La rivoluzione digitale ha cambiato radicalmente la società moderna introducendo nuovi ed efficienti paradigmi che si pongono l'obiettivo di migliorare sensibilmente lo stile di vita delle persone sia in ambito sociale che lavorativo. In tale contesto sta riscuotendo grande interesse, dal punto di vista industriale e giuridico, una nuova piattaforma digitale denominata "blockchain" e le cui potenzialità innovative si stanno estendendo progressivamente, partendo dalle originarie applicazioni alle criptovalute (blockchain è il sottostante informatico della famosa criptovaluta digitale "Bitcoin") estendosi sino ad applicazioni in ambito legale con specifico riferimento al diritto contrattuale (c.d. smart contracts) al diritto bancario, finanziario, assicurativo ed informatico ovvero alle applicazioni in ambito industriale con riferimento al settore dell'Internet of Things (IoT) oppure al settore dell'Automotive (dalla guida autonoma, all'auto iper-connessa, al programma smart driving).

di Francesco Rundo e Sabrina Conoci

TECNOLOGIA "BLOCKCHAIN": DAGLI SMART CONTRACTS ALLO SMART DRIVING.

SPUNTI DI RIFLESSIONE SULLA NORMATIVA E SULLA SOSTENIBILITÀ TECNOLOGICA

Francesco RUNDO, ingegnere informatico, ha un dottorato di ricerca in Matematica Applicata conseguito presso l'Università di Catania. Svolge l'attività di R&D Engineer presso la STMicroelectronics, sviluppando algoritmi e modelli matematici per l'analisi dati in ambito industriale. Da anni svolge il ruolo di Consulente Tecnico di Parte nei contenziosi in ambito civile e penale per l'analisi matematica dei rapporti bancari e degli strumenti di investimento.

Sabrina CONOCI, laureata in Chimica Industriale presso l'Università degli Studi di Bologna e con dottorato di ricerca in Ingegneria dei Materiali, ricopre il ruolo di R&D Manager presso STMicroelectronics occupandosi si attività di ricerca nell'ambito del settore dei dispositivi nanomolecolari, biosensori per l'analisi del DNA e sensori chimici.

1. Introduzione

L'attuale paradigma societario basato sul modello classico segnato dalla normativa vigente in ambito civile, amministrativo e penale, richiede una rivisitazione sostanziale in quanto risulta, spesso, inidoneo a regolare i nuovi processi derivanti dall'applicazione delle nuove tecnologie digitali nella vita di tutti i giorni. A questo si aggiunge, talvolta, l'inadeguatezza dell'infrastruttura hardware e software, sia dei privati che della pubblica amministrazione (si consideri, ad esempio, il caso *Uber-Italia* è la conseguente inadeguatezza normativa oltre che tecnologica). Obiettivo di questo articolo è, pertanto, introdurre ,senza alcuna pretesa di esaustività dell'argomento, una specifica tecnologia digitale che riteniamo meritevole di interesse atteso il potenziale applicativo che questa racchiude: ci stiamo riferendo al framework ***Blockchain*** (che letteralmente significa "catena di blocchi").

Probabilmente non tutti hanno sentito parlare o conoscono questa tecnologia digitale, ma avranno certamente sentito parlare della criptovaluta "***Bitcoin***" che ne rappresenta probabilmente, l'esempio applicativo più noto. L'utilizzo dell'infrastruttura blockchain non si limita chiaramente alle sole criptovalute, ma può essere utilizzata efficacemente per svariate altre applicazioni, tra cui vale la pena menzionare: *Smart Contracts*, *Smart City*, *Automotive (sistemi ADAS, guida autonoma ed auto iper-connesse)*, *Internet of Things(IoT)*, *applicazioni finanziarie e assicurative*, e cosi via.

