Vincenzo Pasquino (*)

# *SMART CONTRACTS*: CARATTERISTICHE, VANTAGGI E PROBLEMATICHE

**Abstract:** The essay – starting from the basic definition of cryptocurrency and from the history of the software called Bitcoin, seen as the first worldwide payment system that works without a Central Bank – analyses the blockchain technology, the current use of this peer-to-peer system, his positives and downsides and describes a probable future use of it: the smart contracts, which could have a major impact on the world of traditional contracts and the world of trade in general.



## 1. — *Introduzione.*

Questo lavoro si propone di analizzare in via generale e sperimentale i profili giuridicamente rilevanti della tecnologia *blockchain*, base del software Bitcoin, e di uno dei suoi possibili utilizzi concreti: gli *smart contracts*. Tale tecnologia potrebbe essere in grado di influire in maniera netta sulle modalità future di raggiungimento di accordi tra privati.

Prima di procedere ad un'analisi specifica su tali strumenti di automazione contrattuale risulta essere utile, ai fini di una maggiore comprensibilità, una breve introduzione riguardante le criptovalute, sorte in seguito all'utilizzo della *blockchain* e, di conseguenza, strettamente correlate all'argomento in esame.

## 2. — *Le criptovalute.*

A partire dagli inizi del 2009, anno di lancio del software Bitcoin da parte

(*) Università degli Studi di Perugia.

dell'enigmatica figura di Satoshi Nakamoto, le monete virtuali hanno avuto una notevole e costante diffusione nel tempo, arrivando ad essere conosciute, ed in parte utilizzate, a livello mondiale.

Il software Bitcoin, nello specifico, si è dimostrato in grado di offrire un'alternativa ai tradizionali canali di pagamento elettronico[1]. Esso permette di registrare e trasferire bitcoin, ovvero una moneta digitale generata dal programma e non correlata a fattori esterni, quali, per esempio, le politiche monetarie[2].

Altra caratteristica fondamentale, per quanto riguarda i bitcoin, le altre criptovalute e, come si vedrà, per la tecnologia "blockchain", è la totale assenza di terze parti intermediarie nel processo di scambio, che quindi vede coinvolti solo i soggetti prettamente interessati all'operazione.

Occorre precisare che, seppure esistano una moltitudine di monete virtuali differenti, tutte presentano alcune caratteristiche comuni. Esse sono create da un emittente privato attraverso software appositi, possono essere acquistate con operazioni tecnicamente irreversibili in cambio di denaro "reale", ma non sono fisicamente detenute dall'acquirente, che, nella maggior parte dei casi, rimane anonimo[3].

La grande diversità di utilizzo delle diverse monete virtuali ha reso necessario, nel 2012, un tentativo di classificazione da parte della Banca Centrale Europea, che, con la relazione *Virtual Currency Schemes* ha proposto tre categorie differenti:

- *closed virtual currency schemes* (modello di moneta virtuale chiusa): in questo caso non c'è connessione con l'economia "reale". Questo modello è spesso definito come "*in-game only*": il soggetto interessato, nella maggior parte dei casi, guadagna monete virtuali in base alle proprie

---

[1] S. Nakamoto (pseudonimo), *Bitcoin: A Peer-to-peer Electronic Cash System*, 2008, in *bitcoin.org/bitcoin.pdf*.

[2] P. Cuccuru, *Blockchain ed automazione contrattuale. Riflessioni sugli smart contract*, in *Nuova giur. civ. comm.*, 2017, p. 107 ss.

[3] R. Bocchini, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento della disciplina tra prospettive economiche e giuridiche*, in *Dir. informaz. e informatica*, II, 1, febbraio 2017, p. 28.

prestazioni online, spendendole, in seguito, all'interno della stessa piattaforma virtuale senza la possibilità di sfruttarle in maniera diversa da quella prevista;

- *virtual currency schemes with unidirectional flow (*modello di moneta virtuale unidirezionale): è possibile usare la valuta reale per acquistare moneta virtuale (per esempio i *Facebook Credits*). Quest'ultima, però, una volta acquistata non può più essere riconvertita;
- *virtual currency schemes with bidirectional flow (*modello di moneta virtuale bidirezionale): tale categoria comprende le monete virtuali totalmente convertibili, acquistabili e cedibili secondo tassi di cambio ufficiali[4].

