ASSOCIAZIONE TRUSTED SMART CONTRACT

"Le offerte iniziali e gli scambi di cripto-attività"

RISPOSTA AL DOCUMENTO DI DISCUSSIONE CONSOB

L'Associazione Trusted Smart Contract è lieta dell'occasione di confronto offerta da codesta Autorità attraverso il Documento per la Discussione in materia di offerte iniziali e scambi di cripto-attività, conosciute sul mercato anche come ICO, dall'acronimo inglese *Initial Coin Offering*.

L'Associazione ritiene cruciale una riflessione sul tema, sia per garantire la necessaria tutela degli investitori, sia per consentire che anche il nostro Paese possa accreditarsi come una giurisdizione nella quale gli emittenti possano con fiducia decidere di effettuare un'offerta di critpo-attività.

Per il perseguimento di entrambi i fini è necessario un quadro normativo di certezza del diritto e di regole eque e chiare, che tengano conto delle peculiarità del settore e si pongano in maniera coerente con le prassi che il mercato è andato sviluppando in questi anni.

L'Associazione Trusted Smart Contract è un ente che ha come scopo quello di studiare ed approfondire tematiche inerenti le tecnologie *distributed ledger* (DLT), *blockchain* e, più in generale, relative alla innovazione digitale nonché gli *smart contracts*, con particolare riferimento agli aspetti legali necessari per garantire che tanto le infrastrutture quanto gli *smart contracts* rispettino e mantengano in ogni momento i requisiti necessari per l'osservanza della normativa legale vigente e siano suscettibili di essere utilizzati da operatori di business, anche regolamentati e si propone inoltre di rivestire un ruolo di guida e di promozione nel campo della normazione tecnologie dell'informazione e delle comunicazioni.

Il sito internet dell'Associazione, dal quale risulta anche l'elenco dei soci, è www.trustedsmartcontract.org.

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?

L'Associazione Trusted Smart Contract (TSC) condivide la centralità degli elementi sopracitati a supporto delle attività di finanziamento di progetti imprenditoriali. L'Associazione ravvisa altresì l'importanza tecnologica dello strumento innovativo degli Smart Contract. L'utilizzo di contratti digitali che eseguano una logica programmativa in un contesto di esecuzione software distribuito è infatti cruciale per la tutela di investitore ed emittente per quanto concerne l'emissione dell'asset, garantendo il pieno adempimento agli obblighi delle controparti, nonché la gestione successiva dell'asset emesso. Infatti, è possibile sfruttare la programmabilità degli smart contract per implementare ad esempio logiche di *locking* dei fondi a garanzia dei termini di *vesting* stabiliti per investitori e promotori dell'iniziativa, regole di *voting* a supporto dei processi decisionali dell'emittente, e vincoli di spendibilità sui fondi al raggiungimento di milestone di raccolta e/o rilascio di semilavorati o primi servizi (già implementati in processi di raccolta di tipologia "DAICO"). Allo stesso tempo, l'implementazione di smart contract necessita di standard e *best practice* che garantiscano l'assoluta aderenza del codice software alla prosa

Via Castellanza, 11
20151 Milano – Italia
Codice Fiscale: 97824970152
info@trustedsmartcontract.org

legale a descrizione di termini e condizioni, riportate solitamente all'interno di un documento "white paper", agli investitori e a tutti gli stakeholder interessati.

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?

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?

In riferimento al regime di "*opt-in*" discusso in Q7 e Q14, L'Associazione Trusted Smart Contract (TSC) condivide l'importanza che l'adesione sia su base volontaria. L'Associazione ravvisa altresì l'importanza di un adeguato arbitraggio normativo stante le possibili asimmetrie che si verrebbero a creare fra operatori che aderiscono facoltativamente ai due regimi previsti. L'associazione evidenzia anche un possibile costo di regolamentazione non determinabile con esattezza ex ante (procedere all'offerta senza ricorrere alle nuove piattaforme per l'offerta di crypto-attività, correndo però il rischio di un inquadramento del token nella categoria dei prodotti finanziari e relativo assoggettamento alla disciplina applicabile, esprime un'incertezza giuridica che può costare molto). In alternativa si potrebbero definire regole precise per sandbox, in modo da ridurre gli spazi lasciati alla libera interpretazione.

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

L'Associazione Trusted Smart Contract (TSC), nell'ottica di preservare il più possibile la tutela dei risparmiatori, ritiene che dovrebbe essere valutata l'introduzione sia di requisiti di onorabilità in capo ai soggetti componenti gli organi amministrativi e di controllo dei soggetti emittenti sia, avendo riguardo alla fase di collocamento delle cripto-attività, tenuto altresì conto del livello rischiosità connesso alle singole iniziative progettuali, di requisiti minimi di patrimonializzazione.