2. La piattaforma Blockchain

L'infrastruttura blockchain può essere descritta semplicemente come una rete globale di dispositivi interconnessi (*nodi*) e nella quale è opportunamente memorizzato un registro digitale pubblico condiviso (denominato in gergo "*Global Distributed Ledger*") il quale è riprodotto opportunamente su ciascuno dei dispositivi-nodi.
Pertanto, all'interno della rete blockchain è memorizzato un notevole quantitativo di dati distribuito opportunamente tra i vari *records* informativi presenti su ciascun dispositivo-nodo. Tali records sono in continua evoluzione sia in relazione al loro numero che in relazione all'informazione in essi contenuta. L'elevata sicurezza dei dati memorizzati nella blockchain è garantita dal meccanismo di funzionamento , di fatto estremamente innovativo. **Elemento chiave del funzionamento della blockchain è la tecnica di memorizzazione dei dati**: una copia dell'intero registro della blockchain (*ledger*) è memorizzata su ciascun dispositivo-nodo partecipante. Ogni record informativo del *ledger* memorizzato su un dispositivo-nodo è composto dalle seguenti due parti:

1. *transazioni*: includono i dati in un formato prestabilito;
2. *blocchi*: questi dettagliano il flusso di operazioni sulle transazioni, in opportuno ordine temporale. Ogni blocco include un codice *hash* di sicurezza.

Le transazioni sono generate dai partecipanti alla rete blockchain in relazione all'utilizzo applicativo che intendono perseguire (*smart contracts, accesso dati, comunicazione tra nodi remoti, trasmissione o invio dati o altro, etc.*.), mentre i blocchi sono generati da partecipanti speciali, i cosiddetti *miners* (letteralmente "minatori"), che utilizzano software, hardware specializzato e potenti algoritmi matematici per validare le transazioni e creare i blocchi.

Quando una transazione digitale viene completata, viene inclusa in un raggruppamento di transazioni (blocco) opportunamente criptato (di solito vengono raggruppati piu blocchi ad intervalli di tempo regolari, tipicamente 10 minuti) e diffusa nell'intera blockchain dove sarà validata dai *miners*, mediante opportuni algoritmi matematici alquanto complessi. Ad ogni blocco validato dai *miners* viene assegnata (sempre mediante un algoritmo complesso) una c.d. *marca temporale (Timestamp).* Ogni blocco validato con marca temporale, sarà aggregato agli altri blocchi in una catena lineare, cronologicamente ordinata e sempre aggiornata, dunque, sarà inviato a tutta la blockchain: in tal modo ogni dispositivo-nodo della blockchain conterrà una copia di questi blocchi in un registro distribuito (ledger). In tal modo la struttura della blockchain sarà decentralizzata e priva di un *arbitro* o di un *server centrale di aribitraggio* oltre che protetta da potenti algoritmi di crittografia. Queste caratteristiche rendono le transazioni della blockchain "autonome" nel senso che queste avvengano automaticamente senza l'intervento di intermediari.

Se un hacker volesse violare un blocco della blockchain, dovrebbe violare tutti i blocchi costituenti la catena associata a quel blocco eseguendo delle azioni non autorizzate su ciascuno dei ledgers associati ad ogni dispositivo-nodo, il cui numero è di fatto sconosciuto a priori è puo, ben essere, elevato rendendo praticamente e materialmente impossibile eseguire un cyber-attacco o un qualsivoglia tentativo di corruzione dati. La seguente figura illustra una tipica struttura della rete blockchain:

