SIA S.p.A.

via Francesco Gonin, 36 - 20147 Milano
t. +39 02 6084.1 - f. +39 02 6084 3920

www.sia.eu - info@sia.eu

capitale sociale euro 22.274.619,51 i.v.
r.i., c.f. e p. iva n. 10596540152
r.e.a. n. 1385874 di Milano

Filiali estere:
Belgicastraat 1 - B-1930 Zaventem - Belgio
Winthontlaan 200 - 3526 KV Utrecht - Paesi Bassi

Milano, 5 giugno 2019

CONSOB
Divisione Strategie Regolamentari
Via G.B. Martini, 3
00198 Roma
Italia

OSSERVAZIONI AL DOCUMENTO PER LA DISCUSSIONE DEL 19 MARZO 2019 – LE OFFERTE INIZIALI E GLI SCAMBI DI CRIPTO-ATTIVITÀ

Sommario

Introduzione 1
Il ruolo di SIA nel mercato dei capitali e l'esperienza nel campo dei registri distribuiti 1
Le osservazioni 2
Il contesto di riferimento 2
Conclusioni 4

Introduzione

Nell'ambito del presente documento il termine Documento per la Discussione fa riferimento al documento pubblicato da Consob il 13 marzo 2019.
Per semplicità di esposizione i termini blockchain, tecnologie basata su registri distribuiti e DLT sono utilizzati come sinonimi anche se tale uso è tecnicamente improprio.

Il ruolo di SIA nel mercato dei capitali e l'esperienza nel campo dei registri distribuiti

SIA è leader europeo nella progettazione, realizzazione e gestione di infrastrutture e servizi tecnologici dedicati alle Istituzioni Finanziarie, Banche Centrali, Imprese e Pubbliche Amministrazioni, nelle aree dei pagamenti, della monetica, dei servizi di rete e dei mercati finanziari.

In qualità di infrastruttura qualificata per i sistemi di pagamento e per i mercati finanziari, SIA è sorvegliata da Banca d'Italia e BCE.

SIA ha deciso nel 2016 di avviare una strategia pluriennale in ambito blockchain per mantenere anche nel lungo periodo il ruolo di leadership nei sistemi di pagamento e nel mercato dei capitali in un eventuale scenario di adozione pervasiva della tecnologia blockchain.

Nell'ambito di questa iniziativa SIA, anche attraverso un costante confronto con le autorità di regolamentazione alla cui vigilanza è sottoposta, ha potuto acquisire un'importante esperienza e consapevolezza riguardo alle implicazioni conseguenti all'utilizzo delle tecnologie blockchain in contesti fortemente regolamentati e con specifici requisiti di sicurezza e compliance quali sono i mercati finanziari.

Le osservazioni

Il contesto di riferimento

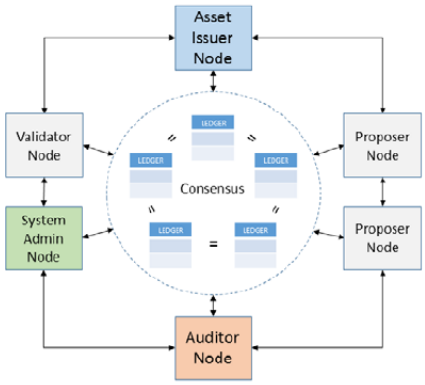
In coerenza con il proprio ruolo di provider tecnologico, SIA ritiene di poter contribuire alla discussione rispondendo al quesito 13 del Documento.

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

Nel rispondere al quesito riprendiamo le considerazioni riportate nel Documento (pag. 13):
"Tenendo conto dei diversi modello di business riscontrabili nella realtà, sarebbe opportuno prevedere che i sistemi di scambio in parola siano dotati di regole e procedure idonee per l'accesso e l'identificazione dei partecipanti in modo tale da rendere inutilizzabili – da parte dei relativi organizzatori che sono responsabili dei processi di ammissione – tecnologie basate su registri distribuiti nella forma c.d. permissionless (ossia con accesso libero anche anonimo) per gli aspetti relativi alla gestione dei processi di scambio e di trasferimento delle cripto-attività sul registro medesimo".
Volendo fornire un contributo alla discussione che non sia legato a specifiche tecnologie e soluzioni, essendo peraltro quello delle tecnologie dei registri distribuiti un settore in piena evoluzione, riteniamo utile fare riferimento al modello concettuale di struttura blockchain proposto dalla Bank of International Settlement, Commettee on Payments and Market Infrastructure nel documento "Distributed Ledger Technology in payment, clearing and settlement – an analytic framework" del febbraio 2017 da cui è tratta la seguente figura.

Figure 2

Ledger distributed across multiple nodes with varying roles or permissions



In funzione della presenza o meno di meccanismi di controllo dell'accesso alla struttura (c.d. permissioning) si possono configurare varie situazioni (la tabella è tratta dallo stesso documento):

Potential configurations of DLT arrangements — Table 1

Description of arrangement	One entity maintains and updates the ledger (for example, a typical FMI)	Only approved entities can use the service; entities can be assigned distinct restricted roles	Only approved entities can use the service; entities can play any role	Any entity can use the service and play any role
Operation of the arrangement	Single entity	Multiple entities		
Access to the arrangement	Restricted			Unrestricted
Technical roles of nodes	Differentiated		Not differentiated	
Validation and consensus	Within a single entity	Within a single entity or across multiple entities	Across multiple entities	

Nella tabella è evidenziata la combinazione di una tipica struttura permissionless.
Oltre al tema dell'accesso va evidenziato l'impatto sul ruolo dei nodi e sulla gestione dei meccanismi di consenso e validazione.
La caratteristica fondante delle tecnologie blockchain di interesse per il mercato è appunto l'introduzione della logica di consenso e validazione: una transazione fra due partecipanti alla struttura è validata e resa efficace non in forza dell'azione di una terza parte accettata come in questo ruolo dai partecipanti, ma da un meccanismo informatico e autonomo messo in atto da più soggetti logici (i nodi "validator" della figura).

