 417,77 Nano, pari a circa 3.793 euro.

1.5 A seguito dell'esecuzione del sequestro, il custode, avv. Ariani, ha riferito che sono state sequestrate le seguenti disponibilità del [redacted]: sulla piattaforma di exchange gestita da [redacted] srl il saldo di 167.76776304 BTC, 514,691,08 EUR e 0,00080000BCG; presso CR Firenze 39.000 euro circa; presso BNL 10 euro; presso Banco di Lucca e Tirreno € 1.000; sul portale Poloniex.com 2 bitcoin, pari a circa 16.800 USD

1.6. Il procedimento è stato istruito con consulenza tecnica d'ufficio, e produzioni documentali, sulle quali le parti hanno svolto ampie deduzioni.

2. Deve essere dichiarato il fallimento [redacted] quale titolare dell'impresa individuale [redacted] ricorrendo i requisiti soggettivo ed oggettivo richiesti dagli artt. 1 e 5 della l.f., ed essendo pacificamente competente il Tribunale di Firenze, considerato che l'impresa ha sede in [redacted].

2.1. La natura di impresa commerciale del debitore emerge dal tipo di attività svolta di realizzazione di siti web, gestione software e hardware e servizi connessi a tecnologie informatiche.

2.2. Con riferimento al presupposto di cui all'art. 1 per la dichiarazione di fallimento, deve osservarsi che il Pubblico Ministero ha prodotto fin dal 12.6.2018 un prospetto redatto dalla Polizia

Postale e delle Telecomunicazioni della Toscana in data 11.6.2018, la quale, analizzando i dati della piattaforma [REDACTED] e accedendo alla scheda Profits, ha potuto visualizzare i profitti registrati dal 1.11.2017 al 30.1.2018. Da tale prospetto – cui sono allegate le stampe di visualizzazione delle relative pagine del sito – emerge che in detto periodo l'impresa individuale di Francesco [REDACTED] prima, fino all'11 gennaio 2018, e successivamente la [REDACTED] Services che le è subentrata, hanno maturato ricavi (profits) relativi agli scambi ("trading profit") per € 1.428.031,22; relativi ai prelievi (withdraws profit) per € 497.155,88, e per depositi per € 71.781,60 (si evidenzia fin da ora che questi sono specificamente riferiti alla criptovaluta Nano, identificata dal codice XRB), per un totale di profitti pari ad € 1.996.968,70.

Ne consegue che sono ravvisabili i presupposti di fallibilità con riferimento all'art. 1 L.F., tanto più che il Firano non ha prodotto, secondo il proprio onere, documentazione contabile da cui risulti l'esclusione dall'area di fallibilità di cui alla norma citata, che contrasti le risultanze dell'accertamento della Polizia Postale sopra riferito.

2.3.1. Al fine di affermare la sussistenza della condizione di procedibilità di cui all'art. 15 L.F. e di sussistenza dello stato di insolvenza è necessario analizzare in cosa sia consistita l'attività della [REDACTED] valutare se sia ravvisabile una responsabilità del gestore del sito per gli ammanchi di criptovaluta, con conseguente sussistenza di debiti.

2.3.2. Con riferimento in primo luogo alla moneta virtuale oggetto di scambio, prelievo e deposito attraverso la piattaforma [REDACTED] si osserva che la valuta virtuale trova una sua definizione nel d.lgs. 90/2017 che, in attuazione della direttiva UE n. 2015/849, modificando le definizioni dell'art. 1, comma 2, della legge anticiclaggio, con la lettera qq) definisce la valuta virtuale come *«la rappresentazione digitale di valore, non emessa 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 e trasferita, archiviata e negoziata elettronicamente»*.

Sulla base del medesimo decreto (lettera ff del medesimo art. 1 comma 2) sono definiti come prestatori di servizi relativi all'utilizzo di valuta virtuale *«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»*.

In un contenzioso (affidente questione tributaria di applicazione I.V.A. all'operazione di cambio di valuta contro criptovaluta e viceversa, ritenuta prestazione di servizio a titolo oneroso in presenza del pagamento della differenza tra il prezzo di acquisto delle valute e quello di vendita ricaricato dall'operatore ai propri clienti) relativo alla valuta virtuale denominata "bitcoin", la Corte di Giustizia UE (Quinta Sezione, sentenza 22 ottobre 2015, causa C-264/14) ne ha parimenti fornito una definizione spiegando che *«la valuta virtuale «bitcoin» è utilizzata principalmente per pagamenti tra privati via internet nonché in taluni negozi online che accettano detta valuta. Questa valuta virtuale non ha un unico emittente ma viene creata direttamente in una rete tramite uno*



speciale algoritmo. Il sistema della valuta virtuale «bitcoin» consente la detenzione e la cessione anonime di valori in «bitcoin» all'interno della rete da parte di utenti che hanno indirizzi «bitcoin». Un indirizzo «bitcoin» potrebbe essere comparato a un numero di conto corrente bancario", e, sulla base di una relazione del 2012 della Banca centrale europea sulle valute virtuali, " una valuta virtuale -può essere definita come un tipo di moneta digitale, non regolamentata, emessa e controllata dai suoi sviluppatori e utilizzata ed accettata tra i membri di una specifica comunità virtuale. La valuta virtuale «bitcoin» fa parte delle valute virtuali «a flusso bidirezionale», che gli utenti possono acquistare e vendere in base ai tassi di cambio. Tali valute virtuali sono simili ad ogni altra valuta convertibile per quanto riguarda il loro uso nel mondo reale. Esse consentono l'acquisto di beni e servizi sia reali che virtuali. Le valute virtuali sono diverse dalla moneta elettronica, come definita nella direttiva 2009/110/CE del Parlamento europeo e del Consiglio, del 16 settembre 2009, concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, che modifica le direttive 2005/60/CE e 2006/48/CE e che abroga la direttiva 2000/46/CE (GU L 267, pag. 7), in quanto, a differenza da tale moneta, nel caso delle valute virtuali i fondi non sono espressi nell'unità di calcolo tradizionale, ad esempio in euro, ma nell'unità di calcolo virtuale, ad esempio il «bitcoin»".

