lacittadinanzaeuropea online
Rivista di studi e documentazione sull'integrazione europea
ISSN 2785-4183
lceonline 2/2022 (*www.lceonline.eu*)

Il problema della rilevanza giuridica dell'errore nella decisione dell'oracolo della blockchain(*)

Laura VAGNI*

Sommario: 1. La *blockchain* come sistema senza errori: una premessa. **2.** Il problema dell'oracolo. **3.** La presupposizione: l'oracolo non mente. **4.** Una recente decisione della *Court of Appeal* di Singapore. **5.** La fiducia basata sul consenso dei nodi e le brecce del mondo reale: le sfide per il giurista

1. La *blockchain* come sistema senza errori: una premessa

La tecnologia *blockchain*, inizialmente applicata alle transazioni finanziarie e, in particolare, allo scambio di criptovalute, ha avuto in anni più recenti ampia diffusione in altri ambiti. Registri distribuiti sono stati sperimentati per l'esecuzione di operazioni nel settore assicurativo, agroalimentare, bancario, dei trasporti, in generale nelle catene del valore[1]. Progetti di sperimentazione della tecnologia *blockchain* sono presenti anche nella pubblica amministrazione, per la realizzazione di sistemi di *governance* più sicuri ed efficienti[2].

La diffusione di questa tecnologia è dovuta soprattutto alla possibilità di eliminare il rischio di errore (*single point of failure*) nell'esecuzione delle diverse operazioni all'interno della catena, attraverso la loro verifica, approvazione e archiviazione da parte dei nodi che compongono il registro distribuito[3]. Il funzionamento della *blockchain*, infatti, non richiede alcuna forma d'intermediazione e, allo stesso tempo, rende completamente sicure e affidabili le operazioni eseguite, non consentendo forme di alterazione o modifica delle stesse. Queste caratteristiche hanno determinato il successo della *blockchain* applicata agli *smart contracts*, garantendone l'auto-esecuzione e l'immutabilità: le clausole dello *smart contract*, codificate secondo formule condizionali (*if, then*), sono eseguite automaticamente, al verificarsi di certe condizioni, indipendentemente da chi conclude il contratto e in quale momento, e sono immodificabili una volta avvenuta la registrazione da parte dei nodi della catena. L'esecuzione degli *smart contracts* è compatibile con il completo anonimato dei partecipanti alla blockchain e non richiede alcuna forma di intermediazione tra le parti contraenti. Si tratta di un sistema c.d. *trustless*, che sembra superare completamente la necessità di una fiducia negoziale tra le parti, dato che la conclusione e l'esecuzione del contratto non sono influenzate da tutti quegli eventi che incidono sulla relazione fiduciaria tra contraenti, con riflessi sul rapporto giuridico.

(*) Viene qui riprodotto con modifiche e aggiunte il testo dell'intervento al seminario internazionale a conclusione del progetto di ricerca DANT- *Decisions and new Technologies*, finanziato dal Dipartimento di eccellenza, Dipartimento di Giurisprudenza, Università di Macerata, sul tema "L'errore nella decisione nell'era dell'intelligenza artificiale", Macerata, 24 settembre 2021.

* Professore ordinario di Diritto privato comparato, Università di Macerata.

[1] Per un'analisi delle molteplici applicazioni di questa tecnologia cfr., J. Prieto, A. Partida, P. Leitão, A. Pinto (eds.), *Blockchain and applications*, *3rd International congress*, Cham (Svizzera), 2022, *passim*.

[2] *Ex multis* cfr. E. Tan, S. Mahula, J. Crompvoets, *Blockchain governance in the public sector: A conceptual framework for public management*, in *Government information quarterly*, 39(1)/2022, p. 101625.

[3] Per un'analisi, in prospettiva giuridica, del funzionamento della *blockchain* applicata agli *smart contracts*, cfr. in italiano A. Stazi, *Automazione contrattuale e "contratti intelligenti". Gli smart contracts nel diritto comparato*, Torino, 2019, p. 99 ss.; C. Pongibò, *Il diritto comparato e la blockchain*, Napoli, 2020, p. 42 ss.

L'esecuzione degli *smart contracts* tramite la tecnologia *blockchain*, tuttavia, non è completamente immune da forme *latu sensu* di malfunzionamento. Una delle principali problematiche riguarda l'attacco di *hackers*: si pensi alla serie di attacchi subiti da Ethereum[4], che ha determinato biforcazioni della *blockchain* (*forks*), causando la disconnessione di alcuni nodi, o la formazione di catene basate su falsi dati, più lunghe della catena originale, compromettendo la verifica delle operazioni e inducendo in errore alcuni nodi[5]. In altri casi, sono stati sfruttati i difetti di programmazione di *smart contracts* per compiere operazioni a detrimento dei partecipanti alla catena[6].

Simili eventi hanno richiamato l'attenzione della dottrina sulla modificabilità-corruttibilità di questa tecnologia, aprendo una riflessione sul modello di fiducia promosso dalla *blockchain*[7]: da un lato, infatti, l'auto-esecuzione e l'assenza d'intermediazione che caratterizzano gli *smart contracts* sembrano completamente superare il problema dell'affidamento tra le parti di una transazione; dall'altro lato, emerge che la "assenza di fiducia" (*trustless*), basandosi sull'idea di immodificabilità-incorruttibilità del sistema, vacilla nel caso del verificarsi di rischi, seppure rari, che la compromettano. Nelle pagine che seguono si cercherà di riflettere su questo tema, concentrando l'attenzione sul c.d. problema dell'oracolo e sulle implicazioni giuridiche di errori o malfunzionamenti ad esso riconducibili.

