GLI SMART CONTRACTS SPIEGATI SEMPLICEMENTE

Sommario

INTRODUZIONE

Oggigiorno è impossibile non incappare nei termini "blockchain", "NFT", "criptovaluta", "metaverso" o "smart contract", tutti afferenti alle innovazioni informatiche rese possibili dalla Distributed Ledger Technology (la tecnologia alla base della blockchain su cui tutte le altre innovazioni si appoggiano).

C'è molto entusiasmo sull'argomento, ma non altrettanta chiarezza, e le novità che si comprendono meno appaiono spesso più prorompenti di quello che in realtà sono.

In questa breve guida ci occuperemo degli smart contracts, che sono in un certo senso il motore attivo di questa rivoluzione digitale e che si riveleranno una tecnologia prorompente anche una volta che la polvere sollevata dall'entusiasmo che circonda questa rivoluzione si sarà posata.

CODICE E BLOCKCHAIN

Prima di spiegare cos'è uno smart contract è necessario fare una breve premessa sui programmi per blockchain.

È ormai noto a tutti che la blockchain, la principale fra le innovazioni permesse dalla Distributed Ledger Technology, è un registro digitale formato da blocchi di dati (da cui il nome), validati e iscritti nel registro attraverso un processo decentralizzato, e salvato su molteplici computer (detti nodi) così da garantirne l'immutabilità e la resistenza nel tempo.

> *Il termine Distributed Ledger Technology (sigla DLT) indica proprio un registro digitale replicato (distribuito) su più computer (nodi) e identifica la caratteristica essenziale di una serie di innovazioni informatiche delle quali la blockchain è solamente la più usata e diffusa.*

Trattandosi di un registro, viene istintivo pensare che sia possibile registrarvi unicamente informazioni, come ad esempio un Bitcoin con indicazione del suo proprietario e, successivamente, la transazione che accerta il passaggio di proprietà di quel Bitcoin a un altro soggetto.

Quel che i più ancora ignorano è che, invece, su una blockchain è possibile salvare altro rispetto a meri e inerti dati.

Infatti, sulla blockchain è possibile registrare anche codice informatico che può dare vita a programmi che vengono eseguiti direttamente sulla blockchain, dopo essere attivati (o come si dice in gergo tecnico "chiamati") da un utente o da un altro programma.

Sulle blockchain, quindi, è possibile "installare" veri e propri programmi informatici, utilizzando la blockchain come una sorta di grande computer virtuale e distribuito. La blockchain più nota e utilizzata a questo scopo è la blockchain Ethereum il cui computer virtuale e distribuito è detto Ethereum Virtual Machine (EVM).

> *Una macchina virtuale (Virtual Machine) è un computer che invece di essere costituito da componenti hardware (CPU, memoria RAM ecc.) viene emulato da un altro computer, che impiega le proprie risorse hardware per simulare un computer dalle precise caratteristiche tecniche. Nel nostro caso la macchina virtuale viene emulata dai nodi della blockchain.*

SMART CONTRACT: COS'È

Data la premessa, è facile intuire che lo smart contract è uno dei tipi di programmi che è possibile "installare" ed eseguire su una blockchain o, meglio, sulla macchina virtuale emulata dalla blockchain.

Lo smart contract non ha una funzione predeterminata e sempre uguale ma può essere programmato in modo da raggiungere differenti scopi. C'è, tuttavia, una costante nel funzionamento di tutti gli smart contracts e che permette di darne una definizione unitaria.

Lo smart contract è un programma che esegue una o più determinate azioni al verificarsi di una o più condizioni consentendo a due o più soggetti di eseguire una prestazione o transazione.

Un modo semplice per spiegare come funziona uno smart contract è usare come esempio lo smart contract ante litteram per antonomasia: il distributore automatico.

Immaginiamo un distributore di bevande e un acquirente interessato a comprare una gazzosa. L'acquirente digita sulla pulsantiera il codice associato dal distributore allo scompartimento dove sono stoccate le bottigliette di gazzosa e introduce le monete corrispondenti al prezzo della bibita. Il distributore verifica che le monete corrispondano al prezzo che nella sua memoria è associato al codice inserito dall'acquirente e attiva lo scompartimento corrispondente, così da far cadere nell'area di raccolta una bottiglietta di gazzosa.

Strettamente parlando, nessuno ha venduto la gazzosa all'acquirente. Il distributore appartiene a qualcuno che si è premunito di caricarlo di bibite e passerà a ritirare i soldi, quindi un venditore c'è, ma questo venditore non si è dovuto preoccupare di stipulare la vendita direttamente con l'acquirente. L'acquirente ha fatto tutto da solo attraverso il distributore, che a sua volta è programmato per eseguire un'azione (liberare la bibita) quando si verifica il pagamento del prezzo (l'inserimento delle monete).

Azione (liberare la bibita) a seguito di avverarsi di una condizione (selezione e pagamento del prezzo in monete) realizzando così la prestazione (consegna del bene bibita) prevista dal contratto (vendita).

Gli smart contracts rispondono agli stessi principi e alle medesime finalità dei distributori automatici, solo sono, come è lecito attendersi, molto più flessibili e complessi.