Sulla base delle definizioni normative e giurisprudenziali sopra richiamate risulta dunque che la criptovaluta è "una digitalizzazione di valore", che viene utilizzata come mezzo di scambio per acquistare beni o servizi, caratterizzandosi per non essere emessa da una banca centrale o altra pubblica autorità, e per non essere necessariamente collegata ad una valuta avente corso legale.

Dette valute virtuali, che sono trasferite, archiviate e negoziate elettronicamente proprio per la loro natura di digitalizzazione di valore, vengono acquistate attraverso delle apposite piattaforme, e possono attraverso le medesime piattaforme essere oggetto di scambio, oltre ad essere depositate in uno spazio di archiviazione. Esse, quali digitalizzazione di valore, si prestano ad essere oggetto di operazioni speculative: anzi, a ben vedere, essendo essenzialmente valori finanziari, si prestano particolarmente proprio ad operazioni speculative in ragione della estrema variabilità dei livelli di fluttuazione che le caratterizzano.

Poiché le criptovalute possono essere oggetto di diritti, vanno considerate quali "beni" ai sensi dell'art. 810 c.c..

2.3.3. Le criptovalute oggetto di acquisto, scambio e deposito su [REDACTED] erano molteplici, ed in particolare era oggetto di scambio sulla piattaforma la criptovaluta Nano rispetto alla quale si sono verificati gli ammanchi lamentati dal ricorrente e dagli intervenuti ed esposti dal Pubblico Ministero.

2.4.1 Francesco [REDACTED] ha articolato la propria difesa sostenendo che:

a) il rapporto fra la piattaforma e gli utenti è tale per cui il deposito assumerebbe una valenza meramente accessoria e strumentale rispetto all'attività di gestione della piattaforma, ed era del tutto gratuito;



b) se si intende parlare di deposito non vi sarebbero dubbi sul fatto che si tratterebbe di un deposito regolare, non sussistendo alcun elemento giuridico in forza del quale configurare un diverso rapporto;

c) il [REDACTED] prima e la [REDACTED] poi avrebbero adottato le cautele e le misure ritenute opportune sotto il profilo della sicurezza informatica;

d) a causa di vizi propri del software Nano, non riconducibili alla piattaforma (tanto che nessun'altra criptovaluta è stata oggetto di attacchi e di furti), si sono dovuti constatare alcuni indebiti prelievi di Nano, in numero contenuto e artificiosamente mascherati, da parte di alcuni utenti, che sono riusciti, in sintesi, a duplicare l'entità dei prelievi così da creare l'ammanco complessivo di circa 15,5 milioni di Nano di proprietà degli utenti;

e) non sarebbe dato di conoscere con esattezza la data degli ammanchi di cui il [REDACTED] si sarebbe reso conto solo l'8.2.2018 procedendo immediatamente alla denuncia;

f) gli ammanchi sarebbero dipesi da falle nel software Nano.

2.4.2 La ricostruzione del [REDACTED] è contestata dal ricorrente, dagli intervenuti e dal Pubblico Ministero sostenendo che nella specie il rapporto tra gli utenti e il gestore della piattaforma dovrebbe qualificarsi quale deposito irregolare, con conseguente sussistenza dell'obbligo di restituzione del *tantundem eiusdem generis* ai sensi dell'art. 1782 c.c..

Comunque, ove anche si facesse applicazione delle norme sul deposito regolare, sussisterebbe responsabilità risarcitoria del gestore in conseguenza della mancata adozione di tutte le misure necessarie a garantire la sicurezza del deposito, in specie considerato che non sarebbe stato rispettato l'onere di immediata denuncia del fatto generatore dell'ammanco, rilevante ai sensi dell'art. 1780 primo comma c.c.

2.5.1 Per disporre di tutti gli elementi necessari al fine di valutare la responsabilità della Webcoin è stata disposta una CTU affinché il consulente descrivesse "il funzionamento della piattaforma exchange online gestita da [REDACTED] Services s.r.l., con particolare riferimento:

- alle modalità di svolgimento del rapporto tra piattaforma e utente sin dal momento della registrazione di quest'ultimo su [REDACTED].com e i servizi offerti dalla piattaforma;

- alla conservazione e alla collocazione delle criptovalute all'interno della piattaforma;

- ai poteri di supervisione e controllo sulle transazioni e sulle movimentazioni delle criptovalute da parte del gestore della piattaforma e agli eventuali ulteriori poteri del gestore.

Al CTU è stato altresì chiesto di riferire "sulle circostanze dell'ammanco di Nano denunciato da [REDACTED] Francesco nel febbraio 2018, anche sull'effettiva datazione dello stesso" individuandone le cause, e di accertare "se fossero state adottate tutte le misure di sicurezza dalla piattaforma e nel caso di risposta positiva descrivendo le stesse e fornendo ogni elemento utile per la valutazione di adeguatezza della misura in considerazione della natura e dell'attività e delle caratteristiche della criptovaluta".



2.5.2. Preliminarmente deve darsi atto che la consulenza si è svolta nel pieno contraddittorio tra le parti – tanto che al CTU è stata concessa una proroga dopo che il consulente del [REDACTED] ha chiesto di poter discutere in un nuovo incontro degli elementi emersi dopo l'ultimo incontro peritale e dopo la consegna della bozza del CTU e delle risposte dei CTP. In seguito il CTU ha sottoposto ai CTP una nuova bozza e le parti hanno fatto pervenire le proprie osservazioni, e il consulente ha predisposto la stesura finale della relazione, tenendo conto di tutte le osservazioni – con ampie ed articolate argomentazioni, fondate sulla descrizione analitica delle indagini svolte nel pieno contraddittorio, immuni da vizi logici.

Il Tribunale ritiene del tutto infondata l'eccezione di nullità della perizia avanzata dalla difesa del [REDACTED] sostenendo che il CTU avrebbe dovuto, a mente dell'art. 195 c.p.c., limitarsi a depositare la bozza, allegando le osservazioni e una sintetica valutazione.

Osserva al riguardo il Collegio che a fronte del consistente numero di osservazioni avanzate dai CTP e della loro complessità – ciò che nitidamente emerge dall'esame delle relazioni dei CTP allegate dal CTU – la scelta effettuata dal consulente di una ristesura finale dell'elaborato peritale in modo che risultassero in essa integrate le osservazioni dei consulenti, al contempo fornendo risposta alle osservazioni medesime – è scelta da apprezzare e condividere atteso che è stata efficacemente adottata al fine di rendere alle parti e al Tribunale una relazione organica, completa e dotata dell'imprescindibile chiarezza espositiva, nulla togliendo al contraddittorio.