2. Il problema dell'oracolo

I nodi della *blockchain* eseguono operazioni e registrano dati che sono stati immessi nel *network*. La catena, di per sé, non ha accesso a dati *off-chain*. Lo sviluppo di questa tecnologia e il suo utilizzo in diversi settori dipende, quindi, anche dallo scambio di dati e dalla comunicazione d'informazioni tra la *blockchain* e il mondo reale. Ciò avviene attraverso gli 'oracoli'. Il termine evoca l'idea mitologica di rivelazioni profetiche ispirate da una divinità e comunicate agli uomini per il tramite di oracoli, veritieri ma spesso enigmatici, ponendo il problema della loro interpretazione[8].

Nel linguaggio informatico e, specificamente, con riguardo alla tecnologia *blockchain*, lo stesso termine 'oracolo' è utilizzato con un significato diverso, ma ugualmente riferito alla comunicazione, in questo caso tra il sistema virtuale della *blockchain* e il mondo esterno alla catena[9]. L'oracolo rappresenta un elemento di collegamento della *blockchain* con dati *off-chain*, consentendo l'immissione all'interno del sistema o il trasferimento all'esterno d'informazioni e dati. Anche questo processo

[4] Ethereum è una delle principali piattaforme che utilizza la tecnologia *blockchain* per la conclusione ed esecuzione di *smart contracts* (https://ethereum.org/it/what-is-ethereum/). Cfr. *infra*, para. 2.

[5] K. Werbach, *The Siren Song: Algorithmic Governance by Blockchain*, in K. Werbach (ed.), *After the Digital Tornado: Networks, Algorithms, Humanity*, Cambridge, 2020, p. 215 ss., in particolare p. 226 ss.

[6] Un esempio emblematico è costituito dalla vulnerabilità di un programma di una start up (DAO) che gestiva un fondo di investimento attraverso uno *smart contract* eseguito su Ethereum. Il programma conteneva una falla che è stata sfruttata attraverso l'utilizzo di una funzione ricorsiva per effettuare continui acquisti di Ether, non consentendo al sistema una verifica, con sufficiente velocità, della disponibilità monetaria per svolgere le transazioni. L'operazione ha consentito di prosciugare i fondi degli utenti con una perdita di milioni di Ether. L'evento ha indotto Ethereum ad operare una *hard fork* della *blockchain*, con effetti retroattivi e conseguente modificazione delle operazioni che erano stare registrate. Cfr. R. Morrison, N. Mazey, S. Wingreen, *The DAO controversy: the case for a new species of corporate governance?*, in *Policy and practice reviews*, 27 maggio 2020, (https://www.frontiersin.org/articles/10.3389/fbloc. 2020.00025/full) che evidenzano come DAO si basava su un modello di *corporate governance* completamente affidato alla tecnologia del registro distribuito e svolgono considerazioni critiche sull'opportunità che alcune forme di organizzazione siano completamente decentralizzate.

[7] K. Werbach, *The Siren Song ecc.*, cit., p. 222.

[8] Il legame tra la profezia dell'oracolo e il problema interpretativo è testimoniato da una pluralità di fonti letterarie. Nella "Apologia di Socrate" di Patone (traduzione dal greco a cura di M. C. Pievatolo, in *Bollettino telematico di filosofia politica*, 2005, para. 21b), si racconta che Cherofonte chiese all'oracolo di Delfi se ci fosse qualcuno più sapiente di Socrate. Ricevuto il responso dell'oracolo, Socrate ritenne che il dio non mentisse, tuttavia si interrogò sulle sue parole e le sottopose ad esame critico: "Che cosa vuol dire il dio? Che cosa nasconde il suo parlare enigmatico?".

[9] Già prima dello sviluppo della *blockchain*, il termine 'oracolo' si trova usato nell'ambito dell'ingegneria del *software*, per stabilire se un certo test ha successo. L'oracolo fornisce dei dati che vengono usati come paragone per valutare il corretto risultato del test.

implica una forma di interpretazione-codificazione dei dati, che avviene attraverso diversi metodi, dipendenti dalla tipologia e dalla fonte del dato.

In letteratura gli oracoli sono diversamente classificati: a seconda della provenienza dei dati e delle informazioni trasferite possono avere natura *hardware*, *software*, ma anche umana[10]. Nel caso di oracolo *hardware*, i dati trasmessi dall'oracolo sono prodotti dal mondo fisico: ad esempio, un sensore che rileva la temperatura di un luogo o di un materiale per immettere il dato in uno *smart contract*, che eseguirà specifiche operazioni sulla base del dato trasmesso. Nell'oracolo *software*, invece, i dati provengono da fonti *on-line*, quali informazioni tratte da specifici siti internet. Non sono infrequenti, inoltre, oracoli umani, i quali possono immettere nel sistema anche dati dipendenti da valutazioni o interpretazioni di altri dati.