Il tipo di smart contract più diffuso è quello che consente di eseguire transazioni di criptovalute. Lo scambio di criptovalute, forse la funzione per eccellenza di tutte le blockchain pubbliche, avviene quindi attraverso smart contract. Si tratta di smart contracts molto semplici che si limitano, quando chiamati, a trasferire la quantità indicata di criptovaluta da un wallet emittente a uno ricevente, anch'essi indicati al momento di chiamare lo smart contract.

> *Il **wallet** è un asset digitale che contiene una serie di chiavi crittografiche che solo chi possiede le credenziali di accesso al wallet può utilizzare. Una chiave pubblica, che identifica il wallet, e delle chiavi private, che permettono al proprietario di attivare altri asset digitali come criptovalute, NFT e smart contracts.*
> *Nonostante il nome (portafoglio) è più semplice immaginarselo come un mazzo di chiavi, ognuna delle quali attiva una serratura.*

Tuttavia, gli smart contracts possono realizzare operazioni anche molto complesse, come ad esempio la gestione delle DAO (Decentralized Autonomous Organizations, in sostanza le società e le associazioni che nascono, crescono e si organizzano tramite blockchain), che richiede molteplici e complessi smart contracts che interagiscono fra loro.

SMART CONTRACT E MONDO ESTERNO: GLI ORACLES

Lo smart contract, quindi, è un programma su blockchain il cui scopo è eseguire in automatico operazioni corrispondenti a transazioni e prestazioni al verificarsi di determinate condizioni.

Appare evidente il vantaggio dato dall'automazione di una prestazione contrattuale. Al contrario di due contraenti umani, lo smart contract non può agire in malafede, perdere tempo, eseguire parzialmente la prestazione od opporre a una delle parti una diversa interpretazione del contratto. Lo smart contract garantisce a chi ne fa uso che, verificatesi le condizioni previste dal contratto, le conseguenti prestazioni verranno eseguite immediatamente e senza fallo.

Tuttavia, per permettere agli smart contracts di poter gestire rapporti che non si limitino a operare su criptovalute, token, NFT o altre risorse native della blockchain su cui "girano" è necessario utilizzare un altro tipo di programma, esterno alla blockchain ma in grado di interagire con questa e gli smart contracts.

Questo tipo di programma si chiama oracle e la sua funzione è quella di reperire informazioni dal mondo esterno e trasmetterle allo smart contract o viceversa. In sintesi, gli oracles sono i ponti che collegano gli smart contracts col mondo reale, permettendo loro di reagire a eventi esterni alla blockchain e di influenzare o innescare eventi esterni.

Per spiegare meglio come uno smart contract utilizza gli oracles possiamo usare l'esempio di uno smart contract programmato per rimborsare il biglietto di un volo in caso di cancellazione.

Questo smart contract è programmato per disporre il bonifico di una somma pari al costo del biglietto aereo, da parte della compagnia aerea o di una assicurazione, sul conto dell'acquirente se il volo viene cancellato.

I dati relativi al soggetto pagante e al soggetto beneficiario vengono inseriti dalle parti nello smart contract, assieme alla somma da rimborsare e al numero identificativo del volo. Un programma oracle connesso ai servizi online che monitorano lo stato dei voli controlla lo stato dello specifico volo e, in caso di cancellazione, trasmette l'informazione allo smart contract, attivandolo. Lo smart contract, a questo punto, attiva un altro oracle, connesso coi servizi bancari del soggetto che deve effettuare il rimborso, che metterà in moto la procedura di pagamento.

Attraverso l'uso di programmi oracle sempre più sofisticati, e in grado di interagire con un numero sempre maggiore di realtà informatizzate (banche, aeroporti, società, enti pubblici ecc.), gli smart contracts potrebbero in futuro diventare lo standard per l'esecuzione dei più svariati rapporti contrattuali.

Tuttavia, perché un futuro di contratti automatizzati diventi possibile, è necessario affrontare la questione della capacità o meno degli smart contracts di soddisfare i requisiti giuridici che un contratto deve avere.

GLI SMART CONTRACTS SOTTO IL PROFILO LEGALE: LO SMART CONTRACT COME STRUMENTO

Nonostante il nome, dal punto di vista legale lo smart contract non è un contratto, allo stesso modo in cui non è un contratto un distributore automatico.

Similmente al distributore automatico lo smart contract è uno strumento tecnico che le parti che stipulano fra loro un contratto possono usare per darvi esecuzione.

Riprendiamo l'esempio dello smart contract programmato per risarcire il viaggiatore in caso di annullamento del suo volo.

Il fatto che lo smart contract riporti i codici IBAN del viaggiatore e del soggetto che si è impegnato a risarcirlo in caso di annullamento del volo e le istruzioni per procedere all'eventuale rimborso, non è di per sé sufficiente per sostenere l'esistenza di un contratto e a vincolarvi le parti.

Viaggiatore e soggetto rimborsante creano lo smart contract perché hanno già stretto un accordo contrattuale, e lo smart contract è solo il mezzo scelto per realizzare quanto previsto da questo contratto. Le parti avrebbero potuto realizzare lo stesso risultato incaricando un terzo soggetto, umano, di controllare l'eventuale cancellazione del volo e di disporre, dotato di apposita procura, il bonifico per conto del soggetto tenuto al risarcimento. Sicuramente non considereremmo questo terzo soggetto, e le istruzioni che ha ricevuto, "il contratto".

