I DOCUMENTI AI TEMPI DELLA BLOCKCHAIN

Il valore legale dei documenti attestati sulla BC

avv. Emanuele Mansuelli

La BC permette di creare una storia immodificabile di cui tutti i partecipanti conoscono la stessa versione

Caratteristiche:

- Registro distribuito tra tutti i partecipanti - DLT
- Non modificabilità del dato
- Autenticità del dato
- Data certa

Altro profilo:

- Possibilità di attestare su BC gli smart contract

La BC nella normativa italiana

Decreto semplificazioni (art. 8 *ter* d.l. 135/2018 conv. in l. 12/2019) **Tecnologie basate su registri distribuiti e smart contract**

- 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.

Un passo indietro: IL DOCUMENTO (analogico)

Nell'ordinamento giuridico italiano non c'è una definizione di **documento**, il Prof. Francesco Carnelutti lo definì come la **"cosa che fa conoscere un fatto"**

Quali aspetti del documento interessano al giurista?

- Il contenitore: la forma scritta (richiesta per finalità probatorie – mezzo di prova – o per la stessa validità dell'atto giuridico – art. 1350 c.c. es: compravendita immobiliare)
- il contenuto (ad esempio: l'espressione di una volontà negoziale) che dà forma all'atto giuridico estrinsecandolo in una forma scritta (quando richiesto)
- la sottoscrizione (individua l'autore del documento e la paternità degli effetti)
- la data (che in alcuni casi viene attestata per maggiore sicurezza, es: atti pubblici, scritture private autenticate)

IL DOCUMENTO INFORMATICO

- Un primato italiano: l'Italia è stato uno dei primi paesi nel mondo a riconoscerne la validità e la rilevanza giuridica sancendo il principio di EQUIVALENZA CON IL DOCUMENTO ANALOGICO (art. 15, comma 2 L. 15 marzo 1997 n. 59 cd. Legge Bassanini)
- definizione di DOCUMENTO INFORMATICO: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1 lett. p) d.lgs. 82/2005 - Codice dell'Amministrazione Digitale)
- Definizione di documento elettronico: qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva (art. 3, n. 35) Reg. UE 910/2014 - EIDAS)
- Art. 46 Reg. UE 910/2014 (EIDAS) stabilisce che un documento elettronico non può vedersi negati effetti giuridici o l'ammissibilità come prova per il solo motivo della sua forma elettronica

LA SOTTOSCRIZIONE NELL'INFORMATICA

Delimitiamo il campo giuridico attuale:

- Regolamento europeo n. 910/2014 (EIDAS) (in vigore dal 1 luglio 2016)
- D.lgs. 82/2005 (CAD: codice dell'amministrazione digitale)
- DPCM 22.02.2013 (regole tecniche)

REGOLAMENTO EIDAS
Electronic IDentification Authentication and Signature

definisce tre tipologie di firme e introduce il concetto di sigillo elettronico ovvero la firma elettronica intestata alla persona giuridica

- Art. 3 n. 10) Firma elettronica → dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare
- Art. 3 n. 11) Firma elettronica avanzata → una firma elettronica che soddisfi i requisiti di cui all'articolo 26
  - *è connessa unicamente al firmatario;*
  - *è idonea a identificarlo;*
  - *è creata con mezzi che il firmatario può utilizzare sotto il proprio esclusivo controllo;*
  - *è collegata ai dati sottoscritti in modo far rilevare ogni eventuale modifica.*
- Art. 3 n. 12) Firma elettronica qualificata → una firma elettronica avanzata a cui è associato un certificato rilasciato da un prestatore di servizi certificativi qualificato

Art. 25 Effetti giuridici delle firme elettroniche: la firma elettronica non può essere esclusa come mezzo di prova per il solo fatto di essere in forma elettronica o perché non soddisfa i requisiti della firma elettronica qualificata

La firma elettronica qualificata ha gli stessi effetti giuridici della firma autografa

CAD
codice dell’amministrazione digitale

si integra con il regolamento EIDAS e aggiunge:

- Art. 1, lett. s) **La firma digitale**: una firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;
- Art 20 CAD: il documento informatico soddisfa la **forma scritta** e ha **l’efficacia probatoria dell’art. 2702 c.c.** quanto vi è apposta la firma avanzata, qualificata, digitale o identificata. 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.
- L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare di firma elettronica, salvo che questi dia prova contraria.

Due garanzie della firma digitale:

1. LA PROVENIENZA DEL DOCUMENTO (Art. 2702 c.c.: la scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta)

2. L'INTEGRITÀ DEL DOCUMENTO la crittografia a doppia chiave asimmetrica garantisce al titolare di chiave provata di cifrare un documento che sarà decifrabile solo da chi possiede la chiave pubblica, senza che sia possibile risalire dall'una all'altra chiave. Il destinatario sa dunque che il mittente può essere solo il titolare di chiave privata (provenienza) e che il documento è integro in quanto altrimenti non sarebbe decifrabile. La funzione di hash estrae un'impronta (digest) dal testo in chiaro. L'impronta è univoca. Il mittente cifra l'impronta con la chiave privata e spedisce testo in chiaro e impronta. Il destinatario applica al testo in chiaro l'hash ed estrae l'impronta poi decifra l'impronta inviata dal mittente e le confronta. Se sono uguali il messaggio è autentico e integro.

LA DATA DEL DOCUMENTO

L’art 2704 c.c. stabilisce le regole per opporre a terzi la data di una scrittura privata. Se non è autenticata la sottoscrizione allora la data non è certa se non:

- dal giorno in cui la scrittura è stata registrata
- dal giorno della morte o della sopravvenuta impossibilità fisica di colui che l’ha sottoscritta
- dal giorno in cui il contenuto della scrittura è riprodotto in atti pubblici
- dal giorno in cui si verifica un altro fatto che stabilisca in modo egualmente certo l'anteriorità della formazione del documento.