Parte della dottrina ha osservato l'utilità che gli oracoli di natura umana potrebbero avere per lo sviluppo degli *smart contracts*, assicurando una maggiore rispondenza del regolamento contrattuale alle vicende che possono riguardare il reale svolgimento del rapporto tra i contraenti[11]. Si pensi, ad esempio, alla possibilità di prevedere una clausola di forza maggiore nello *smart contract* o altre ipotesi di scioglimento del vincolo, che si attiverebbero automaticamente attraverso la comunicazione da parte dell'oracolo del verificarsi di determinati eventi sopravvenuti alla conclusione del contratto. In tal modo, l'esecuzione del contratto verrebbe a dipendere da un dato proveniente dall'esterno della catena e frutto dell''interpretazione' affidata a un oracolo, come ad esempio la valutazione della imprevedibilità e non imputabilità dell'evento al debitore, dell'irresistibilità dell'evento, necessarie per 'attivare' una clausola di forza maggiore.

Gli oracoli costituiscono delle finestre del sistema virtuale sul mondo reale, dalle quali è possibile introdurre all'interno dell'architettura deterministica della *blockchain* anche informazioni non deterministiche, con la conseguente necessità di verificare l'affidabilità dell'oracolo e la veridicità dei dati immessi. Si parla in tal senso di "problema dell'oracolo".

L'oracolo rappresenta un potenziale punto di rottura del sistema *trustsless* della *blockchain*, compromettendo quella "assenza di fiducia" (*trustless*) che vuole essere l'innovazione più importante di questa tecnologia. Un'esecuzione contrattuale automatica basata su un errore dell'oracolo, infatti, sarà comunque registrata da tutti i nodi e diverrà una realtà virtuale immodificabile, ma falsata.

L'utilizzo degli oracoli e i rischi che ne discendono, in termini di compromissione dei dati, hackeraggio, malfunzionamento o corruzione, hanno richiamato l'attenzione della dottrina, al fine di indagare quale struttura e funzionamento debbano caratterizzare l'oracolo per essere 'affidante'[12]. In questa prospettiva, alcuni autori propongono di utilizzare oracoli strutturati secondo un registro distribuito, riproducendo per gli oracoli il sistema *trustless* delle *distributed ledger technologies*[13]. Si tratta, tuttavia, di una strada non sempre percorribile, almeno per non tutti i tipi d'informazioni da trasferire ad uno *smart contract*.

Da un punto di vista giuridico, il tema fa emergere una pluralità di interrogativi, relativi alla natura giuridica dell'oracolo, alla rilevanza giuridica di un errore che incida sulla veridicità dei dati

---

[10] B. Curran, *What Are Oracles? Smart Contracts, Chainlink & "The Oracle Problem"* (https://blockonomi.com/oracles-guide); A. Beniiche, *A Study of Blockchain Oracles*, arXiv:2004.07140 [cs.CR], (https://arxiv.org/pdf/2004.07140.pdf).

[11] E. Tjong Tjin Tai, *Force Majeure and Excuses in Smart Contracts*, in *Tilburg private law working paper series*, 10/2018, p. 1 ss.; Id., *Challenges of Smart Contracts. Implementing Excuses*, in L.A. Di Matteo, M. Cannarsa, C. Pongibò (cur.), *The Cambridge Handbook of Smart Contracts*, *Blockchain Technology and Digital Platform*, Cambridge, 2020, p. 83 ss.

[12] Gli errori che potrebbero compromettere il dato trasmesso dall'oracolo sono diversi, anche in ragione del carattere privato o pubblico della *blockchain*. La dottrina ha sottolineato che il rischio di un errore indotto dall'oracolo è maggiore nelle *blockchain* private. Si pensi ad una *blockchain* per la tracciabilità di un prodotto in una catena di fornitura. I dati e le informazioni riguardo a quel prodotto che sono *off-chain* dipendono da oracoli che a loro volta potrebbero essere gestiti dal leader della catena, in modo tale da selezionare informazioni più favorevoli allo sviluppo di un certo tipo di business. Si parla in tal caso anche del problema "dell'ultimo miglio", cfr. A. Sulkowski, *Blockchain, business supply chains, sustainability, and law: the future of governance, legal frameworks, and lawyers?*, in *Delaware Journal of Corporate Law*, 43(2)/2019, p. 303 ss., in particolare p. 307.

[13] Cfr, A. Beniiche, *A Study of Blockchain*, cit., pp. 3-4; A. Pasdar, Z. Dong, Y.C. Lee, *Blockchain Oracle Design Patterns*, arXiv:2106.09349 (https://arxiv.org/abs/2106.09349).

trasmessi alla catena, all'imputabilità dell'evento dannoso, alle possibili tutele del soggetto danneggiato da una operazione basata su un errore del genere, che non trovano ancora una chiara soluzione[14].