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?

Premessa

Si osserva in primo luogo, in particolare dato che la domanda è inserita nell'ambito del capitolo del documento di discussione dedicato ai sistemi di scambi di cripto-attività, che la tecnologia blockchain viene in considerazione almeno sotto due profili:

- Sotto un primo profilo, una tecnologia DLT è coessenziale all'esistenza stessa di una cripto-attività, come osservato correttamente nella proposta di definizione contenuta nel Riquadro 1;

- Per un secondo aspetto, la tecnologia blockchain potrebbe essere impiegata nell'ambito di un sistema di scambio; in particolare
    - L'utilizzo sarebbe meramente eventuale nel caso di sistema di *centralised exchange*, che normalmente agisce anche quale *custodian* e *provider* di *wallet*;
    - L'impiego di tecnologie DLT sarebbe intrinsecamente connaturato ai sistemi di *decentralised exchange*, che tipicamente si servono di uno *smart contract* per far incontrare domanda ed offerta e soprattutto per eseguire lo scambio tra crypto-asset o tra questi e valuta fiat, con meccanismo di *delivery versus payment*.

Blockchain permissioned e permissionless

Secondo l'Associazione Trusted Smart Contract, l'approccio regolatorio dovrebbe, per entrambi i profili, essere conforme alla scelta legislativa, come correttamente osservato dal richiamo nel Riquadro 1 del Documento per la Discussione.

Il c.d. decreto Semplificazioni (decreto-legge 14 dicembre 2018, n. 135) ha adottato, lo si ricorda, un approccio *technology neutral*, non introducendo discriminazioni tra blockchain *permissioned* e *permissionless*. Tale scelta di politica legislativa è quella normalmente adottata e raccomandata dall'Unione Europea ed è quella meglio in grado di assicurare flessibilità e possibilità di adattamento alle evoluzioni sia tecnologiche che di modelli di *business*.

Si ritiene che questa sia anche una corretta scelta di strategia regolamentare, sia in quanto coerente con la legislazione nazionale ed i principi ispiratori di quella europea, sia perché l'esperienza dimostra che al momento sostanzialmente tutte le emissioni di *crypto-asset* sono effettuate su blockchain *permissionless*.

Come subito si vedrà, si ritiene che adeguati requisiti di sicurezza possano essere forniti da entrambe le tipologie di blockchain.

Il fine dichiarato di garantire l'identificazione dei partecipanti ai sistemi di scambio è senz'altro condivisibile, ma può essere ottenuto in altro modo. Ad esempio, se l'*exchange* agisce anche da *custodian* l'identificazione può essere effettuata direttamente da quest'ultimo. Diversamente, in caso di *direct exchange*, l'identificazione può comunque essere garantita in altri modi, tipicamente *off-chain*, ad esempio tramite il gestore di *wallet* o anche attraverso sistemi di identità digitale, potenzialmente anche su blockchain.

Caratteristiche della blockchain

Veniamo ora ad esaminare i requisiti di sicurezza delle blockchain utilizzate. Si ritiene che tali requisiti valgano per tutte le blockchain, tanto quelle necessarie per l'emissione e il passaggio di proprietà delle cripto-attività, quanto quelle eventualmente impiegate dai sistemi di scambio.

Questo paragrafo sarà diviso in due parti: nella prima esamineremo i requisiti di sicurezza a nostro avviso più importanti allo stato dell'arte; nella seconda, invece, formuleremo qualche osservazione sul modo migliore di normare tali requisiti.

Associazione Trusted Smart Contract

Via Castellanza, 11
20151 Milano – Italia
Codice Fiscale: 97824970152
info@trustedsmartcontract.org

Requisiti di sicurezza

Governance - Blockchain permissioned

In questo tipo di blockchain devono essere considerati in particolare i criteri di composizione iniziale e di gestione nel continuo della compagine dei nodi di autorizzazione, in relazione, in particolare, con l'algoritmo di consenso adottato.

A parte l'ovvia richiesta di requisiti di onorabilità, dovrebbe essere assicurato, infatti, un adeguato conflitto di interessi tra i soggetti gestori dei nodi, per salvaguardare una gestione imparziale e non discriminatoria delle transazioni informatiche operate dal sistema. Il numero dei nodi, sotto questo profilo, è meno rilevante, mentre appare importante la presenza di uno o più nodi "di garanzia", in grado di tutelare gli interessi degli investitori.

