

---

# **Distributed Ledger Technologies (DLT) Blockchain Smart Contracts**

---

**Diritto dell'informatica, servizi informatici e sicurezza dei dati  
Università di Pisa**

---

**Fernanda Faini**



# DIRITTO E ICT



# Regole giuridiche e informatiche (1)

Il diritto deve dialogare con altri insiemi di regole:

**lex informatica o digitalis** → le regole informatiche, le regole applicate dal “codice” (non quello giuridico)

Le regole informatiche condizionano i comportamenti umani, dal momento che:

- abilitano o meno determinate azioni e interazioni
- determinano la facilità nel compimento delle stesse
- collegano o meno effetti
- determinano quali informazioni fornire all'utente

Lex informatica **condiziona ogni altra forma di regolazione**,  
compresa quella giuridica



## Regole giuridiche e informatiche (2)

Ma le regole informatiche sono frutto dell'uomo che può intervenire sulle stesse attraverso il diritto → necessità di non rendere tutto ciò che è tecnologicamente possibile, solo per questo, giuridicamente legittimo



**ciò che è legittimo è un sottoinsieme del tecnologicamente possibile**



Alla tutela giuridica il diritto può affiancare la previsione di misure tecniche capaci di rendere impossibili o disabilitare azioni illecite (es. misure tecnologiche di protezione)



Necessità di **equilibrio nella regolazione** tra diritto e tecnica:

- la tecnica non deve prevalere e dominare sul diritto
- il diritto non deve “domare” e limitare la tecnologia

# DLT E BLOCKCHAIN



# Distributed Ledger Technologies (DLT)

**Distributed Ledger Technologies o DLT** → tecnologie di registro distribuito e disintermediato peer-to-peer, diversamente dalle architetture centralizzate client-server (che si basano sul controllo di un'autorità di gestione)



le voci del database sono replicate in una serie di nodi e la regolazione avviene mediante meccanismi di consenso condiviso

# Blockchain (1)

**Blockchain** → species del genus DLT → “catena di blocchi”, registro o libro mastro digitale → i dati, inseriti per mezzo di crittografia asimmetrica, sono allocati in blocchi, accompagnati da hash e timestamp (validazione temporale), tra loro concatenati attraverso la validazione temporale e il richiamo dell’hash del blocco precedente in quello successivo (immutabilità unilaterale).



Ogni nuovo blocco è validato da alcuni nodi (**miners**) per mezzo della risoluzione di un problema matematico, che vale una ricompensa (serve a incentivare la corretta validazione dei blocchi) → le transazioni sono validate con il consenso della maggioranza degli utenti.

I **meccanismi di consenso** sono diversi → Proof of Work (utilizzato da Bitcoin), Proof of Stake, etc.

Le transazioni possono avere ad oggetto dati oppure beni fisici o immateriali sotto forma di **token**.

# Blockchain (2)

La blockchain

- **in modo immutabile** conserva la memoria storica delle transazioni
- **in modo distribuito e paritetico** garantisce a ciascun partecipante una copia di ciascuna operazione

in tal modo sono garantite **sicurezza e resistenza** rispetto a potenziali attacchi.



Tali caratteristiche rendono il protocollo di comunicazione blockchain assimilabile a un **registro** o un **libro mastro digitale**,  
che non necessita di un intermediario o di un soggetto terzo certificatore



**Lex cryptographia**  
**Internet of Value**

trasforma il modo di scambiarsi valore, gestire le transazioni e meccanismi di fiducia



# Caratteristiche tecniche

- **disintermediazione**, decentralizzazione, distribuzione e vocazione transnazionale
- **immutabilità**, inalterabilità e persistenza dei dati
- **meccanismo distribuito** peer-to-peer di consenso, fiducia e incentivazione
- **trasparenza, tracciabilità e sicurezza**
- funzioni di **hash**, **crittografia asimmetrica** e **validazione temporale**

# Tipologie di blockchain

- **permissionless o unpermissioned o pubbliche** → aperte e liberamente accessibili a chiunque, senza autorizzazioni (Bitcoin ed Ethereum) → assolutamente decentralizzate e distribuite.
- **permissioned o private** → chiuse e non accessibili pubblicamente, dal momento che le autorizzazioni vengono gestite da un'autorità centrale (es. Hyperledger); l'autorità definisce anche regole e ruoli all'interno delle stesse → governance e forma di centralizzazione.
- **consorzi o ibride** → parzialmente decentrate, dal momento che esiste un controllo sul meccanismo di consenso da parte di alcuni nodi selezionati, che hanno maggiore influenza degli altri (es. Ripple).

# Bitcoin ed Ethereum

**Bitcoin** è la prima applicazione pratica della tecnologia blockchain, impiegata per la creazione di una moneta elettronica basata su un protocollo decentralizzato peer-to-peer → risolve problema di sfiducia nel sistema bancario, strumento alternativo di pagamento.

L'inventore è riconosciuto in **Satoshi Nakamoto** (pseudonimo sotto cui si cela la misteriosa identità dell'inventore).

Cfr. S. NAKAMOTO, Bitcoin: A Peer-to-Peer Electronic Cash System, in bitcoin.org, 2008.

**Ethereum** è un protocollo con lo scopo principale di fornire una piattaforma open source per incentivare lo sviluppo di applicazioni decentralizzate (decentralized applications – DApps), come gli smart contracts.

L'inventore è **Vitalik Buterin**.

Cfr. V. BUTERIN, Ethereum White Paper. A next generation smart contract & decentralized application platform, in <https://ethereum.org>, 2013, pp. 1-37.