L'esistenza del contratto, quindi, risiederà fuori dallo smart contract, nella manifestazione espressa - verbale o scritta - dell'accordo fra le parti.

Al massimo, se lo smart contract è sufficientemente dettagliato con riguardo ai soggetti che lo hanno creato e all'oggetto dell'azione che andrà a eseguire, la sua creazione e l'inserimento di questi dati potrebbero essere considerati fatti concludenti: comportamenti diretti in modo inequivocabile all'accettazione di una proposta contrattuale. I fatti concludenti costituiscono una modalità alternativa, rispetto alla manifestazione espressa della volontà delle parti, per la conclusione di un contratto.

Eccezion fatta per questa ipotesi eccezionale, di fronte a uno smart contract quello che bisogna chiedersi, dal punto di vista legale, è quale sia il contratto che vi sta dietro.

Continuando con il nostro esempio, il contratto che prevede il risarcimento del biglietto sarà parte del più ampio contratto stipulato fra il viaggiatore e la compagnia di volo per l'acquisto del biglietto, oppure un apposito contratto assicurativo stipulato con l'assicurazione.

Solo individuando il contratto è possibile risalire alla piena volontà delle parti che hanno creato lo smart contract, e all'insieme delle prestazioni che compongono l'accordo e che dallo smart contract non risultano. Sempre rimanendo sul nostro esempio, lo smart contract non ci dice niente sull'obbligo del viaggiatore di pagare il prezzo del biglietto, o sul premio che questi si è impegnato a pagare alla assicurazione in cambio del risarcimento in caso di cancellazione del volo.

Lo smart contract, quindi, è lo strumento tecnico scelto dalle parti di un contratto per eseguire tutte o parte delle prestazioni previste dal contratto.

GLI SMART CONTRACTS SOTTO IL PROFILO LEGALE: LO SMART CONTRACT COME ATTO GIURIDICO

Premesso che lo smart contract, di per sé, non è dotato di valore legale, è tuttavia possibile attribuirgli valore legale. Si parla, in questi casi, di legal smart contract.

Perché uno smart contract possa diventare un legal smart contract è necessario che contenga al suo interno, oltre al codice vero e proprio che ne assicura il funzionamento, gli elementi essenziali del contratto che il codice informatico aiuterà a eseguire. Esistono due modi per inserire questo contenuto legale nello smart contract.

Il primo modo è attraverso un rimando a un contratto. Si tratta del metodo più semplice, mutuato dall'esperienza delle licenze in ambito informatico.

Nel codice dello smart contract, consultabile da chiunque, viene inserito un riferimento a un contratto, anch'esso liberamente consultabile, assieme a un termine convenzionale o a una frase che stabilisce che lo smart contract è sottoposto alle condizioni di quel contratto.

Le parti, stipulando lo smart contract, accettano di vincolarsi alle previsioni del contratto richiamato ed è grazie a questo rimando che lo smart contract acquista valore legale.

Esattamente come avviene con i software e le relative licenze di utilizzo, dove l'utilizzo del software da parte dell'utente reso edotto delle condizioni della licenza comporta accettazione della stessa.

I vantaggi di questo tipo di legal smart contract sono l'immediatezza data dal dover contenere un semplice rimando al contratto, il poter applicare lo stesso contenuto contrattuale a più smart contracts senza dover intervenire pesantemente nel loro codice e la possibilità di modificare le condizioni contrattuali successivamente alla creazione del legal smart contract, in quanto il contratto risiede fuori da questo - solitamente su una pagina web dove è liberamente consultabile assieme a una indicazione delle modifiche occorse nel tempo.

Lo svantaggio è che, essendo il contratto di fatto scritto altrove, vi possono essere dubbi e contenziosi sul suo contenuto e sull'effettiva volontà di una delle parti di vincolarsi al contratto.

Nei software, infatti, ci sono diversi metodi per dare modo all'utente di visionare la licenza prima di installare o comunque usare il software.

È possibile far apparire un avvertimento a schermo durante l'installazione, con un link che rimandi alla licenza, o addirittura riportare la licenza in una finestra, costringendo l'utente a scorrerne il testo e a manifestare la propria accettazione prima di proseguire con l'installazione o utilizzo.

Con gli smart contracts queste soluzioni non sono, al momento, possibili e il legal smart contract viene creato o attivato senza che le parti vedano prima il testo del contratto richiamato nel codice.

Oggi, il più delle volte, questo non costituisce un problema perché le parti partecipano assieme alla creazione del legal smart contract e, quindi, redigono (o scelgono, in caso di modelli di contratto standard) assieme un contratto del cui contenuto hanno conoscenza e che hanno approvato.

Tuttavia, più si andrà avanti più accadrà che, esattamente come per i software, vi sarà una parte che predispone il contenuto del legal smart contract e un'altra parte che si limiterà ad aderire al legal smart contract attivandolo.

In questa circostanza, la parte che aderisce al legal smart contract potrebbe non avere conoscenza del contenuto del contratto che è andato a sottoscrivere. Potrebbe anche non sapere che il codice richiama un contratto!

Questo comporta il rischio che, al momento di venir chiamato a rispondere delle proprie responsabilità contrattuali, questi opponga la sua incolpevole ignoranza dell'esistenza del contratto e/o del suo contenuto.