Ora, se è vero che nel quadro di un sistema di scambio di cripto-attività è essenziale la sicura identificazione dei beneficiari dei diritti collegati alle cripto-attività stesse, è altrettanto essenziale, al fine della complessiva sicurezza e integrità del sistema, che siano noti i soggetti che partecipano all'attuazione dei meccanismi di consenso che rendono valide le transazioni.

Nell'ambito di una rete permissionless per natura stessa della rete questa identificazione è impossibile.

Riprendendo quindi il quesito e soffermandoci sul contributo richiesto circa le caratteristiche di sicurezza del registri distribuito, riteniamo utile ricordare la particolare declinazione del concetto di sicurezza che si adotta nel campo dei sistemi informativi:

- Disponibilità
- Integrità
- Confindenzialità

In ordine al primo punto è importante sottolineare che le reti permissionless esistenti si basano, per il proprio funzionamento, sull'azione sostanzialmente volontaria di soggetti che autonomamente decidono di partecipare alla rete per ottenerne un beneficio di diretto (è il caso dei miners di Bitcoin) o comunque per sfruttarne le funzionalità, contribuendo così al funzionamento complessivo della struttura.

Inoltre, lo sviluppo del codice informatico che è alla base del funzionamento della rete è gestito da comunità auto-organizzate di sviluppatori non sottoposti ad alcuna forma di sorveglianza, essendo a loro volta (sempre per la natura stessa della rete) anonimi (la creazione dello stesso Bitcoin è attribuita a Satoshi Nakamoto di cui ancora oggi si ignora se sia lo pseudonimo di una persona fisica o di un gruppo di sviluppatori).
Se è vero che a oggi nessuna delle reti permissionless esistenti è stata oggetto di casi di interruzione di servizio, è altrettanto vero che nel caso un evento di questo tipo si manifestasse, nessuno dei soggetti titolari delle cripto-attività registrate sul registro distribuito, come anche i soggetti gestori dei sistemi di scambio, potrebbe identificare una controparte a cui rivolgersi per la risoluzione del problema.
Questa assenza di "liability" nell'elemento strutturalmente fondante comporta un rischio in carico agli investitori molto difficilmente mitigabile.
Se investitori professionali con alta propensione al rischio e elevata competenza circa i meccanismi di funzionamento delle tecnologie a registri distribuiti di tipo permissionless possono prendere una decisione consapevole in merito a tali rischi, non lo stesso si può probabilmente dire della generica platea degli investitori potenziali, specie se un'offerta di questo tipo fosse rivolta alla clientela retail.
Stesse considerazioni possono applicarsi relativamente all'integrità. Come qualunque prodotto informatico, anche il codice sottostante le tecnologie blockchain, in particolare nel caso (peraltro altamente probabile) che i meccanismi di scambio siano implementati attraverso c.d. Smart Contract, è soggetto ad errori che possono portare a una effettiva perdita delle cripto-attività (paradigmantico in tal senso il caso "The DAO"), anche in questo caso in assenza di una controparte responsabile delle misure di mitigazione preventiva e di ripristino.

Considerazioni analoghe sono espresse dal Securities and Market Stekeholder Group di ESMA (documento pubblicato il 19 ottobre 2018 "Own Initiative Report on Initial Coin Offering and Crypto-Assets") e dalla Banca d'Italia (Questioni di Economia e Finanza, n° 484 del marzo 2019). In particolare da quest'ultimo documento citiamo (pag. 7):

"Pre-condizione per un uso estensivo della DLT nel sistema bancario e finanziario e nel sistema dei pagamenti sono: robustezza tecnologica e di governance, interoperabilità, scalabilità, controllabilità da parte del gestore e, ove necessario, del regolatore."

Quanto al requisito di confidenzialità, la natura di una rete permissionless rende sicuramente più difficoltoso il soddisfacimento di questo requisito.

Infine, guardando alle esperienze più recenti sul mercato, si segnala che SIX Swiss Exchange, la principale borsa valori svizzera, ha scelto una piattaforma permissioned (segnatamente R3 del consorzio Corda) per sviluppare le proprie iniziative blockchain.

Conclusioni

Volendo trarre delle conclusioni in funzione di quanto sopra illustrato, riteniamo che la blockchain sottostante a un sistema di scambio di cripto-attività, in particolare considerando uno scenario di adozione alla scala di un mercato finanziario, non possa prescindere da queste caratteristiche:

1. Modello di accesso permissioned
2. Chiara struttura di governance con identificazione certa dei soggetti coinvolti a vario titolo nel funzionamento dell'infrastruttura e delle relative responsabilità. Particolare attenzione deve essere posta al/i soggetto/i titolare della responsabilità di rilascio dei diritti di accesso alla rete e del soggetto/i presso cui sono implementati i meccanismi di consenso.
3. Topologia architetturale tale da rientrare integralmente entro la giurisdizione nazionale o almeno europea e pertanto al di fuori dalle possibilità di intervento e imposizione da parte di autorità extra europee
4. Possibilità di distribuzione geografica dei nodi e che i nodi geograficamente distribuiti possano assumere le differenti funzioni (proposer, validator, …)

5. Capacità di gestire volumi di transazioni a scala di mercato finanziario
6. Architettura tecnologica conforme agli standard e alle best practice in materia di sicurezza informatica
7. Possibilità per un ente regolatore o altra autorità competente di svolgere attività di ispezione anche a livello di codice.