2.5.3. Devono essere quindi respinte le richieste di chiarimenti ed integrazione della CTU formulate a verbale di udienza in data 11.12.2018 dalla difesa del convenuto, considerato che le contestazioni che le supportano non intaccano l'impianto ricostruttivo della consulenza, che ha ampiamente tenuto conto delle difese del convenuto.

2.6.1 Nel merito dell'esito degli accertamenti peritali, si osserva che il CTU, rispondendo alla prima parte del quesito, ha riferito che [REDACTED] forniva *"un servizio di deposito e trading di 10 diverse criptomonete...tramite un portafoglio che l'utente poteva aprire e mantenere attivo gratuitamente, senza commissioni per l'exchange esclusi i costi di prelievo (che non rappresentavano necessariamente un guadagno per l'exchange ma consistevano in un rimborso forfait delle transaction fee da esso sostenute) e quelli di trading (per il quale l'exchange incassava invece una percentuale di 0.020% sul transato). Il deposito serviva esclusivamente per poter permettere agli utenti di avere la liquidità necessaria sull'Exchange per effettuare le operazioni di cambio, non si trattava quindi di un vero e proprio wallet. Non esistevano quindi costi di deposito, fatto salvo per un breve periodo all'inizio della piattaforma durante il quale erano stati attivati dei costi irrisori di deposito (poi quasi subito rimossi) per evitare il problema delle transazioni "SPAM". Per la moneta Nano, non erano presenti costi di prelievo" nonché un "servizio di "trading", mediante il quale gli utenti potevano vendere le criptomonete attestate sul loro wallet per acquistarne altre"*



2.6.2. Quanto alle modalità di svolgimento del rapporto tra piattaforma ed utente il rapporto iniziava con la registrazione, durante la quale l'utente indicava alcuni suoi dati e otteneva l'accesso alla sua area riservata, che doveva essere ulteriormente vincolato da autenticazione a due fattori (con conferma codice PIN ricevuto via email) per avere accesso alle funzioni di trading.

Il Consulente ha segnalato che per quanto dichiarato dal sig. [REDACTED] durante le operazioni di CTU, la piattaforma non eseguiva alcun genere di controllo approfondito in merito all'identità del registrante, né teneva alcuna traccia degli indirizzi IP utilizzati per la registrazione o per i successivi accessi od operazioni, con la conseguenza che in caso di attività illecita (come il furto di criptomoneta) non poteva essere fornito alcun supporto utile a identificare i potenziali autori.

Quindi l'utente "ricaricava" il proprio wallet (assegnatogli con la registrazione) con la criptomoneta di sua preferenza – trasferendola autonomamente a partire da un proprio portafoglio – potendo successivamente impiegarla all'interno dell'exchange per comprarne altra, di tipo diverso, ritirando poi quanto acquistato (o quanto depositato) tramite la funzione "withdraw".

Una volta versati i fondi, in criptomonete sul wallet *"gli utenti potevano gestirli autonomamente ma sempre tramite i servizi forniti e abilitati dall'Exchange, che era preposto a gestire gli spostamenti di criptomonete (quindi trasferimenti tra "monete virtuali" di tipo diverso ma sempre all'interno dell'exchange, che possiamo immaginare come bonifici intra banca) allo stesso modo dei prelievi (trasferimenti di criptomonete dall'exchange verso indirizzi esterni, in gestione diretta da parte dell'utente e quindi di sua proprietà, che possiamo immaginare come bonifici SEPA verso banche esterne o prelievi di contante)"*.

Il CTU ha precisato che *"I fondi trasferiti dagli utenti sull'indirizzo loro assegnato non vi rimanevano, venivano invece spostati per le criptomonete principali (Bitcoin, Ethereum, Nano, etc...) verso un indirizzo principale di [REDACTED] con uno script che ogni notte raccoglieva i fondi dai singoli indirizzi per trasferirli verso di esso"*. Tale modalità, secondo il CTP di parte [REDACTED] era necessaria per consentire i prelievi in sicurezza a partire dall'ammontare di criptovaluta effettivamente depositato da ogni utente sul proprio indirizzo assegnato da [REDACTED]¹.

2.6.3. Rispondendo all'ulteriore quesito sottopostogli il CTU ha accertato che *"le criptomonete venivano conservate in "hot wallet" (cioè portafogli configurati sui server di produzione, cioè quelli connessi a Internet e su cui erano attivi gli utenti e il portafoglio dell'exchange) dove queste rimanevano a disposizione dell'exchange che ne gestiva i prelievi o le compravendite tra criptomonete diverse.*

Questi portafogli erano controllati esclusivamente tramite il codice dell'exchange oppure da coloro che detenevano le chiavi private dei wallet, quindi da Francesco [REDACTED] e il socio Andrea

¹ "tale funzionalità era necessaria per consentire i prelievi: se un utente X deposita 10 NANO sul proprio indirizzo assegnato da BitGemil, e poi, tramite trading, riesce ad ottenere un balance di 100 NANO, è chiaro che non sarà possibile per l'exchange consentire il prelievo di 100 NANO dall'indirizzo dove in deposito ci sono unicamente 10 NANO, per questo motivo, quindi, era importante accentrare i fondi."



██████, che avevano accesso al sistema anche via SSH (un sistema di controllo remoto utilizzato per gestire sistemi).”

Il CTU ha quindi precisato – e ciò è ovvia conseguenza di quanto sopra riportato – che “Gli utenti non avevano la possibilità di gestire autonomamente i loro fondi senza fare uso delle funzionalità della piattaforma ██████, in primo luogo perché gli indirizzi di deposito loro assegnati venivano in breve tempo svuotati per far convogliare le criptomonete verso gli indirizzi principali dell’exchange, in secondo luogo perché gli utenti non disponevano di alcuna chiave privata. Senza autenticarsi sulla piattaforma ██████ che doveva essere attiva e funzionante, era quindi impossibile per gli utenti eseguire attività di trading ma anche semplicemente ritirare i propri fondi, così come – per fare un esempio pratico – per un correntista è impossibile ritirare i fondi depositati presso la propria banca se gli sportelli sono chiusi, il portale web è inattivo e i servizi di credito/debito tramite carte non sono funzionanti”.

