Consiglio Nazionale del Notariato

AREA INFORMATICA

Studio 1_2019 DI

L. 12/2019 – SMART CONTRACT E TECNOLOGIE BASATE SU REGISTRI DISTRIBUITI – PRIME NOTE

(MM– marzo 2019)

Approvato dalla Commissione Informatica il 4 aprile 2019

SOMMARIO: 1. Introduzione – la nuova normativa. – 2. Smart contract – le origini. – 3. Gli elementi essenziali di un contratto, in particolare la forma scritta. – 4. Smart contract e documentazione del contratto. – 5. Smart contract e compatibilità con la normativa generale sui contratti. – 6. Tecnologie basate su registri distribuiti. – 7. Smart contract e tecnologie basate su registri distribuiti.

ABSTRACT

La L. 12/2019, di conversione del D.L. 135/2018, introduce per la prima volta nel nostro ordinamento le definizioni di "smart contract" e di "tecnologie basate su registri distribuiti", attribuendo ai primi (se operanti sulle seconde) il valore di forma scritta, previo rispetto di determinate caratteristiche.
Lo studio contiene una prima analisi di queste novità, volta principalmente a cercare di comprendere l'inserimento (e quindi la compatibilità) di tali nuove figure all'intero della disciplina codicistica dei contratti.
Attraverso un raffronto tra gli elementi essenziali di un contratto (da un lato) ed i requisiti imposti dalla legge (dall'altro), lo studio evidenzia che l'efficacia vincolante di uno smart contract pare essere subordinata al rispetto di condizioni, ora di tipo tecnico (utilizzo effettivo di "vere" tecnologie basate su registri distribuiti, presenza di un meccanismo reale di consenso distribuito) ora di tipo giuridico (documentazione della causa del contratto, identificazione delle parti).
Lo studio evidenzia, altresì, la permanenza di alcune zone d'ombra nella nuova normativa, e precisamente la difficile applicabilità ad uno smart contract di norme dell'ordinamento quali – ad esempio – quelle che attualmente sovrintendono l'interpretazione o la risoluzione del contratto.

1. INTRODUZIONE – LA NUOVA NORMATIVA

Il D.L. 14 dicembre 2018, n. 135 (in GU n. 290 del 14 dicembre 2018) convertito con modificazioni dalla L. 11 febbraio 2019, n. 12 (in G.U. 12 febbraio 2019, n. 36) ed entrato in vigore dal 15 dicembre 2018, introduce nel nostro ordinamento giuridico le nozioni di tecnologie basate su registri distribuiti e smart contract.
Dispone infatti l'art. 8-ter del decreto:
"*1. Si definiscono "tecnologie basate su registri distribuiti" le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento*

e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili.
2. Si definisce "smart contract" un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse. Gli smart contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto.
3. La memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all'articolo 41 del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014. 4. Entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, l'Agenzia per l'Italia digitale individua gli standard tecnici che le tecnologie basate su registri distribuiti debbono possedere ai fini della produzione degli effetti di cui al comma 3".
Detto articolo definisce quindi le nozioni di "tecnologie basate su registri distribuiti" al primo comma e di "smart contract" al secondo, prevedendo al terzo comma gli effetti giuridici della memorizzazione di un documento informatico attraverso l'uso di tali tecnologie basate su registri distribuiti.
Le nozioni introdotte dal legislatore sono, pertanto, in sintesi:
- **smart contract**: "programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse", che "soddisfa il requisito della forma scritta previa identificazione informatica delle parti interessate"
- **tecnologie basate su registri distribuiti**: "tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili".

2. SMART CONTRACT – LE ORIGINI

Il termine "smart contract" è stato coniato negli anni '90 da Nick Szabo, un informatico statunitense, con studi legali e di crittografia, laureatosi presso l'Università di Washington nel 1989 in informatica.
Scrive infatti Nick Szabo[1]: "*L'idea di base dello smart contract è che molti tipi di clausole contrattuali (come la garanzia, l'assunzione dell'obbligazione, la delimitazione di un diritto di proprietà, ecc.) possono essere incorporati nell'hardware e nel software che trattiamo, in modo da rendere la violazione del contratto costosa (se desiderato, addirittura proibitiva) per il soggetto inadempiente*".
Egli, partendo dall'esempio base del distributore automatico di bevande, offre ulteriori esempi applicativi, tra cui uno, ben più "smart", relativo alla possibile gestione automatizzata dei rapporti nascenti dall'acquisto di un autoveicolo mediante pagamento a rate. Grazie, infatti, ad una combinazione di hardware e software installati nel veicolo stesso, Nick Szabo giunge ad immaginare che lo smart contract entri in azione per disabilitare la messa in moto dell'auto in caso di mancato pagamento di un certo numero di rate.