LA VALIDAZIONE TEMPORALE ELETTRONICA

permette di dare certezza circa la localizzazione temporale dell'esistenza di un documento

- DPCM 22.02.2013 (regole tecniche):
  - La marca temporale è il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo
  - Il riferimento temporale è l'evidenza informatica contenente la data e l'ora, che viene associata ad uno o più documenti informatici;
  - L'evidenza informatica è una sequenza di bit elaborabile da una procedura informatica

La marca temporale (time stamp) viene creata (con una coppia di chiavi) e applicata, da un certificatore, al documento. In questo modo data e ora di formazione del documento sono opponibili a terzi (art. 20 CAD; art. 41 DPCM)

art 51 DPCM lo scarto temporale tra il riferimento assegnato alla marca e la sua generazione è nell'ordine di un minuto

- La revoca, scadenza, sospensione del certificato di firma elettronica rende la firma come non apposta (e dunque il documento è da considerarsi privo di sottoscrizione).

- La marca temporale salva la firma: art 62 DPCM le firme elettroniche, qualificate o digitali anche se revocato scaduto o sospeso il certificato, sono valide se associate ad una marca temporale che collochi la generazione della firma ad un momento antecedente la scadenza del certificato

VALORE LEGALE DELLA TRANSAZIONE SU BLOCKCHAIN

- BC permissionless
  - i partecipanti possiedono coppie di chiavi che permettono loro di sottoscrivere transazioni ed esserne titolari.
  - le transazioni rientrano nella definizione di documento elettronico (EIDAS) e documento informatico (CAD)
  - problemi di attribuibilità: le chiavi non sono associate a certificati o a identità definite e dunque non presentano i requisiti normativi per
    - Soddisfare il requisito della forma scritta
    - Avere valenza probatoria quanto alla provenienza/paternità rispetto all'autore
  - Resta aperta la porta alla libera valutazione del giudice in relazione alle caratteristiche di sicurezza, integrità, immodificabilità (art 20 CAD)
    - integrità e immodificabilità sono garantite dalla tecnologia.
    - la sicurezza è da intendere sia come sicurezza tecnica sia come sicurezza degli strumenti di accesso (problema dell'identificazione di chi accede)

- BC permissioned
  - l’accesso è consentito solo ai partecipanti al network
  - uno dei partecipanti può diventare soggetto erogatore della soluzione di firma avanzata (art 55 DPCM) attestando l’identità dei titolari delle chiavi crittografiche usate per la sottoscrizione delle transazioni
  - le evidenze informatiche avrebbero quindi valenza probatoria e sarebbero idonee a soddisfare il requisito della forma scritta

UN CENNO AGLI SMART CONTRACT

Decreto semplificazioni (art. 8 *ter* d.l. 135/2018 conv. in l. 12/2019) **Tecnologie basate su registri distribuiti e smart contract**

- 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.

- Sono programmi per elaboratore
- Attestati su registri distribuiti (es: BC)
- Soddisfano il requisito della forma scritta previa identificazione informatica delle parti
- L’Agid fisserà i requisiti in apposite linee guida

- Lo smart contract nasce prima della BC, da un'idea di Nick Szabo nel 1996 e consiste nell'incorporare una serie di clausole contrattuali direttamente nel software con cui le persone si relazionano automatizzando l'esecuzione delle prestazioni contrattuali rendendo impossibile l'inadempimento
- Il meccanismo è basato sull'avveramento di determinate condizioni che generano conseguenze. Le condizioni possono derivare da eventi **interni** alla BC (es: raggiungimento di una certa data) oppure **esterni** (in tal caso si fa riferimento ad un ORACOLO cioè un software che funziona come INFORMATORE trasferendo allo SC le condizioni esterne → atmosferiche; il raggiungimento di un prezzo di un titolo; il ritardo di un volo…

LO SMART CONTRACT SU BC – PROBLEMA DELL'IRREVERSIBILITÀ

- Esistono in realtà le funzioni cd. kill che permettono di bloccare l'esecuzione in caso, ad esempio, di inadempimento da parte di uno dei contraenti.
- In questo caso l'adempiente potrà rivolgersi al giudice per chiedere la risoluzione del contratto.
- La pronuncia giudiziale di risoluzione, nullità o annullamento del contratto non produrrà immediatamente il venir meno dell'efficacia dovendo contenere anche un obbligo di fare consistente nell'attestazione sulla BC della funzione kill
- ACCENTURE → CHAMELEON HASH: creato per la BC permissioned utilizza una funzione che permette all'amministratore di sistema di cambiare i dati inseriti in BC. Ma la garanzia di immutabilità per certi versi rimane ferma nella misura in cui comunque questi interventi correttivi rimangano tracciabili.

LO SMART CONTRACT E L'ASSENZA DI STANDARD CONDIVISI

- i termini e le espressioni usati dalle parti devono essere comprensibili alla macchina per garantire l'esecuzione automatica
  - *concetti come la forza maggiore o la buona fede necessitano di un intervento interpretativo*

  Si auspica una standardizzazione delle clausole contrattuali utilizzabili negli SC sul modello delle clausole del commercio internazionale: incoterms)

  Una base di partenza: ***progetto Claudette*** *(CIRSFID – Prof. Giovanni Sartor e Prof. Giuseppe Contissa) che ha l'obiettivo di individuare l'estensione delle possibilità di automazione nell'individuazione di clausole illecite nei contratti online con il consumatore*

GRAZIE PER L'ATTENZIONE