Da un punto di vista prettamente giuridico, la definizione e la qualificazione delle criptovalute appare controversa. L'elevata elasticità di Bitcoin, infatti, pone la dottrina di fronte all'impossibilità di fornire una definizione statica, che cristallizzi la materia. Una nozione inadeguata rischierebbe di limitarne lo sviluppo, sopprimendo le potenzialità positive che le monete virtuali, insieme alla tecnologia *blockchain*, potrebbero apportare. Un inquadramento giuridico, però, appare necessario per garantire la non pericolosità delle stesse verso il sistema finanziario[5]. La dottrina non è concorde riguardo la classificazione della fattispecie in esame quale bene giuridico *ex* art. 810 c.c. Se, infatti, da una parte si potrebbe far rientrare il bitcoin nell'ampia categoria di bene immateriale, dall'altra l'attribuzione di diritti di esclusiva su tali beni è guidata da un principio di stretta tipicità[6].

La soluzione che pare essere più convincente colloca le monete virtuali all'interno dell'ampia categoria degli strumenti finanziari. A sostegno di ciò si è espresso il Tribunale di Verona che, nella sentenza n. 195 del 24 gennaio 2017, ha affermato che: «I *bitcoin* rappresentano uno strumento finanziario costituito da una moneta che può essere coniata da qualsiasi utente ed è

---

[4] Relazione BCE *Virtual Currency Schemes*, ottobre 2012, in *https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf*.

[5] R. Bocchini, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento della disciplina tra prospettive economiche e giuridiche*, cit., p. 29.

[6] O.T. Scozzafava, *I beni e le forme giuridiche di appartenenza*, Milano, 1982, p. 422.

sfruttabile per compiere transizioni…»[7]. Tale definizione, comunque, lascia aperta la possibilità di inquadrare le criptovalute sia come moneta privata o complementare, sia come vero e proprio prodotto finanziario. Si rende necessario, in conclusione, sottolineare come il bitcoin sia, in realtà, idoneo a presentare le caratteristiche tipiche di molteplici categorie giuridiche e, allo stesso tempo, a seconda del contesto di riferimento, a distaccarsi da esse. La soluzione potrebbe risiedere, di conseguenza, nell'adottare un approccio asistematico, che guardi la funzione concreta che il bitcoin svolge nei rapporti che, di volta in volta, vengono presi in esame[8].

## 3. — *La* Blockchain.

La tecnologia che sta alla base del software Bitcoin è la *blockchain*. Essa risponde all'esigenza primaria di evitare il *double-spending*. Tale fenomeno consiste nell'impiegare gli stessi fondi virtuali, di trasferimento in trasferimento, infinite volte, alla stregua di un normale documento elettronico. Se ciò fosse possibile crollerebbe l'intero sistema delle criptovalute. Di conseguenza, attraverso lo sfruttamento della tecnologia basata sul *peer-to-peer*[9], tramite una rete a nodi, è stato creato un sistema di scrittura strutturato a blocchi e crittografato: la *blockchain*. La tecnologia *peer-to-peer* garantisce un elevato grado di sicurezza basato sulla decentralizzazione. I dati contenuti in questo "registro digitale", infatti, non sono conservati in un unico server o in un unico spazio di archiviazione, essi sono contemporaneamente presenti su tutti i computer connessi alla rete. Ciò garantisce un'inviolabilità della *blockchain* pressoché totale. Altra caratteristica tipica, oltre la decentralizzazione dei dati, è il sistema di scrittura a blocchi. Questo sistema consente un continuo aggiornamento del database, che aggiunge le infor-

---

[7] Trib. Verona, 24 gennaio 2017, n. 195, consultabile in *www.dirittobancario.it*.

