LE OFFERTE INIZIALI E GLI SCAMBI DI CRIPTO-ATTIVITÀ

DOCUMENTO PER LA DISCUSSIONE

Q1: Si condivide la definizione di "cripto-attività" delineata nel Riquadro 1? Riesce la definizione a catturare le specificità rilevanti della cripto-attività rispetto all'approccio delineato nel presente documento?

Parzialmente. Con la nascita di altre tecnologie, ibride, si assiste alla contrazione di quelle totalmente decentralizzate (e altamente volatili) rispetto a quelle parzialmente o apparentemente decentralizzate. Nell'ambito delle ICO, la piattaforma in maggior uso per l'esecuzione di smart-contracts è Ethereum, richiedendo l'acquisto di Ether (ETH) quale commissione per l'accesso. Tuttavia, dopo l'enorme fluttuazione dei cryptoassets, dal 2017 ad oggi, è sorta nel 2018 la stablecoin[1]. Dette stablecoin offrono la capacità di rendere stabili i cryptoassets attraverso un fondo in garanzia (collateralizzation), una riserva monetaria in fiat (normalmente il dollaro statunitense) o in cryptovalute. Queste piattaforme offrono immediata liquidità e (apparente) diminuzione del rischio negli investitori. Il mantenimento del prezzo in equilibrio oscura in qualche modo l'effettivo rendimento del progetto. La rilevanza delle piattaforme che usano stablecoin risiede nel loro impiego per lo sviluppo di smart contracts[2].

Q2: In particolare, si condivide la centralità degli elementi della finalizzazione al finanziamento di progetti imprenditoriali, dell'impiego di tecnologia basata su registri distribuiti e dello scopo ultimo della circolazione delle cripto-attività in appositi sistemi di scambi?

Parzialmente. Il riquadro 1 sembrerebbe diretto a un solo tipo di tecnologia: "DLT o Blockchain". Queste invece sono due tecnologie, la prima il *genus* e la seconda la *species*. La differenziazione è fondamentale giacché non tutti i cryptoassets hanno un'origine puramente

[1] Stablecoin è un tipo di cryptoasset piattaforma (come Ethereum) che non subisce fluttuazioni di prezzo. Ciò è dovuto alla collateralizzazione delle stesse, tenendo normalmente come riserva il dollaro statunitense, in rapporto 1:1. In questo modo si offre la possibilità a investitori in cryptoassets di convertire e trasformare i propri investimenti in stablecoins e successivamente in dollari, senza commissioni e perdite di cambio. La collateralizzazione può altresì avvenire con gli stessi cryptoassets – questo tipo di collateralizzazione è molto criticato giacché non è possibile capire fino a che punto l'eventuale overcollateralizzation (sovracollateralizzazione) rispecchi o meno la volatilità, ovvero il rischio dell'investimento.

[2] Equilibrium opera quale piattaforma per stablecoin attraverso la collateralizzazione di EOS (https://eosdt.com/). EOS è a sua volta una piattaforma blockchain per lo sviluppo di applicazioni decentralizzate (dApps). Si veda EOS.IO, Technical white paper v2, https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md

decentralizzata. Esempi come Iota[3] o Ripple offrono prova di cryptoassets (digital assets) che non sono (in sostanza) completamente decentralizzate[4].

Allo stesso tempo è da notare che sono in aumento i progetti su blockchain che lavorano su protocollo Proof-of stake (PoS), a differenza del comune proof-of-work (PoW), sul quale sono invece basate Bitcoin ed Ethereum[5]. Invero, nel decreto Semplificazioni del 2018, si fa soltanto riferimento, quale oggetto di regolamentazione, alle "tecnologie e [a]i protocolli informatici che usano un registro […] architetturalmente decentralizzato su basi crittografiche": questa definizione esclude Ripple[6], NEO[7], Bitcoin Gold[8], crypto-assets potenzialmente rientranti nella definizione di strumento finanziario ma che sono in qualche modo centralizzati, e dunque non rientrano nelle definizioni di strumento finanziario a livello europeo.