Se questo, dunque, è il concetto originario di uno smart contract, così come teorizzato dal suo autore, un primo rapido confronto con la definizione normativa pone subito in rilievo la totale assenza, nella norma, di un benché minimo riferimento ad una componente hardware.
La norma, infatti, definisce lo smart contract esclusivamente come un "programma per elaboratore" (quindi come un software), mentre invece nell'idea del suo autore uno smart contract dovrebbe essere una sorta di integrazione tra un software (che contiene le istruzioni), ed un hardware (che tali istruzioni è chiamato ad eseguire materialmente).

1 Nick Szabo "Formalizing and Securing Relationships on Public Networks", 1997

Ed infatti, un distributore automatico ha una componente software, ma anche un hardware che materialmente erogherà il prodotto, ed anche nell'esempio dell'autovettura sarà necessario il dispositivo che inibisca l'accensione fisica del motore.
Insomma, nel mondo degli smart contract, un semplice "programma per elaboratore" non basta, servirà infatti anche un dispositivo ulteriore (che invero potrà essere un apparato hardware ma anche un altro apparato software) su cui lo smart contract sarà programmato ad agire.
La mancata previsione, nella normativa in esame, di un simile aspetto non deve tuttavia essere necessariamente giudicata come una lacuna.
Essa potrebbe semplicemente essere interpretata come la volontà del legislatore di lasciare una certa libertà sul punto, evitando – attraverso una norma sostanzialmente definitoria – di limitare l'utilizzo degli smart contract ad ambiti normativamente predeterminati.
Ciò tuttavia non autorizza l'interprete a dimenticare che uno smart contract è destinato a compiere una o più azioni, nel mondo digitale ma anche in quello reale, richiedendo – molto probabilmente – l'uso di ulteriori dispositivi; dispositivi il cui funzionamento, regolamentazione e condizioni di utilizzo, la norma non disciplina, e che pertanto presumibilmente avranno bisogno di separata disciplina contrattuale.

Evidenziata questa prima, importante, mancanza nella norma (lo si ripete, probabilmente voluta, ma non per questo meno significativa), il primo interrogativo che si pone all'interprete è il seguente: **uno smart contract è (o può essere) un contratto?** Oppure esso attiene unicamente alla fase esecutiva di un contratto che deve preesistere o essere presupposto (come parrebbe suggerire il termine "esecuzione" utilizzato dalla norma stessa)?
La risposta a questa domanda non può dirsi affatto scontata in quanto, da un lato, la norma parla di "effetti predefiniti dalle parti", lasciando così immaginare l'esistenza di un momento di formazione dell'accordo logicamente antecedente allo smart contract.
D'altro canto, tuttavia, la norma stessa indica lo smart contract come fonte di vincolo giuridico tra le parti, aspetto questo che parrebbe contrastante con la preesistenza di un rapporto contrattuale tra le stesse, che essendo già fonte giuridica di un vincolo, renderebbe inutile la previsione di un vincolo ulteriore.
Infine, la norma attribuisce espressamente ad uno smart contract (previa identificazione informatica delle parti interessate), il valore di documento avente forma scritta; circostanza questa che finirebbe per avvicinare la fattispecie in esame ad un contratto vero e proprio.

Comprendere, quindi, se uno smart contract possa essere (esso stesso) un contratto, richiede un preventivo (ancorchè breve) accenno alla teoria generale dei contratti, ed in particolare a quelli che prevedono una forma vincolata: la forma scritta.

3. GLI ELEMENTI ESSENZIALI DI UN CONTRATTO, IN PARTICOLARE LA FORMA SCRITTA

Come è noto, il contratto è definito dall'art. 1321 c.c. come "*l'accordo di due o più parti per costituire, regolare o estinguere tra loro un rapporto giuridico patrimoniale*". Elementi essenziali del contratto, a norma del successivo 1325 c.c., sono: **l'accordo** delle **parti**, la **causa**, **l'oggetto** e la **forma** (quest'ultima quando prevista dalla legge a pena di nullità).
Ripercorrendo, brevemente, tali elementi:
* le parti (o centri di interessi): sono i soggetti rispetto ai quali, o nel cui interesse, il contratto esplica le conseguenze giuridiche pattuite;
* l'accordo: è l'incontro della volontà delle parti ed è quel "quid" essenziale che dà vita al contratto;
* la causa (la cui definizione non sempre è univoca): può essere genericamente indicata come l'elemento giustificativo che rende giuridicamente apprezzabile lo scopo a cui tende in concreto l'attività delle parti;