La tecnologia *blockchain* consente alcuni tipi d'intervento sulla catena, volti a correggere le registrazioni per riallineare le transazioni della catena con il dato reale, in caso di errori o malfunzionamenti dell'oracolo. Così, Ethereum, una delle più diffuse piattaforme decentralizzate utilizzata per la conclusione ed esecuzione di *smart contracts*, contempla la possibilità di attivare l''autodistruzione' del contratto e la sua rimozione dalla catena[15]. L'applicazione della funzione richiede, tuttavia, una modifica del codice da parte di chi ha creato e inserito lo *smart contract* all'interno della *blockchain* e determina la cancellazione del contratto. Si tratta, quindi, di un rimedio che non sempre soddisfa gli interessi delle parti contraenti, le quali potrebbero invece voler conservare il contratto[16]. Si sta studiando anche la programmazione di altre funzioni di modica del contenuto del codice informatico, sulla base ad esempio di una decisione giurisprudenziale che riconosca un determinato rimedio alla parte pregiudicata da un malfunzionamento del sistema. In tal caso, l'esito della decisione dovrebbe essere incorporato all'interno della catena tramite un oracolo, con la necessità di una verificazione del dato e del controllo dell'affidabilità[17]. Occorre inoltre considerare che qualsiasi modifica della catena si pone come eccezione all'idea di immodificabilità delle operazioni, che la tecnologia *blockchain* mira ad assicurare. Gli strumenti offerti dalla tecnologia, pertanto, non sembrano ancora apprestare soluzioni adeguate alla molteplici e diverse disfunzioni che potrebbero verificarsi, seppur in ipotesi rare, a seguito di un malfunzionamento della comunicazione tra *blockchain* e mondo esterno. Le implicazioni giuridiche di queste operazioni di correzione delle registrazioni della catena, inoltre, restano in gran parte inesplorate e inducono ad interrogarsi sulla relazione tra la regolazione della catena virtuale basata sulla tecnologia e la regolazione giuridica del rapporto (reale) tra parti di uno *smart contract*.

3. La presupposizione: l'oracolo non mente

Nel tentativo di lettura del problema dell'oracolo attraverso le categorie giuridiche, ci si interroga sulla possibilità di ricorrere al diritto dei contratti e ai rimedi contrattuali per apprestare tutela alla parte di uno *smart contract*, che subisce un danno derivante da un errore o malfuzionamento riconducibile all'oracolo[18]. In questa prospettiva, si pone anche il problema d'individuare a quali regole contrattuali fare riferimento: la *blockchain* opera in una dimensione spaziale, che prescinde dalle distinzioni tra sistemi giuridici e diritti nazionali, con la conseguente difficoltà d'individuazione del diritto applicabile. Le regole del diritto internazionale privato, basate sull'idea del conflitto di

[14] G. Caldarelli, *Understanding the Blockchain Oracle Problem: a Call for Action*, in *Information*, 11/2020, p. 509 ss.; Id., *Real-world blockchain applications under the lens of the oracle problem. A systematic literature review*, *IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD)*, 2020, pp. 1-6, (https://ieeexplore.ieee.org/ document/ 9380598).

[15] Si tratta della funzione c.d. "Kill", cfr. B. Marino, A. Juels, *Setting Standards for Altering and Undoing Smart Contracts*, in *Rule Technologies. Research, Tools, and Application*, Cham (Switzerland), 2016, p. 151 ss.

[16] R. Herian, *Smart Contracts: a Remedial Analysis*, in *Information & Communications Technology Law*, 30(1)/2021, p. 17 ss., in particolare p. 31.

[17] Cfr. M. Durovic, A. Janssen, *Formation of Smart Contracts Under Contract Law*, in *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platform*, cit., p. 74.

[18] La discussione concerne la stessa riconducibilità degli *smart contracts* alle categorie tradizionali del diritto dei contratti. Senza poter ricostruire la copiosa letteratura in materia, si rinvia per un'analisi dei principali orientamenti in italiano a A. Stazi, *Automazione contrattuale ecc.*, cit., p. 143 ss.; v. anche L. Procopie, *Are Smart Contracts Actually Contracts? How Smart Contracts Can Work Globally*, in *Journal of International Banking Law and Regulation*, 36(1)/2021, p. 25 ss.; A. Savelyev, *Contract Law 2.0: 'Smart' Contracts as the Beginning of the End of Classic Contract Law*, in *Information & Communications Technology Law*, 26(2)/2017, p. 116 e in particolare p. 128 ss.

leggi di ordinamenti geograficamente intesi, non sempre sono utili per rispondere al quesito in modo effettivo[19].

Con le necessarie cautele dovute agli elementi d'incertezza richiamati, l'errore dell'oracolo che si riflette sull'esecuzione di uno *smart contract*, da qualunque causa dipenda, non sembra riconducibile alla figura dell'errore-vizio, mancando elementi distintivi di quest'ultimo: si tratta di un errore che non riguarda la sfera giuridica di una delle parti contrattuali; né esso incide sulla volontà dei contraenti; inoltre non necessariamente è un errore inerente la formazione del contratto. Ancor meno appare invocabile l'istituto della condizione[20]. L'oracolo può trasmettere alla catena dati e informazioni di diversa natura: si pensi ad un contatore che comunica allo *smart contract* i consumi di energia, per la determinazione del prezzo della bolletta. Comunicazioni di questo genere non appaiono qualificabili come condizioni giuridiche.

L'esecuzione dello *smart contract*, che prevede dati trasmessi da un oracolo, presuppone il corretto funzionamento dell'oracolo e l'affidabilità dei dati immessi nella catena.