Inoltre, sempre nel decreto Semplificazioni, si ipotizza quale caratteristica del "token" (digital asset) la non alterabilità o immodificabilità. Questa definizione rispecchia parzialmente la realtà. Nel linguaggio informatico, sebbene non ci sia consenso su molti aspetti definitori in tema di digital assets, la tecnologia blockchain è descritta come *tamper resistant*, vale a dire che è resistente (potenzialmente) alla manomissione. In effetti, non è vero che non siano

[3] Iota (Ticker: MIOTA) si basa sulla tecnologia DAG (Directed Acyclic Graph), la quale è un registro distribuito ma non segue la funzione *hash* come nel caso di blockchain. Il loro progetto si focalizza sulle internet of things (IoT).

[4] In effetti, Iota, seppur promuova nel proprio white paper l'ambito di operatività nei registri distribuiti, ha una funzionalità prevalentemente centralizzata – attraverso un albero di nodi gestito da un coordinatore, the Tangle –, quindi, in teoria, sottoposta a maggiore vulnerabilità rispetto ai progetti lanciati su blockchain. Di conseguenza, le caratteristiche di immutabilità (o come meglio si vedrà nei prossimi paragrafi di resistenza alla modificabilità) verrebbero meno. Ciononostante, nel white paper the Tangle è definito come un sistema più affidabile rispetto al sistema di blocchi di Bitcoin. Serguei Popov, *The Tangle*, April 30, 2018. Version 1.4.3. https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf (ultimo accesso, 3 giugno 2019).

[5] Da notare un futuro incremento di crypto-assets rilasciati su PoS, dovuto alla necessità di tutela e protezione dell'ambiente e della *green economy* sponsorizzata come valore aggiunto al progetto. Inoltre, su questo versante molte aziende si sono definite "mobili", cioè in grado di spostarsi a seconda delle esigenze. Il macchinario operativo di queste attività imprenditoriali viaggia su camion porta container immersi in liquidi refrigeranti, riducendo le emissioni di Co2. Queste startup "itineranti" in realtà viaggiano alla ricerca di giurisdizioni ICO *friendly*. Cfr. De Filippi, Wright, *Blockchain and The Law: The Rule of Code* (Cambridge: Harvard University Press, 2018).

[6] (Ticker: XRP) Centralizzazione della proprietà di token pre-minati. Al momento attuale XRP sta attraversando una continua decentralizzazione. Tuttavia, il dato rilevante è che questo strumento ha avuto origine in modo centralizzato. Si veda Chase e MacBrough, Ripple White paper, 'Analysis of the XRP Ledger Consensus Protocol', https://arxiv.org/pdf/1802.07242.pdf. Cfr. White Paper iniziale, Schwartz, Youngs, e Britto, 'The Ripple Protocol Consensus Algorithm', https://ripple.com/files/ripple_consensus_whitepaper.pdf. (ultimo accesso, 3 giugno 2019).

[7] (Ticker: NEO) Centralizzazione di nodi, laddove uno o più nodi sono controllati da una entità singola. Neo possiede 7 nodi di validazione che sono controllati dal team di NEO.

[8] (Ticker: BTG) Centralizzazione di hash power, ovvero il controllo maggioritario delle funzione hash da parte di un singolo gruppo di miners, da una singola entità. https://bitcoingold.org/wp-content/uploads/2017/10/BitcoinGold-Roadmap.pdf.

completamente immodificabili o inalterabili. Esempi come il DAO[9] dimostrano come non sia immodificabile, o inalterabile, sebbene il costo dell'alterazione (e del successivo ripristino) sia tale da scoraggiare qualunque tipo di attacco al sistema.

Allo stesso tempo, il codice che origina il processo di minting (coniazione) molto spesso lascia spazio alla successiva modificabilità del progetto originale, in riferimento alle caratteristiche della moneta. Per esempio, modificando il tetto massimo di emissione della moneta, o biforcando il progetto originale, creandone uno subordinato o indipendente, simile all'originale[10]. Comunemente, questa biforcazione avviene quando ci sono delle falle nel codice. La biforcazione porta quindi con sé il deprezzamento del valore della moneta (digital asset): spesso accade che il progetto originale perda di valore (in seguito alla perdita di credibilità), mentre quello nuovo acquisisce maggior valore (in funzione del consenso degli investitori "sofisticati" vedi Q9).