Di conseguenza, poiché i fondi di tutti gli utenti erano gestiti centralizzandoli su di un unico conto, il CTU ha affermato, con conclusione inconfutabile ed inconfutata, che “l’unico modo per attribuire a un utente il suo capitale è quello di valutare i dati contenuti sul database, non essendo i wallet “fisicamente” distinti. Non è però possibile, in caso di ammanco, capire di quale utente fossero i fondi scomparsi, dato che i fondi di tutti gli utenti venivano raccolti su di un unico conto”.

Il CTU ha precisato nelle conclusioni che “Non risulta che...sia mai stato disposto movimento di fondi all’esterno dell’exchange dal gestore, a parte il 12 dicembre 2017, data in cui sono stati trasferiti parte dei fondi dall’indirizzo representative ██████ al ██████, in corrispondenza del cambio d’infrastruttura verso la nuova piattaforma: in tale data, 13 milioni di XRB sono stati spostati “a mano”, senza utilizzare le funzioni dell’exchange, che non hanno quindi tracciato il movimento nel database.

Da tale data, l’indirizzo ██████ 1 è diventato un “cold wallet”, al fine di mantenervi alcuni milioni di Nano da escludere dall’operatività dell’Exchange che invece continuava a operare utilizzando come “hot wallet” l’account ██████ 2. Il fine di questa operazione è mantenere “al sicuro” e offline, fuori dalla rete, un conto (██████ 1) e utilizzare invece per l’operatività quotidiana il secondo conto (██████ 2) così come previsto dalle best practices.”

2.7. Alla luce di quanto accertato dal CTU e sopra riportato ritiene il Collegio che emergano chiari elementi per ritenere che le criptovalute, ed in specie quelle denominate Nano – per quanto concerne gli ammanchi oggetto dell’odierna analisi – sono beni fungibili, trattandosi di rappresentazioni digitali espresse in unità portatrici di un medesimo valore, che venivano fatte confluire dal gestore della piattaforma verso un indirizzo principale di ██████ ove erano archiviate quali masse di criptovalute omogenee. Al riguardo risulta priva di pregio l’asserzione per cui i Nano non sarebbero “denaro” né tanto meno “cose fungibili”, avendo una loro precisa identità anche distinta da quella di ogni altra criptovaluta: se ciò fosse vero, anche il denaro non sarebbe un bene fungibile (il ché certamente va escluso, salvi i casi di collezionismo numismatico) considerato che i



dollari sono diversi dagli euro e dalle sterline e ogni banconota reca un numero di serie. E, a ben vedere anche la banconota non è che una "nota di banca", ossia, essenzialmente, una informazione.

Va quindi osservato che anche il rapporto tra utenti ed exchange per la criptovaluta Nano era un rapporto misto di deposito e trading, non potendoci essere commercio in difetto del correlato deposito per tutte le caratteristiche di funzionamento del commercio di criptovaluta e della piattaforma descritte analiticamente dal CTU.

Proprio in ragione della loro fungibilità, una volta che le criptovalute degli utenti erano convogliate sull'indirizzo principale di ██████████, le valute (ovviamente divise per specie) non recavano elementi distintivi circa la loro appartenenza ai singoli utenti, dando così luogo ad un deposito irregolare, cui consegue lo specifico obbligo per il depositario di mantenere sempre a disposizione dei depositanti la quantità integrale, con un coefficiente di cassa del 100%.

Si osservi che lo spostamento in un unico indirizzo dell'exchange assolve per le criptomonete alla medesima funzione economica di ogni deposito irregolare, ossia alla maggiore efficienza nel custodire insieme i beni di diversi depositari, per i quali è irrilevante l'identità della singola criptomoneta, purchè sia sempre a loro disposizione la quantità, *rectius* il valore, di loro titolarità.

Con la conseguenza, propria di ogni deposito irregolare di beni fungibili, che, quando non siano stati individuati al momento della consegna – come è avvenuto esattamente nella specie, ove si consideri quanto riferito dal CTU sul fatto che *"l'unico modo per attribuire a un utente il suo capitale è quello di valutare i dati contenuti sul database, non essendo i wallet "fisicamente" distinti. Non è però possibile, in caso di ammanco, capire di quale utente fossero i fondi scomparsi, dato che i fondi di tutti gli utenti venivano raccolti su di un unico conto"* - entrano nella disponibilità del depositario che acquista il diritto di servirsene e, pertanto, ne diventa proprietario ("La facoltà di servirsi del danaro depositato costituisce un elemento naturale della fattispecie di cui all'art. 1782 c.c.": Cass. 12552/2000), pur essendo tenuto a restituirne altrettanti della stessa specie e qualità, salvo che sia stata apposta un'apposita clausola derogatoria, (Cass. 20 aprile 2001, N. 5843; 23.8.2011 N. 17512; 22.3.2013, N. 7262), clausola derogatoria assente nel caso di specie.

Tale conclusione trova conferma nella circostanza di fatto per cui il ██████████ ha potuto trasferire tutte le criptovalute manualmente verso una nuova piattaforma: significativa al riguardo è la circostanza accertata dalla Polizia Postale e posta dal P. M. a fondamento dell'istanza di sequestro per cui *"nei giorni tra il 2 e il 5 febbraio 2018, due giorni prima della comunicazione effettuata dalla Nano ██████████ dell'avvenuto furto e 3 giorni prima della denuncia presentata...il ██████████ attraverso 9 operazioni sequenziali, ha depositato nel suo portafogli sulla piattaforma ██████████ un totale di 230 Bitcoin, criptomoneta che al cambio nel periodo di riferimento corrispondeva a circa 1.700.000 euro"*, essendo emerso *"che i versamenti dei Bitcoin, sul wallet del ██████████, provenivano da indirizzi riconducibili a quelli utilizzati dai clienti della ██████████ per effettuare i depositi sulla predetta piattaforma"*.



2.8. Quanto ai poteri di supervisione e controllo sulle transazioni e sulle movimentazioni delle criptovalute da parte del gestore della piattaforma e agli eventuali ulteriori poteri del gestore, il CTU ha accertato che il gestore dell'exchange aveva conoscenza delle chiavi private con le quali potevano essere spesi i fondi attestati sui vari wallet, e che le chiavi venivano impiegate tramite i "nodi" che gestivano le varie criptomonete per attivare i vari prelievi che gli utenti man mano richiedevano oppure per convogliare i fondi che gli utenti man mano versavano sui loro indirizzi dedicati.