In termini generali si può affermare che tutte le operazioni che si svolgono nella catena si basano sul presupposto: "l'oracolo non mente". Se l'oracolo mente (a causa di un malfunzionamento del sistema) viene meno un elemento esterno al contratto, relativo all'affidabilità dell'oracolo, che seppur non richiamato dalle parti nel contratto, può incidere sulla sua conclusione o esecuzione, con esiti non voluti dalle parti. L'errore dell'oracolo, osservato da una prospettiva contrattuale, potrebbe allora essere assimilato al venir meno della presupposizione del contratto. Si tratta solo di un'ipotesi interpretativa, che ci si riserva di approfondire con ulteriori studi, ma che sembra trovare qualche conforto nel recente parere della *English Law Commission* indirizzato al Governo, dal titolo *Smart legal contracts*[21]. Il parere raccoglie gli esiti di una *call for evidence* pubblicata dalla *Law Commission* nel 2020 con la finalità di avviare un processo di revisione del diritto dei contratti in Inghilterra e Galles, così da facilitare l'uso e la diffusione degli *smart contracts* e chiarirne le ricadute giuridiche[22]. Ciò con l'ulteriore scopo di aumentare la competitività delle regole contrattuali nazionali e facilitarne la scelta da parte degli operatori nel commercio internazionale.

In questo quadro, la *Law Commission* analizza anche il problema dell'oracolo, valutando la possibile qualificazione giuridica di un suo malfunzionamento o, in generale, del verificarsi di una trasmissione di dati erronei all'interno del sistema *blockchain*. Si richiama l'attenzione sulla necessità delle parti di prevedere, al momento della determinazione del regolamento contrattuale, l'allocazione di simili rischi. Ciò potrebbe avvenire, ad esempio, stipulando un contratto *off-chain*, collegato allo *smart contract*, nel quale le parti stabiliscono lo scioglimento del loro rapporto contrattuale per forza maggiore nel caso di errore, corruzione o malfunzionamento dell'oracolo[23]. In assenza di una espressa previsione delle parti dell'errore dell'oracolo, sembra invece più difficile ritenere che il contratto contenga una clausola implicita, in base alla quale "la parte è liberata dall'adempimento nel caso in cui l'oracolo inizi a trasmettere alla catena informazioni errate"[24].

---

[19] F. Guillaume, *Aspects of Private International Law Related to Blockchain Transactions*, in D. Kraus, T. Obrist, O. Hari (eds.), *Blockchain, Smart Contracts, Decentralised Autonomous Organizations and the Law*, Cheltenham, 2019, p. 61 ss.

[20] L'apposizione di condizioni sospensive o risolutive agli *smart contracts* è potenzialmente ammissibile, tuttavia la dottrina ha evidenziato le problematiche relative alla transazioni eseguite in catena in pendenza di condizione risolutive o prima dell'avveramento della condizione sospensiva. L'immodificabilità delle transazioni, una volta avvenuta la loro registrazione, appare infatti difficilmente conciliabile con la retroattività degli effetti discendenti dal verificarsi della condizione. Per i primi riferimenti in punto cfr. A. Stazi, *Automazione contrattuale ecc.*, pp. 177-178.

[21] English Law Commission, *Smart legal contracts*, *Advice to Government*, London, 2021, n. 401, CP 563, (https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf).

[22] English Law Commission, *Smart contracts*, *Call for evidence*, *December* 2020, (https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2020/12/201216-Smart-contracts-call-for-evidence.pdf).

[23] English Law Commission, *Smart legal contracts*, cit., p. 25.

[24] *Ibid.*, p. 95, para. 4.87, citando gli studi di H. Beale sugli *implied terms*. La *Law Commission* esprime considerazioni critiche al riguardo, evidenziando l'interpretazione restrittiva a cui generalmente sono sottoposte le clausole implicite del contratto, in base alla quale la ragionevolezza della clausola non è di per sé sufficiente a considerarla voluta dalla parti se non esplicitata nel regolamento contrattuale.

Nella *call for evidence* del 2020, sopra richiamata, la *Law Commission* valutava la possibilità di uno scioglimento del contratto a seguito dell'errore di comunicazione di dati esterni al sistema virtuale. La decisione errata dell'oracolo determina in realtà il venir meno di un elemento esterno al contratto che le parti presuppongono – l'oracolo non mente – con l'effetto che il contenuto del contratto potrebbe modificarsi in qualcosa di sostanzialmente diverso rispetto a quanto contemplato inizialmente dai contraenti[25]. Nella *call for evidence* s'ipotizzava l'applicazione in questi casi della *doctrine of frustration*[26], che consente lo scioglimento del contratto se, per eventi sopravvenuti alla conclusione del contratto, quest'ultimo diventa impossibile o il suo contenuto è sostanzialmente diverso rispetto a quello voluto dalle parti. L'ipotesi apre ad una serie di problematiche di ancora difficile soluzione.

La tipologia di dati trasmessi da un oracolo allo *smart contract* può essere molto varia e così anche i vizi che possono intervenire nella comunicazione tra sistema virtuale e realtà esterna per il tramite dell'oracolo. Non sempre, a fronte di un *input* errato dell'oracolo, viene meno una presupposizione del contratto idonea a determinarne lo scioglimento: l'errore potrebbe incidere su una prestazione accessoria o determinare semplicemente una maggiore onerosità per la parte, senza incidere sull'alea normale del contratto. Occorre, inoltre, valutare se e come l'errata decisione dell'oracolo e il suo rilievo giuridico possano tradursi nel sistema virtuale in una modificazione delle registrazioni della catena. Ciò dipenderà anche dalla possibilità di comunicare, sempre attraverso un oracolo, la correzione dell'errore alla catena.