E anche fosse provato che la parte sapeva che lo smart contract che è andato ad attivare costituiva un contratto detta parte potrebbe contestare (a torto o a ragione) che il contenuto del contratto richiamato dal legal smart contract non sia, al momento in cui sorge il contenzioso, lo stesso di quando il legal smart contract è stato attivato.

Insomma, la formazione di un legal smart contract attraverso il richiamo di un contratto esterno rischia di creare incertezza sul suo contenuto e offre il destro a contestazioni.

Un altro svantaggio che va considerato è che ogni modifica unilaterale al contratto richiamato dal legal smart contract rischia di restare priva di effetto nei confronti dell'altra parte se questa non la accetta o quantomeno non gli viene comunicata.

Il secondo modo è attraverso l'inserimento del contratto nel codice. In questo caso il contratto viene scritto direttamente nel codice dello smart contract sotto forma di commento (un pezzo di codice che non fornisce istruzioni al computer ma è destinato a essere letto da esseri umani) e il legal smart contract si considera stipulato nel momento in cui viene creato.

Il vantaggio di questo tipo di legal smart contract è che, contenendo direttamente il contratto, è pienamente autosufficiente, sia sotto il profilo legale che tecnico, e il suo essere caricato in blockchain offre al contenuto legale le garanzie di certezza e immodificabilità tipiche della blockchain.

L'immodificabilità, tuttavia, costituisce anche il principale difetto di questo tipo di contratto che non può essere modificato successivamente, neanche per correggere eventuali errori nella sua formulazione.

Per comprendere meglio prendiamo sempre l'esempio dello smart contract pensato per rimborsare il prezzo del biglietto aereo in caso di cancellazione.

Ipotizziamo che il contratto venga stipulato fra il viaggiatore e una compagnia di assicurazione e che questa chieda, in cambio dell'impegno al rimborso, un premio di "50,00 euro". Nel caso di un legal smart contract con il contenuto del contratto scritto direttamente nel codice basterebbe caricare il legal smart contract privo di una virgola per trasformare il premio in "5000 euro"!

A quel punto le parti si troverebbero con un contratto scritto e salvato sulla tecnologia che più di tutte ne garantisce la certezza e immodificabilità che, però, non corrisponde alla loro volontà. Per risolvere il problema dovranno stipulare un accordo scritto che superi e modifichi quella parte del legal smart contract.

GLI SMART CONTRACTS SOTTO IL PROFILO LEGALE: IL PROBLEMA DELLA IMMODIFICABILITÀ

L'immodificabilità del codice del legal smart contract può poi originare un altro problema, che investe tanto i legal smart contracts formulati scrivendo al loro interno il contenuto contrattuale quanto quelli formulati rimandando a un contratto esterno.

Infatti, mentre le parti di contratto che non vengono eseguite dallo smart contract possono essere modificate comunque attraverso un accordo successivo preso fuori dalla blockchain, le parti che vengono eseguite non possono essere modificate senza creare una differenza fra quanto previsto dal contratto e quanto effettivamente eseguito.

Prendiamo sempre l'esempio del legal smart contract per il rimborso del biglietto aereo e immaginiamo che il soggetto tenuto al rimborso sia la compagnia aerea.

Il legal smart contract può contenere non solo le condizioni contrattuali che regolano l'eventuale rimborso del biglietto, poi eseguito dalla parte informatica del legal smart contract, ma anche le condizioni che regolano il ritiro del biglietto e il check-in.

Ipotizziamo che nel codice del legal smart contract, o nel contratto cui questo rimanda, venga stipulato che il biglietto verrà consegnato via e-mail al viaggiatore e il check-in effettuato online entro due giorni dal volo.

Le parti possono accordarsi successivamente per modificare queste clausole, ad esempio stipulando che il biglietto venga messo a disposizione del viaggiatore in aeroporto e che questi effettui il check-in di persona un'ora prima della partenza, senza particolari problemi. Se il legal smart contract richiama un contratto esterno basterà modificare quest'ultimo. Se contiene le previsioni contrattuali nel codice basterà che le parti stipulino un accordo a parte che superi quanto scritto nel codice.

Se, però, le parti volessero modificare il soggetto tenuto all'eventuale rimborso del biglietto, ad esempio dalla compagnia aerea a una sua società controllata, questo non sarebbe possibile dato che il legal smart contract contiene, nella parte di codice destinata a essere eseguita dalla macchina virtuale, il codice IBAN della compagnia, dal quale far partire il rimborso.

Una modifica contrattuale concordata fra le parti per cambiare il soggetto rimborsante si scontrerà col fatto che, in caso di cancellazione del volo, il legal smart contract farà partire il pagamento dal conto della compagnia aerea che, a quel punto, potrà solo farsi risarcire dalla società controllata che le parti avevano individuato come nuovo soggetto tenuto al rimborso del biglietto.

Le uniche possibilità, per le parti, di evitare ciò sono non attivare il legal smart contract e crearne un altro, soluzione di sicuro non ottimale, oppure essere così accorte, in fase di creazione, da prevedere tutte le possibili modifiche che potrebbero essere apportate successivamente al contratto e prendere gli accorgimenti tecnici per renderle compatibili con il legal smart contract, ad esempio facendo sì che l'IBAN da cui far partire il pagamento possa essere inserito nel legal smart contract dopo la sua creazione.