Q3: Riesce la definizione ad escludere con chiarezza le fattispecie non idonee a costituire oggetto di trattazione secondo l'approccio delineato nel documento (i.e. pure commodity-token non destinati alla circolazione su circuiti di scambio di tipo secondario, valori mobiliari/strumenti finanziari come codificati dalla disciplina EU)?

Sì. Tuttavia, ritengo che debba darsi maggiore enfasi alle fattispecie che ricadono nel commodity token, ampliando il contenuto definitorio di quei token i cui profitti prescindono dalle sole forze dei venditori, promoter, o altri soggetti coinvolti.[11]

Q4: La disciplina vigente per strumenti e prodotti finanziari prevede regole all'ingresso volte a graduare i diversi presidi posti a tutela degli investitori; si condivide la previsione di una disciplina delle cripto-attività regolate che invece non contempla, ad esempio, soglie di valore per esenzioni (riferite alle emissioni sotto soglia) oppure maggiori presidi (per le emissioni sopra soglia)?

La previsione di una disciplina per maggiori presidi, per le emissioni sopra-soglia, è condivisibile. Rispetto alle esenzioni, il mercato dei crypto-assets è ancora un mercato troppo

[9] SEC, 'Securities and Exchange Commission, Release No. 81207/July 25, 2017. Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO'.

[10] Esempi di detta biforcazione sono Ethereum (ETH) e Ethereum Classic (ETC). Nell'ordinarietà degli eventi, tali biforcazioni sono avvenute in conseguenza di una falla del sistema. Invero, la garanzia di immutabilità è stato lo slogan della cybercommunity: la biforcazione prevede quindi il mantenimento del codice originale sotto accusa e la scissione rispetto ad esso con una nuova catena di blocchi.

[11] Si veda la distinzione del mercato statunitense nei Natural Resources Cases, dove certe commodities sono escluse dall'ambito delle securities, date le loro caratteristiche di realizzare profitto solo in funzione del "naturale" incontro tra domanda e offerta, giammai dagli sforzi compiuti da promotori delle stesse. La categoria dei commodity tokens può paragonarsi alla detenzione di monete fiat, le quali esulano dalla regolamentazione europea in materia di strumenti finanziari.

immaturo e incerto, pertanto esenzioni e altre procedure fiscali potrebbero creare il cd. *chilling effect*, arrestando potenzialmente l'innovazione e spostando i capitali in giurisdizioni più liberali.

Q5: Si condivide la proposta di ampliare la gamma delle attività che possono essere effettuate dai gestori di portali di crowdfunding a comprendere anche la promozione di offerte di cripto-attività di nuova emissione? Si chiede inoltre di fornire motivazioni e/o dati a supporto dell'identificazione di eventuali sinergie/opportunità che possano scaturire dallo svolgimento di entrambe le attività, oppure rispetto a eventuali ragioni di contrarietà

Il crowfunding opera in un modo totalmente diverso rispetto agli investimenti in progetti nella blockchain o utilizzando altre tecnologie DLT. Innanzitutto, chi gestisce un crowfunding non ha le capacità tecniche per valutare la complessità e adeguatezza del progetto (vedasi Q9): è vero che ha dei canali che possono agevolare l'ingresso di capitali, ma difetta della gestione su grande scala. L'attività di crowfunding è maggiormente legata a una certa territorialità del progetto, mentre le ICO hanno una platea molto più vasta di investitori. Inoltre, i requisiti previsti dal regolamento crowfunding possono avere un contro-effetto, frenando le attività su DLT[12].

Quando pensiamo a questo settore parliamo di un gruppo di *techs*, ingegneri e sviluppatori di software, senza alcuna competenza giuridica o economica. Sono soggetti tendenzialmente in posizioni antitetiche rispetto a quella di un giurista o economista. Pertanto questi *team* possiedono alte capacità tecniche ma difettano di ragionamento giuridico-economico. La necessità di ricorrere al pubblico senza l'uso di canali tradizionali è stata dettata dal fatto di interrompere il vincolo sia con i cd. intermediari, sia con i requisiti imposti per l'accesso all'investimento pubblico. Infatti, Bitcoin è nata dalla contrarietà a cedere il controllo al di fuori della cerchia dei *techs*, perché non potrebbero essere capite le potenzialità del progetto o le decisioni che possano migliorare il progetto, pur implicando cospicue perdite.