Il CTU ha evidenziato che *"L'unico caso in cui le criptomonete sono risultate essere utilizzate direttamente da [redacted], fuori dall'exchange, è stato in data 12 dicembre 2017, quando circa 13 milioni di Nano sono stati spostati dall'indirizzo utilizzato fino ad allora a quello nuovo, creato contestualmente alla revisione del codice"*.

Il CTU ha riferito che l'exchange riceveva ordini di trading o di prelievo da parte degli utenti e, tramite il codice con cui era sviluppato, provvedeva a informare il nodo che gestiva ogni rispettiva criptomoneta circa le transazioni che dovevano essere eseguite, indicando ad esempio per i prelievi la cifra da trasferire e l'indirizzo di destinazione.

Il CTU ha spiegato che il *"nodo è un software Nano installato dal sig. [redacted] su un computer (o macchina virtuale) collegato all'exchange [redacted]. Il nodo conteneva le funzioni di creazioni account, blocchi, transazioni, firma, etc... in sostanza il nodo è un wallet Nano in tutto e per tutto autosufficiente, ma da solo non può fare nulla senza ricevere comandi dall'esterno, attraverso un canale chiamato "RPC" che viene utilizzato per impartire ordini di trasferimenti, creazione indirizzi o qualunque altro dei comandi disponibili ed elencati all'indirizzo <https://github.com/nanocurrency/raiblocks/wiki/RPC-protocol>"*

Secondo la ricostruzione offerta dal consulente *"Il sig. [redacted], ovvero [redacted] era l'unico responsabile della sua manutenzione. Sempre il sig. [redacted] era la persona che aveva proceduto alla sua installazione e che si occupava della sua manutenzione e aggiornamento ogni qualvolta il team Nano rilasciava degli aggiornamenti del software per migliorare la stabilità, sicurezza o aggiungere nuove funzionalità. Lo stesso era inoltre l'unico responsabile delle comunicazioni da/verso il nodo, in particolare dell'invio di comandi, della corretta interpretazione delle risposte ricevute a fronte di richieste, della gestione di eventuali errori, poiché la comunicazione tra exchange BitGrail e nodo era protetta e riservata"*.

Il nodo, dunque, *"risiedeva direttamente nell'ambiente [redacted]"*.

Secondo la ricostruzione del CTU, ogni volta che il nodo riceveva una richiesta di eseguire una transazione da BitGrail, ne generava il codice, lo firmava con le chiavi private e segrete in esso memorizzate e la trasmetteva verso gli altri nodi della rete Nano, propagando così pubblicamente la transazione e "attivando" quindi la transazione così come un bonifico viene "attivato" nel momento in cui viene comunicato, come minimo, al destinatario dei fondi. Nel mondo della blockchain distribuita, il "bonifico" viene comunicato a tutti i nodi che, chi prima chi dopo, lo segnano nella



loro blockchain locale e propagano ulteriormente la notizia del trasferimento così che tutti i nodi vengano raggiunti e aggiornati.

L'exchange – così come il suo gestore – aveva visibilità solamente sulle transazioni che il software dell'exchange [REDACTED] aveva lanciato e delle quali il sistema aveva ricevuto notifica dai nodi che gestivano le criptomonete.

Non erano stati implementati sistemi di controllo e supervisione dei wallet a livello di blockchain, verificando ad esempio sul nodo (previa verifica dell'avvenuta sincronizzazione e aggiornamento con le transazioni in corso) se le transazioni emesse erano state effettivamente inoltrate sulla rete ma, soprattutto, se esistevano transazioni di uscita dal conto ("account", nel protocollo Nano) di cui l'exchange non era a conoscenza, cosa che risulta essere proprio la circostanza dell'ammanco di Nano.

2.9.1 Quanto all'ammanco denunciato da [REDACTED] nel febbraio del 2018, va in primo luogo evidenziato che, ben diversamente da quanto sostenuto dal convenuto nelle proprie difese, lungi dall'essersi verificato nell'immediatezza della denuncia, esso è databile tra maggio 2017 e dicembre 2017, con alcune fuoriuscite anche a gennaio 2018, dal nuovo indirizzo [REDACTED] 2, la cui migrazione è avvenuta dal dicembre 2017 a fine anno. Il Tribunale osserva che la datazione è stata ricostruita affidabilmente dal CTU - con motivazione ampia e congrua - dando atto di aver utilizzato il metodo della ricerca della transazione precedente sul database [REDACTED], transazione certamente datata – se presente – come tutte quelle contabilizzate nel logfile dell'exchange. Il metodo della transazione precedente è stato poi raffinato con verifiche sui backup della blockchain eseguiti dal team di sviluppo Nano e da verifiche su transazioni con stesso destinatario e stessa cifra occorse in periodi prossimi.

2.9.2 Va evidenziato – trattandosi di questione di sicuro rilievo – che non solo l'ammanco risale temporalmente a molti mesi prima della denuncia, e che il [REDACTED] si era accorto della presenza di ammanchi significativi, quali sono stati quelli del luglio 2017 al momento del loro verificarsi.

Ciò risulta chiaramente dai messaggi della chat Telegram attiva con il team di sviluppo Nano (all'interno della quale [REDACTED] era entrato a dicembre 2016 per uscirne a dicembre 2017) dei quali il Tribunale può tenere conto, considerato che si tratta di documenti già prodotti in atti dalla Procura, rispetto ai quali il CTU, onde rendere il dato utilizzato oggettivo e condiviso, ha provveduto – nell'ambito dei poteri istruttori conferitigli dal Tribunale, nel rispetto dell'art. 15 comma 4 L.F. – a richiedere copia originale della chat ai partecipanti, ottenendo copia ricavata direttamente da esportazione Telegram, che ha allegato.

2.10. Procedendo ad analizzare le modalità dell'ammanco, nel corso delle operazioni peritali è stato accertato pacificamente tra le parti che esso è avvenuto durante il normale utilizzo e ciclo di vita dell'exchange, da parte di normali utenti, inserendo la propria mail e i propri dati, utilizzando il proprio wallet - senza furto di chiavi, forzature di sistemi, né sconfitta della sicurezza



perimetrale, installazione di trojan/backdoor, o vulnerabilità nel protocollo matematico delle criptomonete.