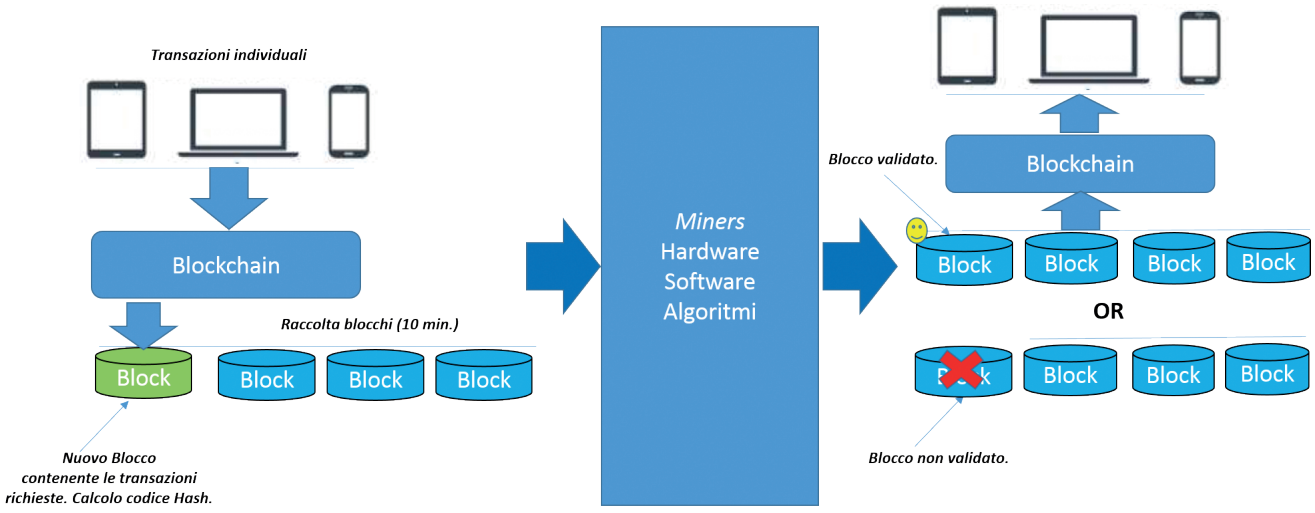

Figura 1 *- 4G LTE: aspetti di sicurezza di dettaglio*

Da quanto sopra si comprende chiaramente che la suddetta architettura informatica richiede un sottostante hardware e software non indifferente attesa la complessità richiesta dal protocollo di gestione dell'intera blockchain.

3. Applicazioni della Blockchain: Dagli Smart Contracts allo Smart Driving

Le summenzionate caretteristiche della blockchain, rendono tale infrastruttura appetibile a notevoli aziende che operano in svariati settori e che di fatto hanno individuato in questa nuova tecnologia una possibile soluzione alle attuali problematiche di settore. Di seguito verranno illustrate alcune possibili applicazioni della blockchain.

a.1 Smart Contracts

Attraverso la tecnologia blockchain sarà dunque possibile eseguire le clausole di un contratto tra più parti mediante un codice o set di transazioni opportunamente criptate le quali specificano (mediante un opportuno protocollo interno) le condizioni contrattuali pattuite tra le parti. Le clausole contrattuali, criptate in transazioni da eseguire nella blockchain, saranno lette ed automaticamente interpretate dai relativi nodi-dispositvi della rete che dunque, attraverso il meccanismo dei "*miners*" sopra descritto, saranno eseguite ed alla fine convalidate con data-certa (marca temporale o *timestamp*). Una volta eseguite e distribuite nella blockchain, dette transazioni inglobate in blocchi con relativo timestamp, andranno ad aggiornare i vari ledgers dei singoli nodi-dispositivi partecipanti alla rete, divenendo di fatto "irrevocabili", sicure ed aventi data certa.
In ambito forense, nei vari contenziosi di natura contrattuale, attraverso l'adozione degli smart contracts e della rete blockchain, si otterebbero vantaggi notevoli nella gestione dei procedimenti giudiziari, in quanto diverrebbe sicuro e semplice: *l'acquisizione della data certa dell'esecuzione contrattuale* (time-stamp del nodo), la *certezza di esecuzione della clausola da parte dei contraenti* (validazione del blocco), la *successione temporale delle esecuzioni contrattuali* (cronologia temporale dei blocchi memorizzata nel ledger dei dispositivi-nodi), etc…