* l'oggetto (concetto anch'esso non univoco): rappresenta l'insieme delle prestazioni e, quindi, qualunque cosa le parti siano tenute a fare a non fare o a dare.
Ultimo, ma non per importanza, è il requisito della **forma**.
Nonostante, infatti, il tenore letterale dell'art. 1325 c.c. sembri affermare l'essenzialità della forma solo nei casi nei quali essa è prescritta dalla legge a pena di nullità, invero una (generica) forma del contratto è sempre essenziale.
Del resto, se è vero che la forma viene normalmente definita come "modo di manifestazione della volontà negoziale"[2] appare del tutto evidente che una volontà contrattuale che rimanga all'interno dell'animo del soggetto interessato non può essere rilevante per il diritto.
Occorre, insomma, sempre che una volontà – per assumere rilevanza – venga portata all'estero e dichiarata.
Una forma, pertanto, del contratto costituisce sempre elemento essenziale.
Ciò che, in taluni casi, la legge impone (o può imporre) è l'utilizzo di una particolare forma per il compimento di determinati atti giuridici o per particolari effetti (si parla – in tali casi – di "forma solenne"). Si tratta, come è noto, di casi eccezionali in quanto la regola generale è la libertà (non assenza) della forma.

Ora, generalmente viene riconosciuta alla forma solenne una duplice funzione: la prima è connessa all'opportunità di predisporre una documentazione della volontà manifestata, al fine di avere la certezza dell'esatto contenuto delle dichiarazioni delle parti (c.d. "funzione di prova"), la seconda è riconnessa all'opportunità di richiamare l'attenzione delle parti sull'importanza dell'atto che stanno per compiere (che potremmo definire "funzione di consapevolezza").

Tra le forme solenni previste dal nostro ordinamento, la principale e più importante è sicuramente la **forma scritta**, imposta dalla legge per il compimento di taluni atti addirittura *ad substantiam* (quindi a pena di nullità).
Scritta è la dichiarazione contenuta in un documento, cartaceo, informatico, su pietra, o su qualsiasi altro supporto che possa essere letto.

Ora, è evidente che - affinché un contratto possa soddisfare il requisito della forma scritta - l'attività di documentazione dovrà investire tutti gli elementi essenziali del contratto. Tutti, pertanto, dovranno essere documentati (non necessariamente in un unico documento, come nel caso dei contratti a formazione progressiva, ma comunque compiutamente documentati).
Ripercorrendo, quindi, velocemente gli elementi essenziali sopra ricordati, nessuna difficoltà particolare può essere individuata nell'incorporare in un documento scritto l'oggetto di un contratto (cioè l'insieme delle prestazioni concordate) o la causa (soprattutto se tipica).
Maggiori problemi sorgono invece nella documentazione delle parti e dell'accordo (o, se si preferisce, della volontà), posto che non sempre il documento può (o deve) essere redatto materialmente dalle parti interessate, per cui occorre individuare uno strumento che sia idoneo a riferire la manifestazione di volontà che fa nascere il rapporto contrattuale alle parti interessante, anche nel caso in cui il documento sia stato predisposto da terzi.

Tale strumento è la **sottoscrizione**.
Ciò che infatti rende un documento imputabile ad un determinato soggetto è la sottoscrizione; essa assolve tipicamente tre funzioni: *indicativa* (in quanto permette di identificare l'autore del

2 A. Trabucchi, "Istituzioni di diritto civile", 1992, p. 150.

documento), *dichiarativa* (in quanto comporta l'assunzione della paternità del documento e della manifestazione di volontà in esso contenuta) e *probatoria* (dell'autenticità del documento)[3].

4. SMART CONTRACT E DOCUMENTAZIONE DEL CONTRATTO

Se quelli sopra ricordati sono i principi generali applicabili ai contratti, ed in particolare ai contratti per i quali la legge impone l'uso della forma scritta, sarà a questo punto necessario verificare se uno smart contract – a cui la norma espressamente riconosce analogo valore di **forma** – soddisfi tutti gli altri requisiti sopra ricordati.

Partendo dagli elementi di più facile individuazione, possiamo senz'altro affermare che uno smart contract sarebbe idoneo a documentare **l'oggetto** del contratto, inteso come l'insieme delle prestazioni convenute dalle parti. Lo dice espressamente le norma in esame nel punto in cui prescrive che il programma per elaboratore agisca sulla "base di effetti predefiniti" dalle parti, ma lo testimonia anche la funzione stessa di uno smart contract, il cui scopo primario è proprio quello di realizzare la prestazione voluta dalle parti.

Qualche difficoltà, invece, lo smart contract pone in relazione alla documentazione relativa alle **parti** del contratto. La norma in esame, infatti, non prevede espressamente alcuna forma di sottoscrizione (nemmeno di tipo informatico) che sia utile allo scopo. La norma, infatti, si limita a prevedere che "*gli smart contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare*".
La novella sembra, sul punto, porsi in linea con quanto già peraltro disposto dagli artt.20 comma 1-bis e 21 comma 2-bis del CAD (Decreto Legislativo 5 marzo 2005, n. 82) che rispettivamente dispongono:
"*Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità.*".
e:
"*Salvo il caso di sottoscrizione autenticata, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale. Gli atti di cui all'articolo 1350, numero 13), del codice civile redatti su documento informatico o formati attraverso procedimenti informatici sono sottoscritti, a pena di nullità, con firma elettronica avanzata, qualificata o digitale ovvero sono formati con le ulteriori modalità di cui all'articolo 20, comma 1-bis, primo periodo.*".