In particolare il CTU ha verificato che esso *“è stato causato da prelievi multipli (detti anche “double withdraws”) che si verificano in circostanze non provate chiaramente. Secondo la dichiarazione del Sig. ██████, infatti, tali prelievi occorrevano in occasioni di malfunzionamento del nodo (egli fa riferimento a possibili “crash” del nodo) tuttavia a oggi non abbiamo certezza della dinamica di tali malfunzionamenti. Potevano esserci altre modalità durante le quali occorrevano tali prelievi multipli o anche situazioni nelle quali il nodo si comportava diversamente da come doveva, magari per sovraccarico: l’assenza del codice sorgente della piattaforma ██████ dell’epoca impedisce di poter simulare l’accaduto. Sicuramente, l’analisi delle transazioni aventi lo stesso TXID presenti in modo massivo a luglio 2017 nella tabella “withdraws” indica come i doppi prelievi erano quasi sempre legati a tentativi multipli di prelievo molto ravvicinato e della stessa cifra, così come tra l’altro rilevato da ██████ già a luglio 2017, così come riportato nella chat Telegram attiva con il team di sviluppo Nano all’interno della quale ██████ era entrato a dicembre 2016 per uscirne a dicembre 2017”.*

Il consulente ha chiarito che con il termine “prelievi multipli” – per come si è verificato nel caso in esame – ci si riferisce a due o più prelievi di pari importo eseguiti da un medesimo conto intestato a ██████. Il CTU ha spiegato che nel caso in esame le richieste di prelievo da parte degli utenti BitGrail comportavano un “bonifico” dal conto unico generale ██████ al conto indicato dall’utente. Egli ha accertato che *“il protocollo Nano prevede sin dalla sua origine la possibilità di evitare prelievi multipli generando la richiesta di prelievo per chi gestisce un unico conto per più soggetti: come emerso nel corso della CTU per far ciò occorre costruire la transazione e tra i parametri da impostare vi è il bilancio del conto e l’hash dell’ultima transazione. Procedendo in tale maniera, anche se arrivassero due richieste di prelievo identiche, solo la prima avrebbe effetto: cioè la transazione sarebbe idempotente”². La ragione per la quale la rete Nano ha potuto eseguire le transazioni ██████ richieste in modo multiplo (ossia quelle non autorizzate oltre la prima, effettivamente autorizzata) deriva dunque dal fatto che ██████ conservava tutta la criptovaluta Nano in un unico portafoglio con un saldo sufficiente a soddisfare qualsiasi richiesta di prelievo. Inoltre, cosa più importante, l’hash (cioè la firma, una sorta di “Codice CRO” come nei bonifici) di ognuna delle singole transazioni componenti le transazioni multiple era diverso, nonostante ██████ richiedesse al nodo un prelievo più volte “convinto” che si trattasse sempre dello stesso prelievo. E in effetti agli occhi del nodo le transazioni sono state elaborate come transazioni*

² Idempotenza” è la proprietà di eseguire una volta sola un comando anche se impartito più volte, anche se identico e in rapida successione. Per fare un esempio “banale” ma chiarificatore: durante il prelievo di contante con il bancomat, anche tentando di premere più volte il pulsante di prelievo, la funzione “idempotente” fa sì che il dispositivo emetta una e una sola disposizione di prelievo, fornendo il contante richiesto una volta sola e tracciando il prelievo una volta sola nell’estratto conto del cliente.

diverse, mentre per ██████ le transazioni di prelievo effettivamente uscite erano singole, con un unico valore hash e un'unica "entry" nel database "withdraws", che teneva traccia appunto di ogni singola richiesta di prelievo "ufficiale", andata poi a buon fine o meno. Dunque ... il prelievo multiplo è da intendersi come una forma abbreviata di "multiple richieste di prelievo da parte di BitGrail" e non di uscite multiple da parte del nodo, che per ogni richiesta faceva uscire i fondi una volta sola, quindi non è la rete Nano che disponeva uscite in maniera multipla ma l'exchange BitGrail che richiedeva più volte al nodo di fare uscire dei fondi che, in realtà, erano già usciti alla prima richiesta".

L'ammanco denunciato da ██████ a febbraio 2018 è stato, quindi, causato da una richiesta di invio generata più volte da ██████ a fronte di una unica richiesta da parte dell'utente. Al nodo Nano tali richieste sono pervenute come richieste differenti tra loro, altrimenti, se fossero state idempotenti come descritto nel corpo della relazione, il nodo Nano le avrebbe scartate evitando il problema che si è verificato.

Il CTU ha precisato che "Pur non avendo avuto modo di riscontrare in dettaglio la circostanza nel codice sorgente di ██████ poiché indisponibile, sulla base della descrizione fornita da ██████ è emerso che a seguito di una prima richiesta di prelievo ██████ cercava traccia dell'esecuzione all'interno del servizio esterno di block explorer Raiblocks. Occorre precisare che lo strumento Raiblocks non nasce per l'uso fatto da ██████ pertanto ogni controllo fatto su di esso non poteva essere considerato affidabile. Per ovvi motivi il nodo poteva inoltre essere disallineato al momento della verifica. In tali casi ██████ inviava una nuova richiesta che di fatto si presentava diversa dalla precedente. Talvolta queste richieste venivano quindi eseguite più volte generando il prelievo multiplo.

In ogni caso, qualsiasi fosse la causa scatenante, è chiaro che ogni prelievo multiplo è nato come richiesta multipla da parte di ██████. Il nodo Nano ha eseguito le richieste pervenute da ██████, non avendo visione sulla reale contabilità dell'exchange".

Gli ammanchi si sono verificati perché gli utenti che si sono appropriati dei Nano avevano scoperto che, richiedendo un prelievo in determinati momenti, vi erano buone probabilità di ottenere due prelievi identici, di cui uno contabilizzato ed "ufficiale" ed uno ulteriore che veniva effettuato una seconda volta, ma non veniva contabilizzato dall'exchange mentre era regolarmente iscritto all'interno della blockchain nel nodo Nano affiancato all'exchange: di conseguenza vi è stata una fuoriuscita di criptovaluta Nano dalla piattaforma senza che le transazioni venissero registrate nel database dell'exchange.