La valutazione del rilievo dell'errore dell'oracolo, in conclusione, dipende da una serie di circostanze che difficilmente possono essere codificate operando una valutazione preliminare, ma spesso richiedono un'interpretazione *ex post*, con la possibilità di riemersione di problemi interpretativi che gli *smart contracts* intendono invece superare. Il rilievo giuridico del presupposto "l'oracolo non mente", infatti, dipenderà dal difetto o errore di comunicazione che in concreto si è realizzato e dalla sua incidenza sul regolamento contrattuale. In questo scenario, caratterizzato da questioni ancora non chiaramente definite da parte della dottrina, il dato che emerge come certo è che la tutela dell'affidamento delle parti nella decisione nell'oracolo è determinante per il futuro sviluppo della tecnologia *blockchain*.

4. Una recente decisione della *Court of Appeal* di Singapore

Tenendo sullo sfondo le problematiche precedentemente richiamate, sembra utile soffermarsi su una recente decisione della *Court of Appeal* (della Repubblica) di Singapore che, pur riguardando un tema diverso, può fornire qualche utile indicazione a comprendere le ricadute giuridiche del problema della verificazione dei dati comunicati da un oracolo ad uno *smart contract*[27]. Il caso riguardava contratti di acquisto di criptovalute conclusi tra due società attraverso una piattaforma gestita dalla società Quoine. La conclusione dei contratti avveniva automaticamente, attraverso proposte di vendita e di acquisto di Ether e Bitcoin, formulate da algoritmi di *trading*[28]. Quest'ultimi assumevano decisioni sulla base dei prezzi e del volume del mercato della piattaforma, pertanto il loro funzionamento dipendeva dalla liquidità degli strumenti negoziati nel mercato di riferimento.

[25] Cfr. English Law Commission, *Smart Contracts, Summary of smart contracts call for evidence*, 17 *December* 2020, p. 17 (https://www.lawcom.gov.uk/project/smart-contracts/).

[26] *Ibid.* La riconducibilità della *doctrine of frustration* alle categorie del diritto civile degli ordinamenti di *civil law* è solo parziale, in particolare la regola non trova perfetta corrispondenza nell'istituto italiano della impossibilità sopravvenuta. Cfr. English Law Commission, *Smart legal contracts*, cit., p. 149, para. 5. 161.

[27] *Quoine Pte Ltd v. B2C2,* [2020] SGCA(I) 02.

[28] Si tratta di un algoritmo capace di prendere posizioni su un determinato mercato, elaborando un grande numero di dati relativi alle quotazioni dei prodotti e compiendo delle vere e proprie scelte in base alle strategie configurate sulla base di un modello matematico. Nel caso di specie la Corte citava la definizione di A. Chaboud et all., *Rise of the Machines: Algorithmic Trading in the Foreign Exchange Market*, *International Finance Discussion Papers*, 29 *September* 2009, p. 1 (http://www.federalreserve.gov/pubs/ifdp/2009/980/ifdp980.pdf).

La società Quoine, che gestiva la piattaforma, era anche il principale operatore del mercato e assicurava la liquidità necessaria all'uso degli algoritmi di *trading*, attraverso continue proposte di vendita e acquisto che erano formulate a loro volta mediante un programma (*Quoine program*). Il programma attingeva ai prezzi di cambio delle criptovalute in mercati esterni alla piattaforma ed elaborava su questa base i prezzi di cambio di criptovalute nella piattaforma. Le quotazioni dei prezzi in piattaforma dipendevano quindi dalle comunicazioni dei tassi di cambio su altri mercati[29]. Il 13 aprile 2017, il gestore della piattaforma eseguiva degli aggiornamenti di password di alcuni sistemi operativi, a seguito dei quali, tuttavia, per un periodo di tempo era stato interrotto l'accesso ai dati esterni alla piattaforma da parte del programma. Ciò determinava, a cascata, una falsificazione del tasso di cambio delle criptovalute stabilito attraverso il sistema di algoritmi: il calcolo algoritmico certamente era esatto, ma la scarsità dei dati presenti in piattaforma determinava una diminuzione di liquidità del mercato, tale da generare offerte di vendita di criptovalute a prezzi abnormi rispetto a quelli di altri mercati.

La società B2C2 era un utente della piattaforma, che a sua volta utilizzava una strategia di acquisto e vendita di criptovalute basata su un algoritmo di *trading*, prevedendo quindi l'automatica accettazione delle migliori offerte contrattuali presenti nel pannello di *trading* della piattaforma. La società concludeva così automaticamente 13 contratti di vendita di Ether per Bitcoin con altre due società, ad un tasso di cambio superiore di ben 250 volte il valore di mercato.

Il gestore della piattaforma, informato del malfunzionamento della comunicazione tra piattaforma e mercati esterni, annullava le transazioni, ma la società B2C2 agiva in giudizio, lamentando l'inadempimento del contratto stipulato tra gestore e utente, che non prevedeva la possibilità di Quoine di annullare le transazioni avvenute tra utenti della piattaforma.

La controversia su cui era chiamata a decidere la *Court of Appeal* non riguardava, pertanto, gli *smart contracts* conclusi tra utenti della piattaforma, ma il diverso contratto tra B2C2 e il gestore Quoine. Quest'ultimo contratto prevedeva una clausola c.d. d'immodificabilità, secondo la quale "una volta che un ordine è stato inserito e comunicato attraverso la piattaforma esso diventa immodificabile"[30]. Quoine riteneva, tuttavia, che tutti i contratti conclusi in piattaforma prevedessero una clausola implicita, che consentiva al gestore della piattaforma di cancellare le transazioni eseguite sulla base di un tasso di cambio abnorme, dovuto ad un errore tecnico o di sistema o ad altro malfunzionamento della piattaforma[31]. Il gestore della piattaforma agiva quindi in giudizio richiedendo l'annullamento dei 13 contratti viziati da errore.