Il punto focale della discussione intorno alle ICO parte dalla premessa che gli appartenenti al *cypherpunk movement* impiegano la tecnologia per risolvere un problema giuridico, rispetto al quale il legislatore si trova a "rincorrere" la tecnologia[13].

Q6: Si condivide la proposta di estendere lo svolgimento dell'attività di gestione di piattaforme per le offerte di cripto-attività anche a soggetti operanti sin dall'inizio ed esclusivamente in cripto-attività (ovvero che non abbiano già avviato un'operatività quali gestori di portali per le offerte di crowdfunding autorizzati dalla Consob)?

[12] Tra gli altri, i requisiti enucleati nell'art. 9 "Requisiti di onorabilità e professionalità dei soggetti che svolgono funzioni di amministrazione, direzione e controllo". Queste figure, al di là dell'essere inadeguate allo scopo in oggetto – non avendo competenze tecniche per la valutazione della viabilità del progetto –, sono troppo onerose.
[13] Denota la nascita della *lex cryptographica*. De Filippi e Wright, *supra*.

D'accordo. Sebbene i loro requisiti, profondamente diversi, debbano essere integrati rispetto ai gestori di portali per le offerte di crowdfunding. Non è escluso che chi già opera come gestore di crowfunding possa implementare i propri servizi da offrire a soggetti interessati allo sviluppo di critto-attività (Riquadro 3).

Q7: L'approccio delineato per lo svolgimento delle offerte in sede di nuova emissione di cripto-attività riesce a conciliare le caratteristiche del fenomeno con le esigenze di tutela degli investitori? Si condivide, in particolare, la previsione di un regime cosiddetto di opt-in, articolato nei termini sopra descritti?

L'approccio corrisponde alle caratteristiche del fenomeno. Il meccanismo dell'opt-in è fondamentale in questa fase di transizione.

Q8: Si ritiene opportuno, nell'ottica della maggiore tutela degli investitori, stabilire uno stretto collegamento fra l'offerta di cripto-attività di nuova emissione, realizzata per il tramite di piattaforme vigilate, e il loro successivo accesso a un sistema di scambi dedicato soggetto a regolamentazione e vigilanza (cfr. paragrafo che segue)?

Sì.

Q9: Quali requisiti minimi si ritiene che debbano possedere i soggetti che emettono criptoattività, affinché queste ultime possano essere accettate per la negoziazione?

Per iniziare, l'autoregolamentazione, non solo tramite buone pratiche del settore, è già presente in fase prodromica[14] per gli sviluppatori che utilizzano il linguaggio Solidity[15]. Il Crypto Currency Certification Consortium (C4), conformato da esponenti di rilievo nell'ambito delle crypto (tra cui Vitalik Butterin, creatore di Ethereum), offre diverse certificazioni. Al momento attuale le certificazioni per sviluppatori di Ethereum (CED) e per Crypto Currency Security Standard Auditor non sono in fase di esecuzione. Tra i requisiti, oltre al superamento di diverse materie di base, ci sono anche l'onorabilità e la professionalità, nonché il rispetto di un codice etico[16].

Diventa indispensabile che gli emittenti sottopongano il progetto a un processo di revisione legale, *audit* del progetto. Questo può avvenire tramite società di audit: i BigFour si sono già dotati di personale che può aiutare in questo processo. Tuttavia, la peculiarità dell'ambiente sul quale viaggiano i crypto-assets rende pressoché vani i tipi di audit tradizionali.

[14] Al momento attuale le uniche certificazioni rilasciate sono quella di Certified Bitcoin Professional (CBP) e Certified Bitcoin Expert (CBX), mentre quella di Certified Ethereum Developer (CED), di durata biennale, è ancora in standby. https://cryptoconsortium.org/certifications/CED

[15] Al momento attuale la maggior parte delle dApps (applicazioni decentralizzate) su Ethereum utilizzano il linguaggio Solidity per lo sviluppo di smart contracts. C. Dannen, *Introducing Ethereum and Solidity. Foundations of Cryptocurrency and Blockchain Programming for Beginners* (Brooklyn, New York: Apress, 2017).