Il CTU ha descritto dettagliatamente le misure che avrebbero potuto essere adottate dal gestore di ██████ evidenziando che "Indipendentemente dal motivo per il quale le transazioni non risultavano immediatamente disponibili sul nodo, ██████ verificava il buon esito del comando di trasferimento (generato a seguito di richiesta di prelievo di un utente) cercando i riferimenti all'interno del block explorer RaiBlocks che però non era attendibile e, per stessa definizione del



protocollo, essendo sostanzialmente un altro nodo nella rete, poteva ovviamente essere non sincronizzato come lo era [REDACTED] il che avrebbe dovuto renderlo non idoneo per alcun genere di controllo di esecuzione delle transazioni” e che “laddove il prelievo multiplo fosse stato effettivamente causato da malfunzionamenti del nodo (che si ricorda essere solo un mero esecutore di comandi di richiesta di trasferimento non idempotenti pervenuti da [REDACTED]), ... [REDACTED] avrebbe dovuto interrompere le operazioni, verificare la contabilità e l’effettiva esecuzione delle richieste pendenti prima di dar seguito a nuove disposizioni”

Con riferimento alle osservazioni del CTP del convenuto, Epifani, sull’impossibilità di generare e firmare transazioni fuori dal nodo prima del 16 dicembre 2017, il CTU ha rilevato che “in realtà la funzione segnalata da Epifani permette d’inviare al nodo un comando di creazione di un blocco anche quando il nodo non possiede le chiavi private. Risulta invece sempre stato possibile eseguire firme fuori dal nodo (cosa di cui già dal 2014 si discute anche in ambito di altre criptomonete) con procedure note già da giugno 2017 e pubblicate su diversi manuali online da parte della comunità Nano.

Dai vari scritti, emerge come l’utilizzo del nodo come “centro contabile” era previsto – come in generale avviene anche per le altre criptomonete – solamente per gli utenti singoli, con il loro wallet privato, senza attività intense o concorrenti. Gli exchange sono sempre stati invitati a gestire in modo autonomo le transazioni, proprio perché conferire tutta la fiducia al nodo implica un alto rischio, non soltanto per le eventuali doppie transazioni.” Si tratta dunque di un rischio che, ad avviso del Tribunale, avrebbe dovuto essere gestito dal gestore della piattaforma, che avrebbe potuto e dovuto limitarlo, nel momento in cui offriva i propri servizi.

E, ben vero che il 16 febbraio 2018 è stata apportata da parte degli sviluppatori Nano una modifica alla funzione Send in modo da renderla idempotente, tuttavia secondo il CTU “questo non significa che prima di queste modifiche non fosse possibile generare e firmare blocchi offline o garantire idempotenza, erano ovviamente operazioni da fare fuori dal nodo, scrivendo opportuno codice nella piattaforma Bitgrail”.

Il [REDACTED], che era consapevole della necessità – per questioni di sicurezza – di firmare fuori dal nodo, tanto che per i Bitcoin ha confermato al CTU che procedeva esattamente in tale maniera, generando e firmando le transazioni di prelievo in Bitcoin fuori dal nodo “Non aveva invece ritenuto di poterlo fare per i prelievi di Nano perché il nodo non forniva gli strumenti per farlo in modo agevole” mentre “tale evenienza si poteva controllare in modo agevole (ad esempio non firmando transazioni in ingresso se non in modo coordinato con i prelievi) e in ogni caso la difficoltà maggiore dello sviluppo del codice per la firma fuori dal nodo avrebbe garantito la completa gestione delle transazioni che invece, demandate al nodo, si è visto poter andare completamente fuori controllo”.

Si trattava certamente di soluzione che avrebbe implicato complicazioni e maggiori spese nello sviluppo e nella gestione: ma, ad avviso del Tribunale, il [REDACTED] avrebbe dovuto adottarle, per



adempiere con diligenza alle proprie obbligazioni, considerata la necessità di garantire la sicurezza di transazioni, effettuate tramite un deposito, con il pagamento di commissioni rilevanti, come quantificate sopra, sia pure parametrata principalmente all'operazione di *trading*, cui era collegato funzionalmente il deposito. Si osserva che benchè per il deposito non fosse di regola previsto un apposito compenso, se non per un certo periodo, tuttavia atteso il collegamento funzionale tra deposito e trading non può fondatamente sostenersi che il deposito fosse effettivamente "gratuito", così come in un volo aereo in cui sia incluso un pasto, esso, lungi dall'essere gratuitamente offerto, è semplicemente stato calcolato tra i costi della compagnia ricompresi nel prezzo complessivo.

Va dunque ravvisata una responsabilità del ██████ – quand'anche si ritenesse di versare in una ipotesi di deposito regolare (ciò che invero il Tribunale esclude, come sopra argomentato al punto 2.7) - per non aver adottato misure idonee ad evitare la perdita dei beni, tanto più ove si consideri quanto ricostruito circa la datazione degli ammanchi e la consapevolezza acquisitane dal ██████ fin dal luglio 2017, e ancora più il 12.12.2017, allorchè ha migrato "a mano" con 9 transazioni la cifra di circa 13 milioni di Nano dall'indirizzo ██████ all'indirizzo ██████2.

2.11. Tanto premesso deve osservarsi che in sede di CTU è stato verificato che tramite il predetto meccanismo del prelievo multiplo sono stati sottratti a luglio 2017 circa 2.5 milioni di Nano, mentre circa 7,5 milioni di Nano sono fuoriusciti ad ottobre 2017.

Per quanto rileva in questa sede, quand'anche il ██████ non avesse avuto modo di avvedersi degli ammanchi (non rilevanti, per quanto ricostruito) anteriori al luglio 2017- ciò che secondo il CTU è possibile - valutando quindi le misure necessarie ad evitare il loro ripetersi, tuttavia dopo tale data è indiscutibilmente ravvisabile una sua grave responsabilità nel non aver adottato le misure idonee ad evitare il danno per fatti di cui, come sopra detto, ha avuto sicura contezza.