Quest'ultima soluzione, tuttavia, richiede molta perizia tecnica, rende il codice più complesso e, soprattutto, depotenzia molto il vantaggio dell'esecuzione immediata e certa assicurata dall'utilizzo di uno smart contract. Nel nostro esempio, se nessuno caricasse l'IBAN dal quale deve partire il rimborso in caso di cancellazione, il legal smart contract non potrebbe funzionare.

È il caso di precisare che la possibilità di ritrovarsi con un contrasto fra le istruzioni informatiche e il contenuto del contratto affligge anche gli smart contract privi di valore legale e che fungono da strumento tecnico per eseguire un contratto stipulato fra le parti fuori dallo smart contract e dalla blockchain. Anche in questo caso ogni modifica al contratto che va a toccare le condizioni e le azioni che lo smart contract deve realizzare si scontra con il problema appena esaminato.

GLI SMART CONTRACTS SOTTO IL PROFILO LEGALE: LA STIPULAZIONE SU BLOCKCHAIN

Come in precedenza scritto, un legal smart contract impegna le parti al rispetto del contratto, ivi contenuto o cui fa riferimento, nel momento in cui lo stipulano. Questo passaggio richiede un approfondimento.

Per propria natura la blockchain opera in un ambiente di pseudonimi, cioè in un ambiente dove i soggetti non sono direttamente indentificati o identificabili.

Infatti, nel momento in cui interagiamo con una blockchain lo facciamo attraverso un wallet, un "mazzo" di chiavi crittografiche che ci permette di conservare e operare coi nostri asset digitali.

Ogni wallet viene identificato dalla propria chiave crittografica pubblica che ne costituisce l'indirizzo (il riferimento necessario per coinvolgere il wallet in una operazione). L'indirizzo del wallet funge anche da suo nome, essendo l'elemento che distingue in modo univoco quel wallet da tutti gli altri.

L'indirizzo è un codice alfanumerico e non è possibile risalire da questo codice al proprietario del wallet, cioè al soggetto che ne possiede le credenziali di accesso e che compie operazioni su blockchain tramite questo.

Di conseguenza, quando operiamo nell'ambiente blockchain, compresa la creazione e attivazione di smart contracts, lo facciamo non col nostro nome e cognome ma con uno pseudonimo, l'indirizzo del wallet, e nessuno può da questo risalire alla nostra identità.

L'utilizzo degli pseudonimi nell'ambiente blockchain costituisce una complicazione per la stipula dei legal smart contracts.

Per aversi un contratto legalmente valido non basta, infatti, la presenza delle condizioni contrattuali ma serve anche che vi sia la manifesta volontà delle parti di aderire all'accordo contrattuale e di vincolarsi al contratto. L'accordo delle parti può manifestarsi in diversi modi ma, nella maggior parte dei casi, si manifesta al momento della stipula del contratto attraverso la sua sottoscrizione da parte dei soggetti stipulanti, che sia tramite firma autografa o attraverso una sottoscrizione digitale che permette di ricondurre, grazie a degli accorgimenti tecnici, la firma digitale a un soggetto precisamente individuato.

La riconducibilità della manifestazione dell'accordo contrattuale ai soggetti che diventano parti del contratto è, quindi, essenziale per la validità del contratto stesso.

Nell'ambito degli smart contracts la manifestazione dell'accordo delle parti è ostacolata dal fatto che, aprendo il codice di uno smart contract, non è possibile risalire alle identità di chi lo ha creato ma solo ai loro pseudonimi rendendo così impossibile capire se le parti coinvolte dallo smart contract si sono effettivamente accordate per la sua creazione.

Riprendiamo l'esempio dello smart contract per il rimborso del biglietto aereo. Il fatto che, una volta attivato, lo smart contract trasferisca dei soldi dal conto bancario della compagnia di volo Alpha Airlines al conto bancario di Mario Rossi non costituisce, di per sé, prova che i proprietari dei wallet tramite i quali è stato creato lo smart contract siano proprio Alpha Airlines e Mario Rossi.

Lo smart contract potrebbe essere stato creato da soggetti diversi in possesso delle necessarie informazioni tecniche sul volo e sui conti correnti di Alpha Airlines e Mario Rossi, o comunque ognuna delle parti potrebbe rifiutarsi di riconoscere gli obblighi risultanti dal smart contract disconoscendo che il wallet coinvolto sia a sé riferibile.

Fintanto che si tratta di smart contract semplici, la pseudonimia non costituisce un problema perché, come già detto, questo è uno strumento tecnico e il contratto che vi è dietro esiste fuori dalla blockchain.

La prova dell'accordo delle parti, quindi, sarà data dalla stipula del contratto esterno alla blockchain.

Il problema si pone, invece, nel momento in cui, attraverso un legal smart contract, si intende stipulare il contratto nella blockchain. In questo la valida stipula del contratto è impedita dalla pseudonimia dei soggetti che creano il legal smart contract.

Per risolvere il problema è intervenuto direttamente il legislatore, il quale, nel definire lo smart contract, ha precisato che questo può ottenere il valore di accordo scritto – equiparando, quindi, la stipula di un legal smart contract a quella di un contratto scritto – solo con l'identificazione dei soggetti "sottoscrittori".