[16] https://cryptoconsortium.org/about

Per converso, il tipo di audit richiesto per il corretto funzionamento delle cripto-attività è un mix tra audit legale, commerciale e tecnico. L'audit tecnico è quello già presente nella prassi, sotto forme diverse, e che riflette le esigenze di sicurezza e affidabilità del codice (progetto)[17]. Questo compito è svolto da agenti che coprono ruoli differenti, non univoci. Al momento attuale, si individuano i seguenti tipi di audit di sicurezza tecnica (o viabilità del progetto): CodeLegit[18], Zepellin[19], IbcGroup[20], ChainLink[21], Provable[22] (già Oraclize). Degni di nota sono CodeLegit e Provable. Il primo, giacché raggiunge qualcosa di molto vicino rispetto a quello che potrebbe essere un ICO gatekeeper[23]. La sua intersezione tra competenze giuridiche e tecniche viene impiegato da sviluppatori per incentivare la veicolazione di informazione (una volta ricoperta dal prospetto e dall'operato degli intermediari finanziari)[24]. Per quanto riguarda la seconda Provable, essa opera tramite una tecnologia denominata TLS Notary, la quale fornisce una prova di autenticità, così come nell'ambito notarile, garantendo la veridicità delle componenti attestati tramite "oracoli". Risulta alquanto interessante che tutte queste tecnologie, operano attraverso lo sfruttamento di Oracles (nel linguaggio informatico sono tecnologie terze che riescono a connettere l'ambiente esterno circostante ad oggetti o software collegati tramite internet: in effetti sono usati molto nell'internet of things, o meglio internet of everything - IoE): questi "oracoli" hanno la capacità potenziale di integrare le promesse dichiarate in documenti correlati (leggasi white paper, etc.) con quelle definite nel codice, oppure condizioni, per esempio rispetto all'acquisto di diritti di voto e controllo[25].

Per quanto riguarda l'audit legale-commerciale è quello già svolto dai revisori legali dei conti e società di audit. Il *quid* che si ritiene sia necessario risiede nell'introduzione di un auditor che riesca a realizzare una maggiore trasparenza del mercato, investendo questo nuovo tipo di intermediario di una funzione pubblica. In questo modo, il suo ruolo è quello di rendere conoscibile l'ambito dell'offerta e del progetto incorporati nel *white paper* (o altri documenti

[17] Il codice viene sottoposto ad un referraggio da parte dei membri della comunità tramite il portale github. Esiste una correlazione tra pubblicazione del codice e buona riuscita dell'ICO, così come dimostrato da Adhami, Giudici e Martinazzi. Tuttavia, la mancata rivelazione del codice molto spesso è associata alla protezione del patrimonio/ proprietà intellettuale. S. Adhami, G. Giudici, & S. Martinazzi, 'Why do businesses go crypto? An empirical analysis of initial coin offerings,' *Journal of Economics and Business*, vol. 100(C), 64-75 (2018)

[18] http://codelegit.com/ CodeLegit offre anche un servizio di arbitrato tra i dententori delle ICO e gli sviluppatori del progetto. Si veda CodeLegit white paper, https://docs.google.com/document/d/1v_AdWbMuc2Ei70ghITC1mYX4_5VQsF_28O4PsLckNM4/edit

[19] Audit prevalentemente di cyber security. https://zeppelin.solutions/security-audits/

[20] Il suo apporto consiste nella redazione di white paper, e assistenza durante le fasi dell'ICO. https://ibcgroup.io/services/

[21] Sfrutta gli oracoli per l'aggregazione di informazioni e integrazione delle promesse, specialmente quando vi è presente una condizione, si pensi al mercato assicurativo. https://chain.link/features/

[22] Agisce come un intermediario tra gli smart contracts utilizzando i dati forniti da altri smart contracts corredati da prove di autenticità. https://provable.xyz/

[23] J. Coffee, *Gatekeepers: The Professions and Corporate Governance* (New York: Oxford University Press, 2006).

[24] Per approfondimenti sui diversi tipi di "intermediari" nel processo pre e post ICO cfr. Villanueva Collao e Winship, *New ICO Intermediaries* (saggio attualmente sottoposto a referaggio).

[25] *Idem*.

grafici e informatici che possano definire in modo leggibile l'offerta) con le promesse effettive presenti nel codice[26].