L'algoritmo di consenso ha un'importanza minore rispetto al caso di una blockchain pubblica, in quanto è noto il soggetto autorizzatore, che rimane quindi sempre soggetto ad una verifica del suo operato ed esposto al risarcimento dei danni e a eventuali sanzioni amministrative in caso di violazioni.

Governance - Blockchain permissionless

Gli elementi di governance maggiormente rilevanti per questo tipo di blockchain sono il numero di nodi e l'algoritmo di consenso.

Numero dei nodi

La sicurezza di una blockchain *permissionless* è basata in modo importante sul numero dei nodi di autorizzazione attivi (non, si sottolinea, dei nodi astrattamente presenti). Dovrebbe pertanto essere assicurata la presenza di un sufficiente numero di nodi di autorizzazione attivi in ogni momento, ossia un numero adeguato in relazione all'algoritmo di consenso adottato.

Algoritmo di consenso

L'algoritmo di consenso (come già ricordato) è particolarmente rilevante nel caso di blockchain *permissionless*, nel cui caso dovrebbe essere tenuto in particolare considerazione.

La finalità dovrebbe essere quella di assicurare la parità di trattamento dei destinatari delle offerte che si trovino in identiche condizioni, evitando – tra l'altro – che vengano autorizzate transazioni non corrette e che vengano rifiutate transazioni corrette.

Anche in questo caso, non si ritiene sia possibile prendere posizione in astratto rispetto all'ampia varietà di algoritmi che la prassi in questo momento conosce e che sono comunque in rapida evoluzione.

Identificazione dei soggetti che effettuano transazioni

In ogni caso, come correttamente osservato da codesta Autorità e come affermato anche pocanzi, è necessario che venga garantita l'identificazione dei soggetti che effettuano le transazioni, conformemente, tra l'altro, alla normativa antiriciclaggio vigente.

L'identificazione è una fase che può tipicamente avvenire *off-chain* e – come sopra osservato – può avvenire con diverse modalità (incluso anche, come esempio ulteriore a quelli già riportati, con l'integrazione col sistema SPID), per cui – si ribadisce – è indipendente dalla scelta tecnologica di avvalersi di una blockchain pubblica o privata.

Conservazione digitale

Dovrebbe essere previsto in ogni caso l'obbligo di conservazione digitale, con le modalità previste dal Codice dell'Amministrazione Digitale, delle transazioni effettuate sulla blockchain in fase di offerta iniziale e successivamente. Tale obbligo dovrebbe estendersi per il periodo di conservazione delle scritture contabili (in via normale 10 anni, come previsto dal codice civile).

In linea di principio, quindi, almeno un nodo della blockchain dovrebbe assumere contrattualmente quest'obbligo nei confronti dei sottoscrittori, si tratti di blockchain *permissionless* o *permissioned*. In entrambi i casi, infatti, non esiste una garanzia di esistenza della struttura per tale periodo minimo.

È appena il caso di osservare come il venir meno della blockchain o la riduzione o compromissione dei nodi di conservazione esporrebbe l'investitore al rischio di vedere compromesso irrimediabilmente il proprio diritto, che esiste solo nel mondo digitale.

Open source

Un elemento che viene valutato positivamente dai partecipanti alle ICO è tradizionalmente la disponibilità di *software open source*. Questo infatti consente di effettuare verifiche indipendenti sul funzionamento dei programmi informatici e sulla corrispondenza tra quanto promesso nel *white paper* e nel resto della documentazione contrattuale in prosa legale con quanto previsto dal codice informatico.

Approccio regolamentare

Da tutto quanto sinora rappresentato, ed in particolare dall'ultimo punto, che appare forse il più importante, si possono trarre alcune considerazioni sull'approccio regolamentare da adottare.

In primo luogo, e come sempre in questi casi, l'approccio deve essere *technology neutral*.

In secondo luogo, risulta evidente come sia difficile fornire una volta per tutte elementi di riferimento in un quadro tecnologico e strutturale in continua e costante evoluzione.

Appare quindi raccomandabile rinviare la normazione a standard tecnici di settore e, in attesa della loro elaborazione da parte di organizzazioni internazionalmente riconosciute, ad apposite *opinion* che prendano in considerazione gli elementi tecnici e di *governance*, da mettere a disposizione unitamente al resto della documentazione resa disponibile col *white paper*.

Presidente Associazione Trusted Smart Contract

Prof. Avv. Fabio Maniori

Associazione Trusted Smart Contract

Via Castellanza, 11
20151 Milano – Italia
Codice Fiscale: 97824970152
info@trustedsmartcontract.org