L'art. 8 ter del D.L. 135/2018 stabilisce che l'identificazione deve avvenire con un procedimento informatico che risponda ai requisiti fissati dall'Agenzia per l'Italia Digitale con linee guida che questa avrebbe dovuto adottare entro tre mesi dalla conversione in legge del decreto-legge in esame. Tuttavia, oggi queste linee guida non sono ancora state adottate.

> ***D.L. 135/2018, art. 8 ter, commi 1 e 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.*

In assenze delle linee guida si sono sviluppate due scuole di pensiero sulla possibilità o meno di stipulare legittimamente un legal smart contract.

La prima ritiene che, fintanto che non sarà individuato dall'Agenzia per l'Italia Digitale il procedimento per l'identificazione informatica dei sottoscrittori, questa possibilità non sussiste e, di conseguenza, che l'inserimento (direttamente o tramite riferimento) in uno smart contract di previsioni contrattuali costituisce, al massimo, prova del contenuto di un contratto che trova il suo fondamento altrove.

La seconda, invece, ritiene che in presenza di elementi di prova in grado di attribuire univocamente i wallet coinvolti nella sua creazione alle parti del contratto sia già possibile attribuire valore legale a un legal smart contract, in ragione del riconoscimento di cui all'art. 8 ter D.L. 135/2018.

Questi elementi di prova possono essere forniti in diversi modi, l'importante è che diano sufficiente certezza della riconducibilità del wallet a un soggetto determinato.

Una possibile modalità potrebbe essere attraverso la registrazione in blockchain di un file in possesso solo del proprietario del wallet che effettua la registrazione. Solitamente la registrazione di un file non avviene caricando direttamente il file in blockchain ma attraverso la registrazione in blockchain del suo codice hash. Chiunque possa esibire il possesso del file il cui codice hash combacia con quello registrato può provare di essere il proprietario del wallet che ha effettuato la registrazione.

> *Il codice o impronta hash è un codice alfanumerico che si ottiene applicando una funziona crittografica particolare a un file.*
> *Dal codice hash non è possibile ricostruire il file di partenza. Il file di partenza darà sempre lo stesso codice hash, salvo venga modificato. Anche la più impercettibile modifica di un bit porterebbe alla creazione di un codice hash completamente differente.*
> *Per queste sue caratteristiche, il codice hash viene considerato il sistema più semplice ed efficiente per registrare file in blockchain. In pratica è come se invece di registrare direttamente il file se ne registrasse l'impronta digitale, provando in questo modo che chi ha effettuato la registrazione possedeva il file cui l'impronta appartiene.*

Un altro sistema potrebbe essere prevedere un'operazione su blockchain da eseguire al momento di dimostrare la proprietà del wallet. Ad esempio, registrare in blockchain una stringa di testo corrispondente a una frase ben precisa (es. "La rana in Spagna gracida in campagna"). Se la frase registrata dal wallet X

corrisponde alla frase che Caio ha dichiarato che avrebbe registrato si avrà la prova del suo essere il proprietario del wallet X.

Questi sono solo due esempi di come si potrebbe provare la proprietà di un wallet e, di conseguenza, identificare le parti di un legal smart contract.

Chi volesse aderire a questa seconda scuola di pensiero, nella temporanea assenza di un sistema riconosciuto dalla legge, deve quindi preliminarmente accordarsi con l'altra parte del contratto su quale metodo di prova si intende adottare, al fine di ridurre i rischi di contenzioso successivamente alla stipula del legal smart contract.

LA PORTATA APPLICATIVA ATTUALE DEGLI SMART CONTRACTS

Da questa veloce analisi relativa al profilo legale degli smart contracts abbiamo evidenziato come, a dispetto del nome, questi programmi non siano sempre contratti veri e propri. Anzi, nella maggior parte dei casi si tratta soltanto strumenti impiegati per dare esecuzione a contratti tradizionali.

Solo in una minoranza di casi gli smart contracts sono contratti veri e propri e, anche in quei casi, la loro effettiva validità legale è ostacolata dalla difficoltà di trovare un sistema univoco e validato dalla legge per ricondurne il contenuto alla volontà di due o più soggetti determinati.

Nonostante queste criticità, l'utilizzo dei legal smart contracts diventerà in futuro sempre più diffusa e arriverà il giorno in cui stipularne uno sarà frequente tanto quanto accettare la licenza d'uso di un software o iscriversi a un servizio online.

Tuttavia, fino a quel momento e salvo eccezioni, gli smart contracts che verranno impiegati non potranno che essere smart contracts semplici: strumenti innovativi per dare esecuzione a contratti stipulati fuori dalla blockchain.

Di seguito, una veloce carrellata degli smart contracts attualmente più diffusi:

Smart contracts per gestire i pagamenti

Grazie alla tecnologia blockchain gli smart contracts permettono di eseguire i pagamenti nelle modalità e alle condizioni indicate senza bisogno di doversi affidare a un terzo intermediario che potrebbe rivelarsi inaffidabile e, addirittura, senza bisogno che i soggetti interessati si attivino per disporre i pagamenti.

In ambito commerciale si tratta di una enorme innovazione perché riduce enormemente il rischio di inadempimento contrattuale della controparte, che non potrà rifiutarsi di pagare, e annulla il rischio di problemi con i soggetti intermediari.