Si prevede, insomma, che la funzione identificativa delle parti di uno smart contract avvenga attraverso un "processo" di identificazione di cui la norma non fornisce alcuna descrizione, limitandosi a prevedere che esso debba solo soddisfare taluni requisiti (tra l'altro non prefissati, ma la cui individuazione viene demandata ad AgID).

3 Cfr. E. PROTETTI' – C. DI ZENZO, La legge notarile, Milano, 1985, pag. 241; G. CASU, L'atto notarile tra forma e sostanza, Milano-Roma, 1996, p. 148 e ss.; G. PETRELLI, Documento informatico, contratto in forma elettronica e atto notarile, in Notariato n. 6/1997, p. 567.

Ora, la somiglianza dal punto di vista letterale della formula utilizzata dal legislatore per gli smart contract, rispetto a quella già in precedenza usata nel CAD per il documento informatico, pone all'interprete alcuni interessanti interrogativi.
In primo luogo, dalla formulazione utilizzata dal legislatore nel CAD emerge che questo "processo" di "identificazione" rappresenti qualcosa di alternativo (e quindi di diverso) rispetto alla "firma" (digitale, qualificata o avanzata).
La lettura sistematica di entrambe le norme, quindi, potrebbe sollevare l'interrogativo se sia consentito ad AgID – nell'ambito della delega alla medesima attribuita in materia di smart contract – prevedere comunque l'utilizzo di firme digitali, qualificate o avanzate, per l'imputabilità di uno smart contract ad un soggetto o se (come previsto per il documento informatico in generale) debba trattarsi esclusivamente di processi differenti ed ulteriori rispetto all'apposizione di una "firma"[4].
In secondo luogo, la delega ad AgID appare così ampia da finire per attribuire a tale Ente in via esclusiva la pesante responsabilità di adottare misure idonee ad evitare fenomeni di sostituzione di persona, senza una benché minima copertura normativa sul punto.

Ancor più problematica risulta, invece, sempre nella nuova normativa sugli smart contract, la documentazione dell'**accordo** delle parti.
Riprendendo infatti il raffronto con le norme del CAD di cui si è detto, e sopra riportate, spicca la mancata riproposizione nella norma sugli smart contract dell'inciso secondo cui il processo di identificazione deve avvenire "*con modalità tali da garantire (...) in maniera manifesta e inequivoca, la sua riconducibilità all'autore*".
Sembrerebbe, in altre parole, mancare, nella normativa sugli smart contract, un meccanismo che consenta di documentare una manifestazione inequivoca della volontà delle parti.
In realtà, ad una più attenta analisi, così non è.
Anche nella norma definitoria in esame è infatti possibile intravvedere l'elemento della volontà – anche se (forse) in parte celato sotto termini utilizzati in modo del tutto inconsueto.
La chiave di volta è rappresentata dal termine "esecuzione" contenuto nella definizione normativa di smart contract che qui di seguito, per comodità, si riporta: "*Si definisce "smart contract" un programma per elaboratore (...) la cui esecuzione vincola automaticamente due o più parti*".
Ora, tradizionalmente con il termine "esecuzione" del contratto ci si riferisce (giuridicamente parlando) a quella fase del rapporto contrattuale, **successivo** alla sua conclusione, in cui le prestazioni dedotte nell'accordo vengono eseguite dalle parti.
Se tuttavia applicassimo questa tradizionale definizione alla norma sullo smart contract otterremmo inevitabilmente un nonsenso giuridico.
L'esecuzione, infatti, intesa come adempimento, non può certamente generale vincoli, in quanto – semmai – l'adempimento determina l'estinzione (e non il sorgere) di un'obbligazione.
Se dunque questo – con tutta evidenza – non può essere il significato da attribuire al termine "esecuzione" riferito (nella norma) allo smart contract, allora il vero significato dovrà essere ricercato in altro registro linguistico e – più precisamente – non in quello giuridico, ma in quello informatico, ove il termine "execution" significa "The performance of an instruction or program"[5].
Esecuzione, pertanto, significa "avvio" del programma, ossia lettura delle istruzioni caricate e loro memorizzazione all'interno del sistema. Non significa pertanto loro immediata "esecuzione" nel senso giuridico del termine.

4 Sarebbe tuttavia necessario a questo punto verificare la compatibilità di tale impianto normativo con il regolamento eIdas (REGOLAMENTO (UE) N. 910/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO) nel quale la nozione di «firma elettronica» è indicata come l'insieme di "dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario **per firmare**".

5 https://en.oxforddictionaries.com/definition/execution

Sarà pertanto l'azione materiale di "dare avvio" al programma l'elemento che fornirà la prova (e quindi la "documentazione") della manifestazione della volontà di una parte di accettare le istruzioni in esso contenute, e quindi sarà l'**avvio congiunto** del programma, ad opera delle parti interessate, a documentarne l'accordo.