Invero, nella fase del minting (nell'emissione o trasformazione in token o in cryptocurrency), le oggettive caratteristiche dell'offerta sono plasmate nel codice, *ergo* sono codificate. Alle origini del movimento *cypherpunk* non occorreva dotarsi di un documento "human readable", cioè intellegibile alle persone non appartenenti all'ambiente informatico. Infatti, i primi investitori erano membri della comunità *cypherpunk*, in grado di decifrare il contenuto dell'offerta e del progetto. In questo modo, la crypto-community ha eliminato virtualmente ogni intervento volto a mediare tra le parti, come accade nei comuni mercati finanziari. La democratizzazione dei mercati finanziari ha modificato la rosa dei potenziali investitori, comprendendo anche investitori *non sofisticati*, incapaci di leggere il codice. L'opera di decodificazione è una delle funzioni del ICO gatekeeper – nuovo intermediario.

Studi empirici hanno dimostrato come, nella stragrande maggioranza di lanci di ICO, nel periodo 2018, ci sia stata una copiosa inconsistenza tra le promesse descritte in formati "human readable" - come white papers, messaggi pubblicitari su canali youtube o social media, e altri - e quelli concretatisi nel codice[27]. Detta inconsistenza è foriera di manipolazioni di mercato e truffe ai danni degli investitori non sofisticati. Al momento attuale la maggiore asimmetria è data dalla pubblicizzazione di diritti di voto non presenti nel codice.

A questo proposito l'opera dell'auditor si svolge nel più grande quadro delle regolamentazioni europee[28], ma con una variante: così come nel caso della professione notarile, sono attività usufruite da privati ed erogate da privati, nell'ambito della libera professione ma svolgenti funzioni pubbliche[29]. Questa funzione non solo garantisce trasparenza e fiducia nei mercati finanziari, oltre al buon esito dell'ICO, ma una significativa diminuzione delle asimmetrie informative attualmente imperanti nella blockchain.

[26] Infatti, le fasi di audit dei progetti si concretano nella traduzione, riconciliazione e verificazione della consistenza delle promesse fornite attraverso un linguaggio intellegibile rispetto a quelle completamente verificate. *Idem*.

[27] S. Cohney, D. A. Hoffman, J. Sklaroff, Jeremy D. Wishnick, 'Coin-Operated Capitalism' *Columbia Law Review*, Forthcoming; U of Penn, Inst for Law & Econ Research Paper No. 18-37, SSRN: https://ssrn.com/abstract=3215345 or http://dx.doi.org/10.2139/ssrn.3215345; (ultimo accesso 4 giugno 2019).

[28] European Parliament and the Council Regulation (EU) 2014/537 of 16 April 2014 on specific requirements regarding statutory audit of public-interest entities and repealing Commission Decision 2005/909/EC [2014] OJ L158/77.

[29] Da segnalare come queste funzioni, seguendo la linea della blockchain community, possano essere svolte da società virtuali od operatori virtuali. Per un esempio di gestione tramite sistemi autonomi nel diritto societario si veda Bayern, Burri, Grant, Hausermann, Möslein, e Williams, 'Company Law and Autonomous Systems: A Blueprint for Lawyers, Entrepreneurs, and Regulators', in *Hastings Science and Technology Law Journal*, vol. 9:2, summer 2017.

Q10: La proposta definizione di "sistema di scambi di cripto-attività" è idonea a comprendere i modelli di business, allo stato noti, di circuiti per la negoziazione di crypto-asset?

Sì. Tuttavia, occorre sottolineare - specialmente nelle DTL totalmente decentralizzate, tipo blockchain - che nell'emissione di questi valori mobiliari (criptoassets o digital assets – come preferirei denominarli al fine di comprendere una maggiore quantità di fattispecie), non esiste il corrispettivo di emittente così come definito dalle regolamentazioni nazionali ed europee. Invero, nella blockchain il team facente parte del progetto sviluppa e ingegnera il progetto, ma è la comunità che emette la moneta. Nel caso delle ICO, non pre-mined (pre-minate), dai matematici che risolvono i puzzle. Quindi ci rivolgiamo a una cerchia di soggetti indeterminati e non localizzabili, o meglio ai quali non è possibile sottoporre la nostra giurisdizione. Ad ogni modo, se il legislatore decide di ricomprendere nella nozione di emittente anche (o solo) chi sviluppa il progetto, allora deve essere specificata la specialità della situazione rispetto a quella dei comuni emittenti[30].