In particolare, questo impiego degli smart contracts torna utile nel caso di rapporti commerciali fra soggetti che operano in Stati o addirittura continenti differenti, cioè in quei casi dove la lontananza fra le parti aumenta il rischio di inadempimenti o problemi con gli intermediari.

Smart contracts per gestire la supply chain

Attraverso gli oracles uno smart contract può ricevere ogni tipo di dati dall'esterno, compresi quelli relativi alla movimentazione di merci.

È possibile creare un token, cioè un dato digitale registrato nella blockchain, associato a un prodotto (del quale riporta, ad esempio, il numero di serie) e attraverso uno smart contract che gestisca questo token verificare che il prodotto venga movimentato come da contratto, ottenendo anche di automatizzare le conseguenze.

Ipotizziamo che un prodotto debba essere consegnato a spese e a rischio del venditore fino a un magazzino e, una volta lì, trasportato fino alla sede dell'acquirente a spese e rischio di quest'ultimo.

Grazie allo smart contract ogni passaggio non verrebbe semplicemente accompagnato dalla consegna di documenti e dalla firma di bolle di trasporto ma verrebbe registrato anche nella blockchain. Ogni soggetto coinvolto (venditore, acquirente, vettori, magazzinieri), infatti, dopo aver effettuato la propria attività all'interno della catena di trasporto richiamerebbe, con l'aiuto di un oracle, lo smart contract inserendo l'informazione del completamento dell'attività.

Si avrebbe così il grande vantaggio di conservare traccia certa di tutti i passaggi, che diventerebbero incontestabili grazie alle garanzie di certezza, durata e immodificabilità della blockchain, eliminando le possibilità di contezioso connesse, ad esempio, a bolle consegnate ma non sottoscritte, errori di trascrizione dei dati sui documenti cartacei ecc.

In più, vi è l'automazione consentita dallo smart contract. Nel nostro esempio, la comunicazione che la merce è arrivata al magazzino potrebbe attivare lo smart contract perché comunichi la cessazione della responsabilità del venditore alla compagnia assicurativa presso il quale questi aveva assicurato la merce. Mentre a fronte dell'accettazione senza riserva da parte dell'acquirente lo smart contract può far partire il pagamento del prezzo.

I vantaggi dell'uso degli smart contracts nel campo della logistica sono potenzialmente innumerevoli.

Non-Fungible Token (NFT)

I token, in ambito blockchain, sono asset digitali che assolvono a tutta una serie di funzioni. Le stesse criptovalute sono dei token, anche se per distinguerle dagli altri le si chiama coin. I NFT sono asset caratterizzati dal fatto di non essere fungibili.

Una cosa si dice non fungibile quando non può essere sostituita da una cosa simile avente le stesse qualità. Un esempio semplice per distinguere fra cose fungibili e non fungibili è pensare alla differenza fra la valuta e i quadri.

Anche se le banconote sono fra loro solamente simili, avendo ciascuna un numero di serie che la distingue dalle altre, è indifferente possedere la banconota da 20 euro con il numero di serie che finisce in …1 o quella col numero di serie che finisce in …2, perché possiedono le medesime qualità, cioè valere 20 euro. Le banconote, quindi, sono fungibili perché ognuna può essere sostituita da una banconota della stessa divisa e taglio.

I quadri invece sono molto diversi fra loro e si può dire che due quadri diversi (per dimensioni, tecnica, soggetto, autore ecc.) non condividono altre qualità se non di essere entrambi quadri e non è affatto indifferente possederne uno rispetto all'altro. I quadri, quindi, non sono fungibili perché, essendo differente possedere un quadro rispetto a un altro, non possono essere sostituiti da altri quadri.

I NFT, pertanto, sono token che per le loro qualità non possono essere sostituiti da altri token e sono costituiti da smart contracts che all'interno del proprio codice descrivono dette qualità.

L'uso più noto dei NFT è di fungere da certificati di autenticità e di proprietà per le opere digitali. In questo modo chi possiede il NFT può vantare di essere il legittimo proprietario dell'opera digitale individuata al suo interno, solitamente attraverso il nome dell'opera e un collegamento a una risorsa online che ne contenga copia.

Questo uso è stato considerato dirompente nel mondo dell'arte, avendo aperto alla possibilità di creare una scarsità artificiale in un ambito, quello delle opere digitali, dove non è possibile parlare di "copia originale" nel senso tradizionale del termine.

Tuttavia, il potenziale commerciale dei NFT risiede nelle loro altre possibili applicazioni. Un NFT può fungere da tessera, permettendo solo a chi lo possiede di accedere agli spazi (digitali e/o fisici) esclusivi di una società, e ai servizi e prodotti che solo lì vengono erogati (ad esempio uno showroom esclusivo, uno store online riservato o un ristorante aperto solo a soci).

Un NFT può anche fungere da voucher personalizzato, con il quale la società assicura a un proprio cliente una combinazione di premi e bonus pensata unicamente per il possessore di quello specifico NFT.

Implementare i NFT nel proprio business è abbastanza semplice, basta pensare quali vantaggi si vuole garantire con il NFT, crearlo e metterlo in circolazione (assegnandolo a un proprio cliente o mettendolo in vendita). Chiunque vorrà usufruire dei relativi vantaggi dovrà solamente dimostrare di essere in possesso del NFT.