A fronte del significativo ammanco di ben 2.5.milioni di Nano, ██████ avrebbe dovuto, secondo un canone di ordinaria diligenza, attivarsi per accertare esattamente la causa e adottare misure idonee. Ciò non è avvenuto tanto che la sua reazione - avendo rilevato chiaramente l'attacco in corso nelle date del 14-15 e 16 luglio 2017 e la sua tipologia, come evidenziato dal CTU - è stata quella di mettere in blacklist gli utenti collegati a questi episodi: ossia 5 o 6 account. Si tratta all'evidenza di una soluzione che anche ex ante non poteva che essere considerata del tutto inadeguata: sarebbe come se, a fronte del furto effettuato da alcuni ladri che abbiano una copia delle chiavi di una casa, agevolmente acquistabili sul mercato - ci si limiti a levare loro le chiavi: in effetti gli attacchi sono "rallentati", ma giusto il tempo di dare ai "ladri" (vecchi e/o nuovi) il tempo di munirsi di nuove chiavi e di utilizzarle in assenza dell'adozione di un sistema di prevenzione da parte dell'exchange del ripetersi dei fenomeni di appropriazione di criptovalute, resi possibili proprio dalle modalità di funzionamento della piattaforma.

Anzi quello che è stato accertato dal CTU è che vi era - tra l'altro - una *"gestione delle scritture contabili dell'exchange estremamente approssimativa che pone evidentemente in capo a ██████ una condotta di estrema negligenza (rimediare ad errori tramite spostamenti manuali non*



tracciati apre la strada a qualunque scenario)" con i quali ha cercato di rimediare ad un, ulteriore, baco nel sistema (che non merita qui approfondire, ma ampiamente analizzato, comunque, dal CTU). Al contempo non è stata adottata una misura di sicurezza (quale adottata dopo febbraio 2018) per quantificare l'entità del furto: ossia un controllo "che avrebbe potuto essere eseguito con sforzi minimi" secondo il CTU con la semplice verifica periodica del saldo totale di ogni criptomoneta dell'exchange, comparata con il saldo degli indirizzi di raccolta dei fondi, anche in forma di controllo quantomeno approssimativo per rilevare ammanchi particolarmente rilevanti, eseguibile con frequenza anche giornaliera con una semplice query - controllo che non risulta mai fatto - invero inspiegabilmente - fino al febbraio 2018.

3. Da quanto sopra esposto si ricava l'attendibile sussistenza di debiti di ██████ che, ove si abbia riguardo alla qualifica del deposito delle criptovalute in termini di deposito irregolare, è pari al valore che le stesse avevano al momento degli ammanchi, per 120 milioni di euro (considerato che l'80% delle stesse è stato sottratto).

Ma anche in ipotesi di qualificazione del rapporto tra la ██████ Solutions e gli utenti in termini di deposito regolare (che invero il Tribunale non ravvisa), vi sarebbe certamente responsabilità risarcitoria del ██████. Ciò sia ove si consideri il disposto dell'art. 1780 c.c., atteso che non solo le perdite sono derivate da un fatto a lui imputabile, ma anche è mancata l'immediata denuncia ai depositanti dei fatti per cui aveva perduto la detenzione - considerata la negligenza nella prestazione dei servizi successiva a luglio, con ammanchi di 7,5 milioni di Nano (contro i 2,5 del luglio), che porta ad una valutazione dei debiti in misura tale da superare lo sbarramento procedurale fissato dall'art. 15 LF e la soglia di cui all'art. 1 L.F.

La medesima responsabilità dovrebbe comunque ravvisarsi anche ove si intendesse fuoriuscire dall'inquadramento nel contratto tipico di deposito o in contratto misto a deposito, risultando comunque la relazione contrattuale disciplinata dai canoni generali degli artt. 1176 c.c. (diligenza nell'adempimento secondo i parametri del buon padre di famiglia e della natura dell'attività professionale esercitata) e 1218 c.c., sulla responsabilità contrattuale del debitore.

4. Per quanto attiene poi alla sussistenza del presupposto oggettivo di cui all'art. 5 l.f., si osserva che la condizione di insolvenza emerge dalla palese sproporzione tra l'ingente entità dell'esposizione debitoria conseguente alla gestione dell'impresa (che certamente dovranno essere oggetto di analitico e puntuale accertamento nel prosieguo della procedura) e le disponibilità di Francesco ██████, quali risultano dall'esecuzione del sequestro, tanto più considerato che l'impossibilità di restituire le risorse sottratte o di garantire un risarcimento adeguato emerge nitidamente dal contenuto dei comunicati pubblicati sul sito www.██████.com, con proposta di soluzioni transattive, riportate dal ricorrente e dal Pm negli atti introduttivi, ed allegate. L'impresa, peraltro, è stata cancellata dal registro delle imprese.



5. Come curatore fallimentare si nominano, congiuntamente, considerati i presumibili profili di complessità nella gestione della procedura, il dott. Giampiero Castaldi e l'avv. Tommaso Ariani

P.Q.M.

Visti gli artt. 1, 5, 6 e 16 del R.D. 16/03/1942 n. 267

dichiara

il fallimento di [REDACTED] quale titolare dell'impresa individuale .
[REDACTED] CF [REDACTED] con sede in
[REDACTED] Via [REDACTED] 235

nomina

giudice delegato la dott. Silvia Governatori e curatori il dott. Giampiero Castaldi e l'avv. Tommaso Ariani i quali faranno pervenire la propria accettazione entro 2 giorni dalla comunicazione.

ordina

alla fallita di depositare in cancelleria entro 3 giorni i bilanci e le scritture contabili obbligatorie, nonché l'elenco dei creditori, ove non ancora eseguito.

assegna

ai creditori ed ai terzi che vantano diritti reali o personali su cose in possesso della fallita termine fino a 30 giorni prima dell'adunanza per la presentazione al curatore delle domande di insinuazione ai sensi dell'art. 93 come modificato dal D.L. n. 179/2012 convertito nella L. 221/2012

stabilisce

che l'esame dello stato passivo abbia luogo dinanzi al giudice delegato nella adunanza del 07/05/2019 ad ore 10:30

Autorizza

la prenotazione a debito delle spese e diritti della presente sentenza e degli adempimenti consequenziali.

dispone

la pubblicazione e annotazione della sentenza ai sensi dell'art. 17 L.F. a cura della Cancelleria, che procederà altresì alla formazione del fascicolo ai sensi dell'art. 90 L.F..

Così deciso in Firenze il 19/12/2019, dal Tribunale come sopra composto, su relazione della dott. Governatori.

La presidente est

Dr. Silvia Governatori