a.2 Smart City e Smart Driving: Dall'auto iper-connessa alla guida automatica

Recentemente è stato pubblicato un nuovo standard internazionale che ha classificato opportunamente i livelli di automazione della guida. In tale documento sono stati definiti, nello specifico, sei distinti livelli di guida automatica.
Elemento comune dei livelli di automazione è la definizione di algoritmi di apprendimento dati durante la guida dell'autoveicolo e che includono i dati *biometrici e fisiologici di chi guida*, le *informazioni visive* (Car-vision) relative all'esterno dell'auto (strade, segnaletica, oggetti esterni, ostacoli, etc..), sull'interazione con altri veicoli, etc.. Questi dati sono acquisiti attraverso opportuni sensori ubicati internamente ed esternamente l'abitacolo dell'auto.

Alcuni car-makers o aziende legate al mercato automotive intendono raccogliere i dati acquisiti da questi sensori e di cui le auto moderne sono dotate, rendendoli disponibili attraverso l'infrastruttura blockchain, dunque in forma sicura, a tutte le auto dotate di tale tecnologia. In tal modo, attraverso l'infrastruttura blockchain sarà possibile mantenere iper-connesse le auto tra loro ed in modo sicuro ed a prova di qualsivoglia cyber-attacco. Si potrà altresi', informare le auto a guida autonoma circa le condizioni della strada, eventuali incidenti, deviazioni o altro , il tutto facilmente reperibile attraverso le informazioni memorizzate nella blockchain e rese pertanto accessibili a tutti i nodi-dispositivi. Nell'ambito *Smart City*, l'interconnessione attraverso una rete blockchain, tra autoveicoli e nodi urbani intelligenti contenenti informazioni sul contesto urbano, avverrebbe in modo sicuro e criptato ovvero resistente a qualsivoglia tentativo di accesso o manomissione indesiderato, permettendo cosi un efficiente controllo urbano.
La figura che segue descrive lo scenario applicativo della rete blockchain in ambito smart-city / smart driving:

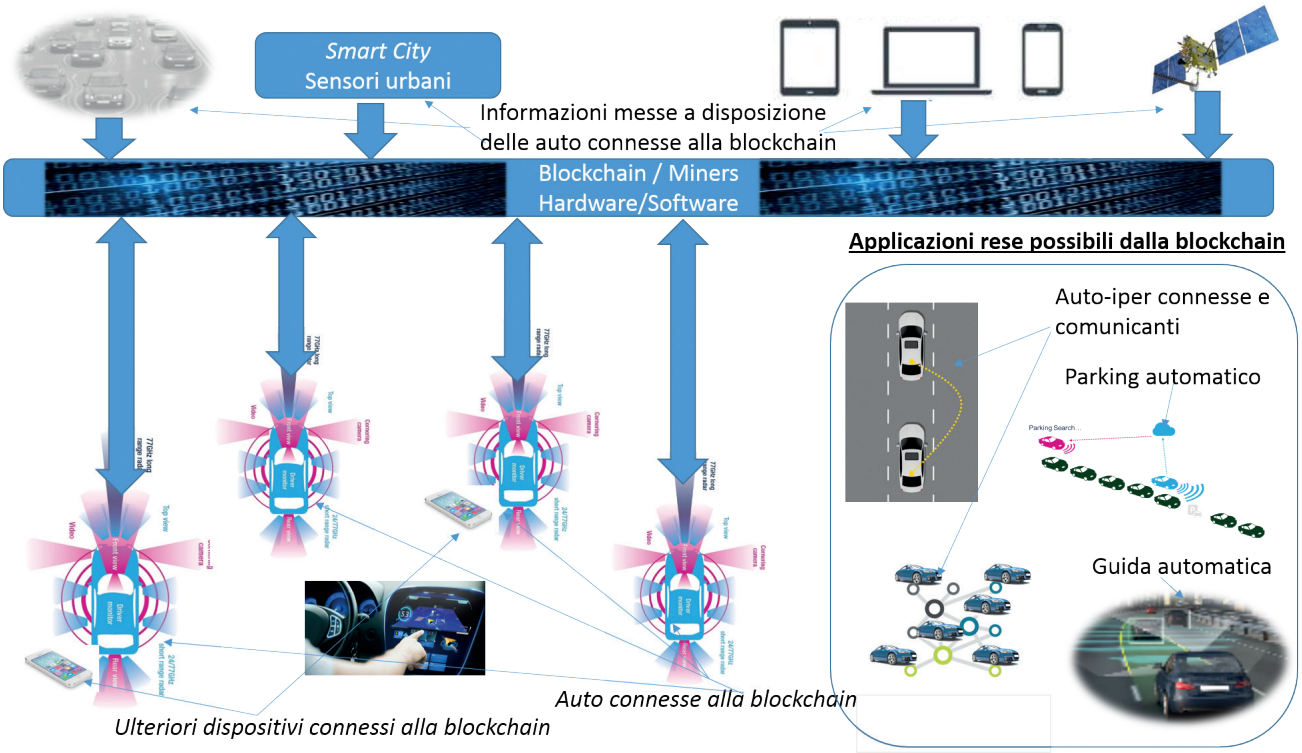

Figura 2 - *4G LTE: aspetti di sicurezza di dettaglio*

In ambito forense, nei procedimenti giudiziari in sede civile e penale e riguardanti casi di sinistri stradali, l'utilizzo della tecnologia blockchain può migliorare sensibilmente la gestione del contenzioso atteso che attraverso l'utilizzo dei dati memorizzati nei nodi della blockchain sarà possibile ricostruire in maniera precisa ed accurata la dinamica dell'incidente oggetto del contendere (velocita di guida, stato del conducente, sequenza temporale, etc..). Ciò permetterà una soluzione veloce del contenzioso riducendo al minimo i rischi di una decisione giudiziaria errata.

4. La rete blockchain: Requisiti hardware e software

I paragrafi precedenti hanno evidenziato l'elevata efficienza e potenzialità della rete blockchain in relazione alla sicurezza delle transazioni/informazioni ed in relazione ai possibili vantaggi in svariati ambiti applicativi sia sociali che industriali. Tuttavia, tale efficienza richiede un prezzo in termini di infrastruttura hardware e software necessaria a supportare l'elevato carico computazionale richiesto dal processo di esecuzione e convalida delle transazioni (che come detto richiede tra l'altro la soluzione di complessi problemi di matematica nonlineare e di crittografia matematica) nonchè per permettere una connessione remota efficiente e robusta tra i nodi-dispositivi.
In tale ambito la proposta degli autori è quella di dotare la rete blockchain (la parte dei sistemi *miners*) di sistemi embedded dedicati, che permettono di risolvere velocemente il carico computazionale richiesto.

5. La tecnologia blockchain e gli aspetti normativi

Da quanto sopra descritto appare evidente che l'utilizzo della piattaforma blockchain suggerisca delle riflessioni in merito all'attuale normativa vigente in ordine alle indicazioni codicistiche di natura contrattuale nel caso degli smart-contracts ovvero civile-penale nel caso dell'automotive (smart-city e/o smart driving). Nel contesto giuridico italiano, la conclusione dei contratti sia pubblici che privati, richiede delle precise formalità previste dalla normativa codicistica e talvolta dalla normativa specifica di settore. Più in dettaglio, il codice civile prevede una apposita sezione relativa ai contratti ed alla loro redazione (si rinvia il lettore agli artt. 1321 – 1469 c.c.).