Ma l'aspetto più problematico in uno smart contract è senza dubbio la documentazione della **causa** del contratto.
E' evidente, infatti, che un programma per elaboratore, scritto peraltro in linguaggio non naturale ma unicamente in linguaggio di programmazione, conterrà solo istruzioni di tipo esecutivo. Difficilmente, esso conterrà anche istruzioni di tipo "descrittivo" in quanto – banalmente – esse non sono istruzioni. Di certo non è tenuto a contenerle, sia in quanto non necessarie per l'elaborazione da parte del calcolatore, sia in quanto non previste dalla norma (che prescrive solo l'indicazione degli *effetti* voluti dalle parti, e non altro).
Ne consegue che non sempre uno smart contract sarà idoneo a documentare anche la causa del contratto.
Se infatti possiamo con facilità ricavare la causa di uno smart contract che sovrintenda al funzionamento del distributore di bevande, non altrettanto possiamo dire di uno smart contract che (ad esempio) semplicemente contenga l'istruzione di pagamento di una somma da un soggetto ad un altro; pagamento che potrebbe in astratto trovare la propria causa in molteplici tipologie negoziali (prezzo di una compravendita? mutuo? pagamento di una obbligazione? liberalità?) ma che potrebbe anche essere illecita.
E' infatti di tutta evidenza che non sempre è agevole ricostruire la comune intenzione delle parti, semplicemente analizzando il momento attuativo del contratto, soprattutto per quei contratti che prevedono obbligazioni a carico di una sola parte[6].

La norma - pertanto - lascia aperto un problema, senza offrire, per esso, alcuna soluzione.
Sarà allora lecito immaginare che la soluzione passi: o attraverso il "volontario" inserimento in uno smart contract di informazioni non necessarie per la sua esecuzione informatica, ma necessarie per la sua qualificazione giuridica, o attraverso una tipizzazione degli smart contract attraverso l'imposizione di modelli standardizzati prefissati, la cui causa sia quindi predeterminata (che tuttavia sarebbe oltremodo limitante e di ostacolo per un rapido sviluppo di una simile tecnologia), oppure attraverso l'integrazione dello smart contract con un documento contrattuale ulteriore e separato, che contenga gli elementi omessi.

5. SMART CONTRACT E COMPATIBILITÀ CON LA NORMATIVA GENERALE SUI CONTRATTI

Alla luce della disamina che precede, appare potersi concludere che uno smart contract potrà porsi prevalentemente come "strumento" di supporto o come "parte" di un più ampio accordo contrattuale, magari redatto secondo forme più "tradizionali", curandone e semplificandone l'aspetto relativo all'adempimento delle obbligazioni pattuite. Nonostante, infatti, esso possa ritenersi astrattamente idoneo – pur con qualche importante difficoltà – a costituire (una volta emanate le linee guida AgID) unica fonte del rapporto contrattuale, tale idoneità appare (al momento) ristretta ad ipotesi di contratto dalla struttura assai basilare.

6 Del resto non tutti i contratti hanno la struttura "semplice" dell'acquisto di una bevanda dal distributore automatico, per cui – all'aumentare della complessità dell'accordo negoziale – la sola documentazione del momento attuativo del contratto difficilmente potrà fornire adeguata misura del complessivo accordo negoziale, e della sua liceità.

Ma vi è di più, perché anche volendo considerare strutture contrattuali semplici, da tradurre interamente in smart contract, la normativa in esame lascia comunque alcune zone d'ombra inesplorate, chiamando l'interprete al difficile compito di mettervi un po' di luce.
In particolare, dubbia è la compatibilità di uno smart contract con taluni gruppi di norme che sovrintendono la generalità dei contratti.

Ci si riferisce in primo luogo alle norme relative all'**interpretazione del contratto**. Uno smart contract non è scritto in linguaggio naturale, ma unicamente in linguaggio di programmazione, il quale ha un unico significato: quello attribuito dall'elaboratore a cui il programma viene sottoposto.
Se, da un lato, tale caratteristica è considerata (dai suoi sostenitori) uno degli aspetti più positivi di uno smart contract, per la sua capacità di essere insensibile alle differenti interpretazioni che ciascuna mente umana può dare di un medesimo documento, dall'altro non si rinviene nella norma alcuna sterilizzazione delle regole codicistiche relative alla interpretazione del contratto (artt. 1362 e seguenti c.c.), la cui applicazione ad uno smart contract, tuttavia, non può che risultare a dir poco difficoltosa[7].