Q11: I requisiti sopra individuati, il cui accertamento è condizione per l'attribuzione della qualifica di sistema di scambi di cripto-attività da parte della Consob, sono presidi sufficienti a neutralizzare i rischi connaturati alla negoziazione di cripto-attività?

Sono sufficienti. Si veda Q9 per l'integrazione in tema di sicurezza e di riduzione delle asimmetrie contrattuali e informative.

Q12: I requisiti sopra individuati, il cui accertamento è condizione per l'iscrizione del sistema nel registro tenuto dalla Consob, sono presidi sufficienti a neutralizzare i rischi connessi alla custodia delle risorse finanziare, delle cripto-valute e delle cripto-attività da parte del sistema, nonché alla realizzazione di un regolamento efficiente e sicuro delle contrattazioni che avvengono sul sistema?

Concordo.

Q13: Quali caratteristiche dovrebbe avere la blockchain al fine garantire un adeguato livello di sicurezza del registro distribuito su cui le cripto-attività vengono registrate e trasferite?

Come descritto sopra (Q2 e Q9), nell'ambito dei distributed ledgers, la sicurezza è determinata dalla affidabilità dell'algoritmo. Che si impieghi la tecnica PoW o PoS, l'importante è che le transazioni vengano registrate. In questo senso, gli Exchange hanno un ruolo precipuo nella corretta esecuzione dei trasferimenti. Inoltre, le piattaforme di scambi (exchange) che sono anche custodial devono essere dotate di un sistema di cold storage (immagazzinamento a freddo - disco

[30] In effetti, in casi come questo al quale assistiamo l'elemento determinante è quello già definito da Lessig, il *patetic dot*, l'oggetto della regolamentazione scompare sostituito da sistemi codificati e autonomi. Lessig, *Code: Version 2.0* (New York: Basic Books, 2006).

esterno) che riesca a garantire la sicurezza dei valori contenuti nello stesso. Al momento attuale esistono degli exchange noncustodial[31]: per questi ci sono maggiori difficoltà di regolamentazione, dal momento in cui non è possibile monitorare il volume delle transazioni e l'identità dei soggetti partecipanti, posto che non occorre creare un account e passare per i diversi livelli di controllo/protezione (Kraken, maggiore exchange tedesco, ne ha fino a 4 livelli per poter usufruire della piattaforma). Al contempo, l'uso di questi exchange custodial tutela maggiormente gli sviluppatori, le piattaforme e i loro investitori[32]. Offre una garanzia di affidabilità e trasparenza.
Tuttavia, si tenga presente che molti exchange che trattano monete di successo non sono portati a cooperare e preferiscono tutelare la riservatezza dei loro clienti[33]. Al contrario, sempre frutto della cultura cypherpunk, credono ferventemente negli organismi di autoregolamentazione.

Q14: Si condivide la scelta di introdurre un meccanismo di "opt-in" per l'iscrizione nel registro dei sistemi di scambi di cripto-attività, che sarebbe tenuto dalla Consob?

Totalmente condivisibile.

Q15: In connessione con l'eventuale introduzione di un regime speciale per l'emissione e la circolazione delle cripto-attività, con l'obiettivo della tutela degli investitori, si ritiene opportuno che le autorità valutino la previsione di un regime transitorio in ragione del quale la prosecuzione degli scambi di token già emessi risulti possibile solo a condizione che l'organizzatore del sistema di scambi registrato presso la Consob abbia verificato la sussistenza e la pubblicità di adeguate informazioni per gli investitori sui token scambiati?

Sì, totalmente d'accordo.

[31] Per esempio Shapeshift. https://shapeshift.io/#/coins
[32] Tra le molte difficoltà, la possibilità di vedere persi i propri investimenti per via di un banale errore nel trasferimento dei cryptoassets.
[33] La posizione di Kraken rispetto al diniego di cooperazione internazionale. https://blog.kraken.com/post/1561/krakens-position-on-regulation/