[8] C. Tatozzi, *Bitcoin: natura giuridica e disciplina applicabile al contratto di cambio in valuta avente corso legale*, in *Ridare.it*, 9 agosto 2017.

[9] Ovvero un'architettura in cui tutti i computer connessi svolgono la funzione sia di client che di server.

mazioni di tutti i trasferimenti di moneta digitale – o di ogni altro tipo di dato che si voglia inserire in tale registro- ai precedenti, creando un insieme di "strati" di informazioni. Ciò consente di monitorare ogni singolo blocco autorizzato, impedendo che lo stesso si ripeta e, allo stesso tempo, mantenendo i dati sensibili anonimi.

Affinché un blocco di operazioni venga autorizzato è necessario che la maggioranza degli utenti del network si esprima favorevolmente riguardo la legittimità della versione aggiornata della *blockchain*, che viene fatta circolare dai nodi che decrittano, attraverso la potenza di calcolo delle loro macchine, il blocco di operazioni. Non tutti gli utenti, ovviamente, sono inclusi nel "procedimento del consenso". Esistono degli utenti qualificati, chiamati *miners*, che mettono a disposizione del meccanismo il potere di calcolo dei loro dispositivi ottenendo, in cambio, l'assegnazione di nuovi bitocin (generati, o meglio estratti, dall'algoritmo[10]).

I trasferimenti di moneta virtuale autorizzati e, di conseguenza, registrati sulla *blockchain*, godono di certezza, immutabilità ed unicità[11].

## 4. — *Gli* smart contracts.

La tecnologia *blockchain*, nonostante la recente origine, dimostra delle potenzialità che vanno ben oltre il "semplice" utilizzo come base per i software delle criptovalute. Se, infatti, questo può essere considerato un utilizzo tipico, si sta assistendo ad un superamento dello stesso a favore di un uso più vasto e, di conseguenza, potenzialmente problematico di questo registro digitale.

In tempi estremamente recenti, infatti, è stato ripreso un termine rimasto, fino ad oggi, semplicemente teorico: *smart contract*.

---

[10] La serie di calcoli necessaria a risolvere il blocco di operazioni

[11] P. Cuccuru, *Blockchain ed Automazione Contrattuale. Riflessioni sugli smart contract*, cit., p. 107.

Gli *smart contracts* combinano dei protocolli informatici con le interfacce utente per formalizzare e rendere sicuri degli accordi tramite una rete[12].

Sono, in altre parole, degli strumenti che, utilizzando la tecnologia *blockchain*, sono in grado di registrare delle informazioni e, al verificarsi di particolari condizioni precedentemente stabilite, eseguire dei termini senza l'intervento di terzi intermediari.

Appare logico pensare che la *blockchain*, in grado di registrare qualsiasi tipo di informazione con un elevato grado di sicurezza, si presti particolarmente allo sviluppo di questi particolari strumenti che, anche in senso non prettamente giuridico, sono dei canali per la conclusione di accordi.

Essi presentano delle caratteristiche tipiche:

- si presentano in forma digitale;
- sono composti da un insieme di codici crittografici, che svolgono la funzione di "clausole contrattuali" (es. al verificarsi della condizione *x* si esegue il termine *y*);
- sono irrevocabili: essendo l'esecuzione del contratto completamente automatica e gestita dal software è impossibile, una volta sottoscritto e avviato, modificare lo *smart contract*.

Il vero vantaggio di formalizzare ed eseguire degli accordi con questa modalità risulta essere il pressoché totale azzeramento dei rischi di inadempimento contrattuale. Lo *smart contract*, infatti, una volta avviato, non è influenzabile e viene eseguito automaticamente al compimento delle condizioni in esso insite.

Una differenza sostanziale con il contratto tradizionale, infatti, è rappresentata dal non affidare la vincolatività dell'accordo ad una fonte normativa esterna. Nei contratti tradizionali, esiste comunque la possibilità delle parti di scegliere se rispettare gli accordi o sopportare il peso delle conseguenze legali derivanti dal proprio inadempimento[13]. L'accordo inserito in una *blockchain,* al

---

[12] N. Szabo, *Formalizing and Securing Relationships on Public Networks*, in *First Monday*, vol. 2, n. 9, 1° settembre 1997, in *http://journals.uic.edu/ojs/index.php/fm/article/view/548/469*.