La Corte respingeva la domanda, escludendo la riconducibilità del malfunzionamento del programma (*Quoine program*) all'errore contrattuale: l'anonimato delle parti contraenti e l'automaticità del meccanismo di formazione del consenso non consentivano di qualificare l'errore come vizio della volontà; mancava in particolare l'elemento della riconoscibilità dell'errore da parte di B2C2, che non aveva la possibilità di conoscere la controparte e valutare le condizioni contrattuali, determinate sulla base di operazioni algoritmiche[32]. Non poteva parlarsi neanche di un errore comune alla parti, perché non si rinveniva una comune intenzione di concludere i contratti al tasso di cambio del mercato. Al contrario, B2C2 aveva programmato l'algoritmo di *trading* per effettuare gli acquisti al prezzo minimo praticato sulla piattaforma[33].

La falsificazione dei tassi di cambio delle criptovalute non era dovuta ad un errore dell'algoritmo, ma all'interruzione della comunicazione tra il *network* e i mercati esterni. Le parti avevano errato sul

[29] Si trattava di un sistema molto complesso, che prevedeva anche una correzione del mercato mediante l'immissione di prezzi virtuali, generati da algoritmo, qualora il livello di liquidità scendesse sotto una certa soglia. Cfr. *Quoine Pte Ltd v. B2C2,* cit., para. 18.

[30] Cfr. *Quoine Pte Ltd v. B2C2*, cit., para. 22. Le condizioni generali di contratto predisposte da Quoine stabilivano una *Irreversible Action Clause* secondo la quale "[…] once an order is filled, you are notified via the Platform and such an action is irreversible". B2C2 richiamava la vincolatività della clausola per sostenere l'impossibilità di Quoine di intervenire sui contratti conclusi tra utenti.

[31] Cfr. *Quoine Pte Ltd v. B2C2*, cit., para. 35.

[32] *Ibid.*, para. 42.

[33] *Ibid.*, para. 129.

presupposto delle loro contrattazioni: "[il malfunzionamento] può plausibilmente essere considerato un errore sul presupposto, sulla base del quale sono stati fatti gli ordini di acquisto, ma in nessun caso può essere ritenuto un errore sulle clausole che i contratti contenevano o avrebbe dovuto contenere"[34]. La Corte specificava ulteriormente: "In effetti, l'errore in questo caso è consistito precisamente in un erroneo presupposto da parte delle controparti su come la piattaforma funzionava. In altri termini, essi credevano effettivamente che la piattaforma non sbagliasse"[35].

In conclusione, le parti avevano confidato sulla verità dei dati, ma il venir meno di questo presupposto non liberava Quoine dall'adempimento del contratto con gli utenti, poiché i contratti conclusi automaticamente in virtù dell'algoritmo di *trading* erano immodificabili. La Corte negava anche la possibilità per Quoine di richiedere un indennizzo sulla base dell'ingiustificato arricchimento della società B2C2[36]. L'azione di ingiustificato arricchimento, infatti, può essere esperita quando l'arricchimento di una parte contrattuale sia avvenuto a spese dell'altra parte, mentre nel caso di specie la società Quoine non aveva subito un depauperamento, a causa della conclusione di contratti di vendita a prezzi notevolmente superiori rispetto a quelli previsti da altri mercati. Diversamente si può dire per gli utenti della piattaforma danneggiati dalla falsificazione dei tassi di cambio: la Corte, pur non intervenendo sul punto, accennava alla possibilità per quest'ultimi di richiedere un indennizzo alle controparti[37].

Il venir meno del presupposto "l'oracolo non mente" non inficia la validità e l'efficacia degli *smart contracts* conclusi automaticamente tra gli utenti, benché l'esecuzione dei contratti conduca ad esiti iniqui. L'azione di ingiustificato arricchimento, in questi casi, potrebbe costituire un rimedio, improntato all'equità del caso concreto, per tutelare la parte depauperata che non ha accesso ad altre forme di tutela, né di natura contrattuale né basate su interventi di correzione della tecnologia utilizzata.

5. La fiducia basata sul consenso dei nodi e le brecce del mondo reale: le sfide per il giurista

Gli oracoli svolgono la funzione fondamentale di permettere la comunicazione tra il *network* e il mondo esterno. Si tratta di elementi essenziali per il buon funzionamento della *blockchain* e il suo sviluppo in vari ambiti, che, allo stesso tempo, rappresentano un rischio di compromissione della "assenza di fiducia" (*trustless*) che caratterizza questa tecnologia. L'oracolo, infatti, fa emergere la necessità di una verificazione dei dati immessi nel sistema virtuale, ponendo il problema della sua affidabilità.