Ciò premesso, appare chiaro che l'applicazione degli smart-contracts attraverso la tecnologia blockchain sebbene presenti notevoli vantaggi, si scontra con una normativa che non ne consente una agevole applicazione.
Per dare una idea delle problematiche richiamate sopra, ci si limita a fare riferimento ai requisiti minimi imposti dal nostro ordinamento in relazione alla redazione di un contratto. Affinche uno smart contract possa definirsi equiparabile giuridicamente ad un contratto classico, dovrebbe contenere in maniera chiara, puntuale e precisa, gli elementi di cui all'articolo 1325 del codice civile ossia: *"1) l'accordo delle parti; la causa; l'oggetto; la forma(quando prevista)"*.
In uno smart contract generato su una rete blockchain, questi elementi risultano quantomeno di difficile individuazione e interpretazione, dunque, risulta alquanto ardua la loro individuazione sia in regime di verifica della loro validità che, ancor peggio, in sede di contenzioso in quanto sia il giudice che un eventuale perito tecnico (CTU) dovrebbero essere in grado di ricavare i requisiti ex art. 1325 c.c. dall'analisi dei blocchi della blockchain!

Un tema che sicuramente deve essere considerato è altresi', il rapporto tra lo smart contract e le previsioni normative che richiedono la forma scritta *ad substantiam* per certi contratti (art. 1350 c.c.), o che richiedono altre formalità quali la presenza di testimoni, la forma pubblica, etc.. Altro aspetto da valutare riguarda la modalità di sottoscrizione degli smart contracts e l'efficacia di tale sottoscrizione. Con poche eccezioni, affinche ci sia piena corrispondenza tra una sottoscrizione classica ed una digitale (convalida transazione/blocco sulla blockchain) è necessario l'utilizzo di un sistema di firma digitale, ovvero di un sistema di criptaggio a chiave pubblica/chiave privata, ai sensi dell'art. 21, comma 2, del D.lgs. 82/2005; ex art. 2702 c.c. Inoltre c'è da dire che la redazione di un contratto include spesso delle clausole che vanno interpretate sulla base di principi interpretativi caratterizzati da un certo grado di "elasticità", in base alla singola fattispecie applicativa alla quale si riferiscono (vedi art. 1362 c.c.). Uno smart contract, che per definizione è "immodificabile" ed eseguito secondo un algoritmo *deterministico*, potrebbe rivelarsi incapace di eseguire correttamente le clausole contrattuali aggiuntive o ad applicazione differita nel tempo o al verificarsi di certe condizioni (si pensi ai contratti bancari e finanziari) non potendo tutte le variabili trovare "traduzione" algoritmica.
Analogamente nel campo dell'automotive (smart city o smart driving) o di qualsivoglia altra applicazione, sebbene i vantaggi della tecnologia blockchain sono molteplici, questi devono comunque essere soppesati con una normativa talvolta miope al progresso tecnologico. Pertanto andrà certamente rivisto ed integrato, il *codice della strada*, il *codice della privacy e di gestione dei dati sensibili* considerato l'utilizzo di tali dati nella blockchain (condivisione pubblica tramite *ledger*) e le modalità di accesso alla rete.

6. Conclusioni

È indubbio che la blockchain racchiuda un potenziale innovativo non indifferente per applicazioni in svariati ambiti industriali e sociali. Ciò nonostante è lecito dubitare, per i motivi accennati sopra, che essa possa essere facilmente applicabile con l'attuale normativa di settore. Realisticamente, gli autori auspicano un futuro investimento di tempo e risorse da parte delle aziende , della società e del legislatore riguardo l'implementazione di un sistema di condivisione dati basato su tecnologia blockchain ovvero nell'emanazione di una normativa che sia in piena sintonia con il progresso tecnologico. Infatti, attraverso l'adozione della tecnologia blockchain si otterebbe un notevole impulso nei programmi di sviluppo tecnologico attuali (si vedano i programmi "Smart City" o "Smart Driving") contribuendo a migliorare notevolmente il livello di sicurezza della società e contribuendo altresi' a migliorare l'efficienza della macchina amministrativa e giudiziaria nel nostro paese. ©