[13] C.J. Goetz, R.E. Scott, *Liquidated Damages, Penalties and the Just Compensation Principle: Some Notes on an Enforcement Model and a Theory of Efficient Breach*, in *Columbia Law Review*, vol. 77, 1977, pp. 554-558.

contrario, non lascia spazio alla volontaria violazione delle condizioni stabilite. La garanzia di esecuzione dei rapporti deriva direttamente dal *code layer* nel quale essi si verificano[14]. Questo fenomeno causa un'inevitabile compressione della libertà di agire delle parti, che sono spinte verso l'adempimento.

Se la tecnologia degli *smart contracts* presenta dei possibili vantaggi in grado di migliorare e far progredire il mondo degli accordi, specialmente quelli a distanza, essa non è però esente da problematiche di non secondaria importanza.

Si pensi, per esempio, alla necessità che siano presenti, in un contratto, i requisiti essenziali previsti dall'articolo 1325 c.c. Tali elementi potrebbero essere di difficile individuazione all'interno di un contratto presente in una *blockchain*, in quanto si presenterebbe sotto forma di codice crittografico.

Riguardo alla forma, poi, dovrebbe essere considerato il rapporto tra gli *smart contracts* e le disposizioni di legge relative alla necessità della forma scritta *ad substantiam* o per garantire particolari garanzie. La questione è se un contratto così programmato possa essere idoneo a rispettare tali disposizioni legali, venendo così equiparato a tutti gli effetti ad un contratto avente forma scritta *ad substantiam*. Tale problematica, secondo il parere del sottoscritto, appare facilmente superabile. Un contratto definito secondo codice crittografico e inserito in una *blockchain* che, come già specificato, fornisce al proprio contenuto i requisiti di immutabilità, certezza e unicità, appare idoneo a garantire le stesse- se non maggiori- garanzie di un contratto tradizionale che prevede la forma scritta. Si tratterebbe, in altre parole, di un contratto scritto non in lingua corrente ma in linguaggio macchina. Per avvicinare tale metodo di scrittura al linguaggio "comune", alcune società, chiamate *smart contracts solution providers*, hanno sviluppato il c.d. *"split" contracting model*, che riprende alcuni aspetti dei contratti ibridi, leggibili sia da persone fisiche che da un software (i *Ricardian Contracts*). Lo *"split" contracting model*, similmente, collega in maniera indissolubile un contratto in forma scritta all'architettura tipica degli *smart contracts*[15].

---

[14] P. Cuccuru, *Blockchain ed Automazione Contrattuale. Riflessioni sugli smart contract*, loc. ult. cit.

[15] D. Di Maio, G. Rinaldi, *Blockchain e la rivoluzione legale degli smart contracts*, in *http://www.dirittobancario.it/news/contratti/blockchain-e-la-rivoluzione-legale-degli-smart-contracts*.

Tale metodo contribuirebbe, senza dubbio, a limitare la barriera causata dall'utilizzo di linguaggi diversi pur non eliminandola del tutto. Soggetti privi di un'adeguata preparazione tecnica potrebbero, infatti, incorrere in serie difficoltà nel predisporre e valutare appieno le clausole contrattuali espresse in codice. Sembra opportuno ricordare, inoltre, l'impossibilità di correggere un qualsiasi errore una volta inserita l'istruzione all'interno della blockchain. Ci si trova nella paradossale situazione in cui una tecnologia nata per facilitare gli accordi tra le parti, evitando il rischio di inadempimento e snellendo la procedura - dal momento in cui essa non dipende dalla presenza di intermediari terzi- risulta essere di difficile applicazione, se non tramite il ricorso ad esperti del settore informatico.