In secondo luogo, ulteriori difficoltà potrebbero incontrarsi nell'applicazione agli smart contract delle norme codicistiche sulla **risoluzione del contratto**. Non ci si riferisce tanto alla risoluzione volontaria o negoziale, che avviene quando le parti decidono di comune accordo di sciogliersi dai vincoli contrattuali (mutuo dissenso) o convengono fin da subito la possibilità di scioglimento unilaterale (recesso). Tali facoltà, infatti, ben potrebbero essere contenute in apposite istruzioni contenute nello smart contract[8].
Ciò che appare sicuramente più problematica è la compatibilità degli smart contract con le norme che disciplinano le ipotesi di risoluzione legale, previste dal nostro ordinamento quando sorgono particolari problemi nel corso del rapporto contrattuale.
Se infatti è in astratto possibile immaginare che uno smart contract sappia gestire una risoluzione di un contratto per inadempimento[9] o per impossibilità sopravvenuta, ci sembra invero difficile immaginare che un programma per elaboratore possa (ad esempio) gestire anche l'eccessiva onerosità sopravvenuta posto che essa, per definizione codicistica, trova applicazione unicamente in presenza di avvenimenti straordinari ed imprevedibili.

E tale problematica ci sembra, peraltro, ancor più rilevante se si considera che – per espressa previsione normativa – gli smart contract per avere un riconoscimento legale dovranno necessariamente operare "su tecnologie basate su registri distribuiti" espressamente caratterizzate da protocolli informatici "non alterabili e non modificabili" (quindi nemmeno ad opera di un giudice).

6. TECNOLOGIE BASATE SU REGISTRI DISTRIBUITI

La normativa in esame richiede espressamente che uno smart contract debba operare su **tecnologie basate su registri distribuiti**, e di esse offre la seguente definizione: "*tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili*".

7 Si pensi solo alla norma che impone di interpretare il contratto secondo "buona fede".
8 Quid juris, tuttavia, se nulla prevede lo smart contract in proposito? Se la norma parla di programma che vincola automaticamente sulla base degli effetti predefiniti, sussiste margine per una interruzione volontaria del programma se tale facoltà non è stata ab origine prevista?
9 Ancorchè appaia difficile pensare che uno smart contract possa – ad esempio – essere in grado di applicare i principi di cui all'art. 1455 c.c., i quali presuppongono la capacità di valutare se l'inadempimento abbia (o meno) una scarsa importanza, avuto riguardo all'interesse dell'altra parte.

Si tratta, invero, di una definizione che riutilizza termini e concetti evidentemente ricavati dalla dottrina (soprattutto estera) di settore[10], ma sulla cui formulazione già molti hanno rinvenuto "*margini di ambiguità ed incompletezza*"[11].

Un registro distribuito può essere descritto come un registro di transazioni o di documenti dislocato in differenti luoghi e presso differenti soggetti, e nel contempo privo di un'autorità centrale che mantenga il controllo sul registro e fornisca un presidio contro le possibili manipolazioni.

Dal punto di vista informatico, il vantaggio dei registri distribuiti è evidente: essi eliminano il c.d. problema del "single point of failure" (letteralmente "singolo punto di vulnerabilità"). Infatti, mentre in caso di registro centralizzato un attacco perpetrato all'autorità centrale consentirebbe ad un malintenzionato di prendere il controllo del registro e di alterarlo, in un registro distribuito l'attacco sarebbe notevolmente più difficile, poiché richiederebbe il simultaneo attacco di tutti (o almeno della maggioranza) delle copie del registro esistenti.
Maggiore, pertanto, è la diffusione di un registro distribuito, maggiore sarà il suo livello di sicurezza.

Anche i registri distribuiti, tuttavia, hanno importanti criticità, ed infatti non è un caso che – finora – si siano sviluppati prevalentemente sistemi di registrazione basati su registri centralizzati.
In particolare, l'aspetto più critico in un registro distribuito attiene al meccanismo di **formazione del consenso** alla registrazione.
In altre parole, mentre in un registro centralizzato è preciso compito dell'autorità che lo governa quello di effettuare o validare le singole registrazioni, nei registri distribuiti (in quanto privi di autorità) deve necessariamente essere individuato un processo "collettivo" (diremmo quasi "democratico") che approvi le singole registrazioni. E ciò crea non pochi problemi pratici.

Un semplice esempio chiarirà questo concetto di fondamentale importanza.

Immaginiamo che in un ufficio si decida di gestire in modo "distribuito" l'agenda degli appuntamenti. A ciascun impiegato, quindi, viene consegnata una copia identica dell'agenda, con l'espressa facoltà per tutti di fissare i nuovi appuntamenti.
Orbene, non è difficile immaginare che passerà ben poco tempo prima che il caos regni sovrano, che un medesimo appuntamento venga assegnato contemporaneamente da due impiegati differenti a due clienti differenti usando due agende differenti, e che ben presto le copie (ab origine identiche) inizino a differenziarsi l'una dall'altra, rischiando di incorrere in quello che – tecnicamente – viene definito il problema del "double spending" (letteralmente "doppia spesa")[12].