La dottrina ha evidenziato che proprio il problema dell'oracolo rischia di vanificare l'innovazione più importante della *blockchain*, consentendo una possibile falla nel sistema (*single point of failure*)[38]. Occorre considerare, tuttavia, che tutti i sistemi binari non possono comunicare con l'esterno in assenza di meccanismi che consentano *input* e *output*; anzi la loro utilità dipende essenzialmente dalla capacità di comunicare. In un tentativo di massima semplificazione, si potrebbe dire che queste forme di tecnologia (come altre) sono utili se soddisfano le esigenze delle persone e, quindi, comunicano con il mondo reale. Proprio questa interrelazione, che il problema dell'oracolo fa emergere con evidenza, induce a riflettere sull'uso del termine "trustless" e rimeditarne il significato: la *blockchain* promuove un modello di fiducia basato sul consenso dei nodi alternativo alla fiducia fondata sull'affidamento (nell'altra parte negoziale o in un terzo). Queste declinazioni della fiducia richiamano sistemi regolatori diversi che sono in relazione e, in alcuni casi, entrano in contraddizione, come avviene nell'ipotesi in cui l'affidabilità dell'oracolo è compromessa a causa di un errore. La

[34] *Ibid.*, para. 114: "This might conceivably be seen as a mistake as to the premise on which the buy orders were placed, but it can in no way be said to be a mistake as to the terms on which the contracts could or would be formed".
[35] *Ibid.*, para. 115: "In fact, the precise mistake in this case was a mistaken assumption on the part of the Counterparties as to how the Platform would operate. In other words, their real belief was that the Platform would not fail".
[36] *Ibid.* para. 130.
[37] *Ibid.*, para. 132.
[38] Cfr. per i primi riferimenti in italiano C. Poncibò, *Il diritto comparato*, cit., p. 76.

decisione della *Court of Appeal* di Singapore sopra analizzata, seppur non riferita alla tecnologia *blockchain*, offre un esempio significativo di questa dinamica.

Per ovviare a simili problemi, una parte della dottrina suggerisce che alla conclusione di uno *smart contract* si accompagni un accordo *off-chain* tra le parti, che contempli rimedi giuridici per l'ipotesi in cui si realizzi, a causa di malfunzionamenti di diverso tipo e dovuti a diverse circostanze, una divergenza tra i dati registrati nella catena virtuale e il concreto assetto di interessi voluto dalle parti[39]. Si tratta di una soluzione non sempre attuabile per una pluralità di ragioni, a cominciare dall'anonimato che spesso caratterizza le parti di uno *smart contract*. Essa tuttavia ha il pregio di evidenziare come la tecnologia *blockchain* non disegna un'architettura regolatoria avulsa dal diritto[40]. Gli *smart contracts* rappresentano piuttosto un aspetto di un rapporto contrattuale complesso regolato da una molteplicità di fonti: la 'legge' del codice informatico[41], le regole del mercato, le regole sociali, le regole contrattuali. Si tratta di mondi regolatori complementari piuttosto che alternativi, che si combinano diversamente a seconda del concreto assetto di interessi che le parti intendono realizzare[42].

In questo contesto il diritto (e il giurista), che sembrerebbe perdere il 'monopolio' della regolazione del contratto, è in effetti proiettato in una complessità che valorizza il ruolo dell'interprete e la capacità di cogliere la giuridicità inespressa di nuovi modi di relazionarsi e negoziare.

Abstract

La diffusione della blockchain in una pluralità di ambiti dipende anche dalla promessa di questa tecnologia di superare il problema della fiducia tra parti di una transazione (sistema trustless). L'immutabilità e l'incorruttibilità che caratterizzano la blockchain rischiano invece di essere compromesse dal problema dell'oracolo. La blockchain comunica con il mondo esterno al network tramite oracoli, facendo emergere la necessità di verificare i dati trasmessi dall'oracolo. L'articolo analizza il problema dell'oracolo da una prospettiva giuridica, focalizzando l'attenzione sulla rilevanza giuridica dell''errore' dell'oracolo. L'autrice distingue tra fiducia contrattuale e fiducia basata sul consenso dei nodi della blockchain, intese come espressioni di sistemi di regolazione del rapporto negoziale complementari piuttosto che alternativi.

Parole chiave: blockchain, oracoli, trustless, smart contracts, fiducia contrattuale, affidamento

*

The development of blockchain and its application to many different ambits depends also on the promise by this technology to eliminate the need of trust between parties (trustless system). The oracle problem risks to compromise the immutability and incorruptibility of the blockchain. Indeed, the blockchain communicates with the world off-chain through oracles, consequently the data transmitted by oracles need to be verified. The paper analyses the oracle problem from a legal perspective, focusing the attention on the legal relevance of an error by a blockchain oracle. The author distinguishes between the parties' confidence based on the consent of the nodes and the contractual reliance, and she argues the complementarity between the technological rules and the law of contract.

Key words: blockchain, oracles, trustless, smart contracts, contractual reliance, confidence

[39] Si tratta di un'indicazione presente anche nello studio della English Law Commission, *Smart legal contracts*, cit., p. 113, para. 5.39.
[40] K. Werbach, *Trust, But Verify: Why the Blockchain Needs the Law*, in *Berkeley Tech. L.J.*, 33/2018, p. 489 ss.
[41] Riprendendo la nota affermazione di L. Lessig, *Code is Law: On Liberty in Cyberspace*, in *Harvard Magazine*, 1/2000, p. 1 ss.
[42] Cfr. K. F.K. Low, E. Mik, *Pause the blockchain legal revolution*, in *International Law Quarterly Review*, 69(1)/2020, p. 135 ss., che osservano che in certi contesti il modello di fiducia proposto dalla tecnologia *blockchain* non è adeguato a realizzare gli interessi delle parti, che richiedono invece un'attività di intermediazione, portando l'esempio dell'attività di intermediazione bancaria.