Tale intervento terzo, di conseguenza, inserisce nella procedura di creazione dello *smart contract* un grado di imprevedibilità "umana" che lo riavvicina inesorabilmente al contratto tradizionale. Nella fase di creazione – o meglio di trasposizione di esigenze delle parti in codice crittografato – si potrebbe, infatti, verificare un'incomprensione tra soggetto ed intermediario, che tenderebbe a semplificare le istruzioni giuridiche impartitegli per facilitarne l'esecuzione da parte di un sistema informatico[16].

Altro aspetto di estrema rilevanza per uno studio circa l'utilizzo degli *smart contracts* in ambito di accordi aventi rilevanza giuridica è, senza dubbio, quello della decentralizzazione. Essa è una caratteristica tipica della *blockchain*. Maggiore è il grado di apertura, e quindi di dispersività delle informazioni, tanto il registro informatico risulta essere non modificabile. Una delle problematiche di maggior rilievo che sorge in materia di *smart contracts* è, per l'appunto, che risulterebbero impossibili anche le modifiche legittime alle condizioni programmate e successivamente lanciate nella *blockchain*.

Tale rigidezza strutturale costituirebbe un serio limite anche per gli eventuali interventi legittimi di autorità pubbliche – garanti del rispetto di scelte politiche e legislative – e per l'applicazione di istituti tipici del diritto contrattuale, quali, per esempio, quello della nullità o del recesso.

---

[16] D.K. Citron, *Technological Due Process*, in *Washington University Law Review*, vol. 85, 2008, p. 1249, secondo cui «Programmers may be tempted to write code employing a simplified three-month rule, leaving out the complicated and arguably confusing exceptions».

Una parte di dottrina prende in considerazione, come possibile soluzione, una sorta di ibridazione delle piattaforme decentralizzate. Si creerebbero delle *blockchain* private, dette *permissioned*, che consentirebbero di restringere l'accesso degli utenti attraverso un'identificazione e di pre-selezionare i nodi che autorizzano le operazioni. In questo modo, secondo tale dottrina, si creerebbe, attraverso questi nodi identificabili, un punto di contatto tra sistema giuridico e sistema informatico, in quanto le decisioni giudiziali e le istanze tra le parti avrebbero dei destinatari concreti[17]. Di contro, però, andrebbe considerato il fatto che i principali vantaggi derivanti dall'utilizzo della *blockchain*, e di conseguenza degli *smart contracts*, risiedono proprio nella caratteristica della decentralizzazione e automazione di dati.

A prescindere dal metodo utilizzato, infatti, consentire a dei terzi – seppur autorizzati – una "intrusione", renderebbe il processo di automazione contrattuale macchinoso e con un "grado di imprevedibilità" più alto. Verrebbero a mancare le caratteristiche tipiche della non modificabilità, dell'irrevocabilità, della certezza dell'adempimento e, in parte, dell'automazione stessa del contratto, rendendo questa tipologia di accordo probabilmente più complessa rispetto alla stipula di un contratto tradizionale.

In conclusione, gli *smart contracts* rappresentano, indubbiamente, una tecnologia con un altissimo potenziale d'utilizzo, a patto che vengano accettati pacificamente come strumenti idonei a rappresentare in maniera completa la volontà delle parti. Tale accettazione avverrà, presumibilmente, solo una volta raggiunta una regolamentazione o, quantomeno, una regolarizzazione in grado di offrire delle garanzie agli utenti fruitori di tale servizio. Appare necessario, di conseguenza, un bilanciamento di interessi tra i vantaggi derivanti dalla non regolamentazione stessa e le esigenze di "sicurezza" richieste per un utilizzo su larga scala. Creare delle piattaforme ad accesso ristretto potrebbe sicuramente alleggerire la problematica, senza però poter impedire la diffusione di *blockchain* a nodi anonimi e, di conseguenza, di accordi e contratti stipulati tra privati e non suscettibili di modifiche e controlli.

---

[17] P. Cuccuru, *Blockchain ed Automazione Contrattuale. Riflessioni sugli smart contract*, cit., loc. ult. cit.