In altre parole, i registri distribuiti pongono il difficile problema della creazione di un meccanismo di **consenso distribuito**, che consenta di evitare che singole registrazioni si accavallino oppure che si disponga più volte delle medesime risorse.

Si tratta invero di un problema di difficile soluzione[13], che fino ad oggi ha reso – come si diceva – poco conveniente l'adozione di registri di tipo distribuito, preferendo il più sicuro sistema del registro centralizzato, garantito da una autorità centrale.

10 https://www.investopedia.com/terms/d/distributed-ledgers.asp
11 Sul punto: "Blockchain e smart contract: le novità previste dal Decreto semplificazioni", di Galli Marco e Garotti Licia - http://www.quotidianogiuridico.it/documents/2019/02/26/blockchain-e-smart-contract-le-novita-previste-dal-decreto-semplificazioni
12 Per una breve definizione: https://it.wikipedia.org/wiki/Doppia_spesa
13 In passato era noto come il "problema dei generali bizantini", per una compiuta illustrazione: https://www.cryptominando.it/2018/07/25/problema-generali-bizantini-bitcoin/

La prima vera soluzione informatica al problema del consenso distribuito si deve a tale Satoshi Nakamoto[14] il quale ha ideato i bitcoin: un sistema di pagamento basato su un registro distribuito che non richiede la presenza di una banca per funzionare, e nel quale le registrazioni dei trasferimenti di (cripto)valuta vengono archiviate in una catena di blocchi (c.d. blockchain) attraverso un meccanismo informatico noto come "proof of work", che consiste in un complesso (quanto ingegnoso) meccanismo matematico volto a consentire a nodi di una rete (che non si conoscono tra loro) di raggiungere ugualmente il consenso nella validazione delle transazioni.

Invero, anche la soluzione offerta dai bitcoin per il raggiungimento del consenso distribuito, per quanto geniale ed innovativa, ha già dimostrato di presentare numerosi problemi (di lentezza, di costi in termini energetici, ecc.) che hanno spinto gli informatici a sperimentare nuovi e differenti sistemi[15] di consenso distribuito.

Ciò che qui interessa, tuttavia, non è stabilire se tali metodi siano o meno efficaci, né mettere in rilievo le pur esistenti problematiche che permangono anche nei registri di tipo distribuito; ciò che qui interessa è chiarire il fatto che qualunque registro distribuito deve necessariamente confrontarsi con il problema della formazione del consenso distribuito, e con il meccanismo di "remunerazione" che ne dovrebbe essere alla base.
Se infatti, si demanda ad una collettività il compito di effettuare delle validazioni in un registro, occorre anche porsi il problema di creare un incentivo economico senza il quale, ben presto, nessuno sarebbe disposto a partecipare alla tenuta del registro.
Non è un caso, infatti, che in tutti i principali registri distribuiti attualmente in funzione si assista anche alla presenza di un ecosistema di remunerazioni.

La normativa in esame, invero, non affronta minimamente alcuno di questi aspetti.

E se da un lato ciò è un bene, visto che la continua ricerca di innovativi modelli matematici rischierebbe di essere frustrata da troppo rigide definizioni normative, dall'altro una simile dimenticanza potrebbe anche ingenerare l'errata convinzione che – ai fini di legge – non sia affatto necessaria la implementazione di un meccanismo di consenso distribuito.

Una simile affermazione, ove fosse proposta, non può tuttavia essere condivisa.

E ciò non tanto perché astrattamente impossibile[16], quanto piuttosto perché un registro distribuito, ma al tempo stesso posto sotto il controllo di una "autorità" o di una ristretta cerchia di soggetti, difficilmente potrebbe rispettare il requisito di essere "*non alterabile e non modificabile*" richiesto espressamente dalla norma.

Invero, da più parti è stato evidenziato che nessun registro distribuito è – in astratto – inalterabile ed immodificabile[17], se attaccato con la dovuta "potenza di calcolo", per cui, se ciò è vero, allora ne consegue che il significato dell'inciso normativo non può essere inteso nel senso di imporre garanzie

14 Pseudonimo sotto il quale si cela il teorizzatore (o i teorizzatori) dei bitcoin.
15 Per una disamina si segnala: "Introduzione ai sistemi di consenso: Proof-of-Work e Proof-of-Stake" di Francesco Galanti https://medium.blockchainedu.net/introduzione-ai-sistemi-di-consenso-proof-of-work-e-proof-of-stake-e6564ddad6aa
16 E' possibile infatti immaginare registri distribuiti c.d. "permissioned" (cioè registri che, seppure in cui vi sia una certa forma di controllo nell'accesso o nel loro utilizzo).
17 Anche le blockchain pubbliche più conosciute, Bitcoin ed Ethereum, possono essere alterate con il consenso della maggioranza dei nodi e, perciò, esposte ai cosiddetti attacchi del 51%. I sistemi finora teorizzati semplicemente rendono difficile, ma non impossibile, un attacco al registro distribuito.

di assoluta inalterabilità ed immodificabilità[18]. Esso allora dovrà essere necessariamente inteso come sinonimo di assenza di un soggetto dotato *ab origine* del potere di alterare o modificare il registro. In pratica, la norma – in coerenza con la natura stessa dei registri distribuiti – richiede espressamente che non vi sia alcuna autorità che sovrintenda al registro[19].