A ben vedere, si tratta di attività che potrebbero essere realizzate con altri mezzi, magari analogici, ma la gestione attraverso NFT consente di rendere il tutto molto più sicuro, semplice ed eventualmente automatizzabile.

Token di partecipazione

Un token può essere utilizzato anche per rappresentare quote di partecipazione.

È importante premettere che, al momento, un token registrato in blockchain non può sostituire asset regolati da normative particolari come, ad esempio, le azioni societarie e gli atti di comproprietà immobiliare.

Tuttavia, in tutti i casi in cui è possibile dividere il possesso, gli oneri e i vantaggi di un asset o di una attività senza dover ricorrere a formalità particolari, i token sono uno strumento sicuro e flessibile.

Possibili usi possono essere, ad esempio, legare ai token i diritti di voto in una associazione, distribuire token in cambio di finanziamenti per un progetto e una volta che sarà realizzato ricompensare i possessori dei token con delle utilità (parte dei ricavi, prodotti o servizi gratuiti ecc.).

Un uso complesso che alcune società fanno dei token è la possibilità di far partecipare le persone alla gestione di immobili attraverso token che vengono dati in cambio di soldi, che la società usa poi per l'acquisto e la manutenzione degli immobili, e che danno diritto a ricevere una somma periodica parametrata ai guadagni che la società trae dall'affitto di questi.

Insomma, anche in questo campo le soluzioni possono essere moltissime e i token mossi dagli smart contracts consentono un livello di sicurezza e automazione non raggiungibile con altri sistemi.

COME IMPLEMENTARE NELLA PRATICA GLI SMART CONTRACTS NEL PROPRIO BUSINESS

Dopo aver visto cosa sono e come funzionano gli smart contract, e alcuni esempi di applicazione, è il momento di spendere poche parole sugli aspetti più pratici della loro implementazione.

Come detto, gli smart contracts sono un esempio di programma che gira su blockchain e quindi si implementano come i normali software, con l'aiuto di un programmatore e accedendo a risorse, come server e computer, organizzate da un sistemista. Due figure, quelle dello sviluppatore software (o della società di sviluppo software) e del sistemista con le quali già collaborano la maggior parte delle società, soprattutto se hanno anche solo parte del loro business che si muove in rete.

Tuttavia, l'implementazione degli smart contracts richiede figure specializzate. Soprattutto chi crea il software deve sapere come lavorare su una virtual machine in blockchain, conoscenza non posseduta da tutti gli sviluppatori.

Una volta trovate le figure tecniche specializzate per implementare gli smart contracts, e i programmi oracle eventualmente necessari, che s'intende usare in combinazione con lo smart contract è bene, prima di partire, farsi assistere da un avvocato specializzato.

Infatti, anche se non si usano dei legal smart contracts ma degli smart contracts semplici, è necessario accordare il loro uso con i contratti stipulati con i fornitori e i clienti che ne saranno coinvolti e, soprattutto,

accertarsi che l'uso che si ha in mente non incontri degli ostacoli a livello legale. Ad esempio, perché si intende usare lo smart contract per una attività che, per legge, richiede dei requisiti formali cui questo strumento non può assolvere.

Una volta trovate le figure adatte, tuttavia, implementare gli smart contracts non risulta più complesso dell'implementazione aziendale di una qualsiasi altra tecnologia.

CONCLUSIONI

Come abbiamo visto, lo smart contract è, prima e innanzitutto, un formidabile strumento tecnico per l'esecuzione di prestazioni contrattuali.

Il suo essere liberamente programmabile, la flessibilità, la possibilità di interfacciarsi con infinite informazioni e ulteriori strumenti permessa dall'uso degli oracles e le garanzie di durata, certezza e immodificabilità offerte dalla blockchain ne fanno uno strumento che in futuro verrà sempre più utilizzato e che è destinato a sostituire molti degli strumenti e delle figure professionali cui oggi ci affidiamo per l'esecuzione delle prestazioni contrattuali.

Non solo, lo smart contract può diventare un vero e proprio atto giuridico, in grado di vincolare le parti a contratti esterni o diventare essi stessi contratti.

Tuttavia, questa ulteriore possibilità è da prendere in considerazione solo in quei casi in cui è sensato unire il contratto e lo strumento destinato a eseguirlo e questo, a mio avviso, può essere il caso di smart contract molto semplici, dove le possibilità di problemi e conflitti fra parte tecnica e legale del codice sono minime, o molto complessi, dove pressoché tutte le prestazioni contrattuali devono essere eseguite tramite lo smart contract. In quest'ultimo caso, inserire il testo legale direttamente nel codice può offrire una soluzione elegante per creare un contratto chiaro, trasparente e inequivocabile.

La creazione di uno smart contract, legal o meno, andrebbe sempre effettuata con l'assistenza di un legale che conosca tanto il diritto delle nuove tecnologie che quello del settore in cui lo smart contract andrà ad agire, ad esempio il diritto commerciale.

Vuoi utilizzare uno smart contract per il tuo business? Sei interessato a saperne di più?

Contatta RUP LEGAL & CONSULTING

info@ruplegal.com - +39 349 6458130