Ciò, quindi, rende la normativa in esame del tutto incompatibile con tutti quei registri distribuiti che tuttavia non prevedano anche una formazione altrettanto distribuita del consenso.
Il motivo di questa limitazione, non essendo di tipo tecnico (ben potendo uno smart contract girare su registri permissioned o addirittura su registri di tipo centralizzato), dovrà essere ricercato nella *ratio legis*: se lo smart contract deve essere fonte di obbligazione e di vincolo per le pari, esso non può certo essere collocato all'interno di un registro su cui "qualcuno", non dotato (ex lege) dei requisiti di garanzia e terzietà di norma riconosciuti allo Stato, abbia facoltà e poteri di intervento o modifica; il potenziale danno per il cittadino sarebbe evidente.

Insomma, la garanzia del cittadino o proviene dallo "Stato", attraverso il ricorso ad una autorità statale (Agenzie delle Entrate, Anagrafe, ecc.) come avviene negli attuali registri centralizzati, oppure dovrà provenire della "collettività" attraverso la realizzazione nel registro distribuito di una sorta di esercizio diretto del potere democratico.

Se tale è la ricostruzione, tuttavia, emerge in tutta evidenza un'ulteriore lacuna del dettato normativo: poiché abbiamo sopra chiarito che la garanzia di inalterabilità ed immodificabilità di un registro distribuito dipende direttamente dalla sua maggiore o minore diffusione, quanto deve essere distribuito un registro affinché sia considerato affidabile? Questo è un aspetto che la norma non disciplina affatto.

7. SMART CONTRACT E TECNOLOGIE BASATE SU REGISTRI DISTRIBUITI

Alla luce della disamina che precede, sarà allora forse possibile trarre alcune considerazioni in relazione alle conseguenze derivanti dall'obbligo (imposto dalla norma in esame) per gli smart contract di operare necessariamente attraverso tecnologie basate su registri distribuiti.

In primo luogo, va evidenziato il fatto che tale imposizione evidentemente deriva da una espressa volontà del legislatore, posto che uno smart contract potrebbe benissimo funzionare anche all'interno di un registro di transazioni di tipo centralizzato, per cui tale previsione appare – di fatto – introdurre una limitazione di operatività degli smart contract.
Tale limitazione, tuttavia, non è affatto di poco conto, poiché essa rischia di far dipendere il riconoscimento legale di uno smart contract da una verifica prettamente di tipo tecnico circa l'effettivo utilizzo (o meno) di una "vera" tecnologia basata su un registro distribuito e non di una tecnologia basata su un registro centralizzato, ma "cammuffata".
In tale ottica, assume rilevanza la mancanza sopra evidenziata circa l'assenza di una previsione normativa relativa alla soglia minima oltre la quale un registro possa dirsi effettivamente distribuito. E' infatti evidente a chiunque che immaginare un registro distribuito (ossia realizzato su una architettura informatica di tipo distribuito), ma in concreto affidato solo ad uno o due nodi, finisce per realizzare un registro che in ben poco si differenzia da un registro centralizzato.

18 Si tratterebbe, infatti, di un requisito impossibile tecnicamente da raggiungere o da garantire, con la conseguenza che l'intera normativa rischierebbe di non trovare mai applicazione.

19 Per ulteriore chiarezza, il riferimento della norma a registri distribuiti non alterabili o modificabili non deve essere letto in senso assoluto (posto che non esiste un sistema informatico in assoluto non alterabile o modificabile), quanto piuttosto nel senso che in essi non deve essere prevista alcuna figura che abbia il potere (o anche solo la teorica possibilità) di alterare o modificare il registro.

In secondo luogo, la norma richiede che lo smart contract "**operi su**" un registro distribuito e non semplicemente che si appoggi ad esso.
Ciò significa che non sarà sufficiente utilizzare il registro distribuito solo per "provare l'esistenza" di uno smart contract (ad esempio memorizzando in esso l'hash – o impronta), ma sarà necessario che l'intero smart contract sia custodito ed operante all'interno del registro distribuito[20].

Infine uno smart contract sarà autonoma fonte di vincolo per le parti contraenti solo se esso opererà su registri distribuiti dotati anche di meccanismi distribuiti di formazione del consenso alle registrazioni, senza i quali non potrebbe dirsi rispettato il principio normativo di "inalterabilità ed immodificabilità" nel senso sopra individuato.

Michele Manente

20 Sul punto, la somiglianza del modello normativo con quello posto alla base della Piattaforma Ethereum è evidente.