# QUADRO NORMATIVO E STRATEGICO



# Premessa

Rilevano i profili che caratterizzano la storia del rapporto tra diritto e tecnologia:

- da un lato **esigenza di governance** collegata alla necessità di un **approccio sovranazionale**
- dall'altro **scontro ontologico tra le caratteristiche tecniche e il rispetto di principi e norme del diritto**, esacerbato da:
  - logica orizzontale e dal meccanismo distribuito peer-to-peer di consenso e fiducia, che mal si concilia con il sistema di tutele basato sulla centralizzazione e sul controllo
  - problemi di coordinamento delle norme nazionali con le norme europee



# Risoluzione del Parlamento europeo del 3 ottobre 2018 sulle tecnologie di registro distribuito e blockchain

- ✓ **creare fiducia attraverso la disintermediazione** → DLT è una tecnologia a scopo generico in grado di migliorare l'**efficienza** dei costi delle transazioni **eliminando intermediari** e costi di intermediazione, oltre ad aumentare la **trasparenza delle transazioni**, ridisegnando anche le catene del valore e migliorando l'efficienza organizzativa attraverso un decentramento affidabile
- ✓ un paradigma informatico che può **democratizzare i dati** e **rafforzare la fiducia e la trasparenza**, fornendo un percorso sicuro ed efficace per l'esecuzione delle transazioni
- ✓ **i rischi e i problemi non sono ancora completamente noti**
- ✓ necessità di un **quadro favorevole all'innovazione che consenta e incoraggi la certezza del diritto**

# Iniziative Commissione UE su tecnologie di registro distribuito (DLT) e blockchain (1)

- **EU Blockchain Observatory and Forum** → febbraio 2018  
Ha la funzione di raccogliere informazioni, mappare le principali iniziative, monitorare gli sviluppi e analizzare le tendenze, esaminare il potenziale socio-economico e affrontare le sfide, cercando di garantire un approccio uniforme e comune a livello europeo. Ha formato due gruppi di lavoro:
- ✓ **Blockchain Policy and Framework Conditions Working Group** → deputato a definire le condizioni politiche, legali e regolamentari necessarie per la diffusione su larga scala delle applicazioni basate sulla blockchain e designato ad esaminare questioni quali smart contracts e data protection.
- ✓ **Use Cases and Transition Scenarios Working Group** → chiamato a concentrarsi sui casi di utilizzo più promettenti, con particolare attenzione alle applicazioni del settore pubblico come identità e servizi, assistenza sanitaria, energia e rendicontazione ambientale.

Interessanti i **report tematici** prodotti dall'Osservatorio → <https://www.eublockchainforum.eu/eu-blockchain-observatory-forum>

# Iniziative Commissione UE su tecnologie di registro distribuito (DLT) e blockchain (2)

- **European Blockchain Partnership** → lanciata nell'aprile 2018, scambio di competenze ed esperienze in campo tecnico e normativo, al fine di sviluppare applicazioni blockchain a livello europeo. Ingresso dell'Italia nel settembre 2018. Mira a consolidare il ruolo dell'Europa nello sviluppo e nella diffusione della tecnologia blockchain per mezzo di un approccio uniforme a livello europeo → i rappresentanti dei Paesi partecipanti lavorano, al fine di stabilire le linee di intervento utili per sfruttare il potenziale dei servizi basati sulla blockchain a beneficio dei cittadini, della società e dell'economia.

Il partenariato coopera per la creazione dell'**European Blockchain Services Infrastructure (EBSI)**, capace di supportare la fornitura di servizi pubblici transfrontalieri nell'Unione europea, utilizzando la tecnologia blockchain e garantendo alti standard di sicurezza e protezione dei dati personali.

# Art. 8-ter d.l. 135/2018 conv. in l. 12/2019

## Tecnologie basate su registri distribuiti e smart contract (1)

1. Si definiscono “**tecnologie basate su registri distribuiti**” le tecnologie e i protocolli informatici che usano un **registro**
  - condiviso
  - distribuito
  - replicabile
  - accessibile simultaneamente
  - architetturealmente 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.**

**Sovrapposizione erronea tra distributed ledger technologies e blockchain** → alcune caratteristiche connotano più propriamente queste ultime, in particolare le permissionless (inalterabilità, immutabilità e verificabilità dei dati da parte di ciascun partecipante).

# Art. 8-ter d.l. 135/2018 conv. in l. 12/2019

## Tecnologie basate su registri distribuiti e smart contract (2)

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'art. 41 del regolamento (UE) n. 910/2014.



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.



# PROBLEMATICHE GIURIDICHE



# Normativa di riferimento in tema di documenti informatici e data protection

- **regolamento eIDAS n. 910/2014** del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno → abroga la precedente direttiva 1999/93/CE
- **codice civile**
- **d.lgs. 82/2005 - Codice dell'Amministrazione Digitale (CAD)** → modifiche e integrazioni nel corso degli anni, da ultimo con il **d.lgs. 179/2016** e il **d.lgs. 217/2017**.
- **regolamento UE 2016/679 e normativa italiana** (d.lgs. 196/2003 modificato dal d.lgs. 101/2018)

# Validazione temporale (1)

- **criticità nel coordinamento tra la norma italiana e la normativa europea**
- ai sensi dell'art. 8-ter, la memorizzazione di un documento informatico attraverso l'uso di DLT produce gli effetti giuridici della validazione temporale elettronica di cui all'art. 41 del reg. (UE) eIDAS n. 910/2014  
↓
- art. 41 del reg. (UE) eIDAS n. 910/2014 prevede gli effetti giuridici sia della **validazione temporale semplice** sia della **validazione temporale qualificata**, che hanno **effetti giuridici diversi**
- **validazione temporale semplice** → la valutazione è rimessa al libero apprezzamento del giudice
- **validazione temporale qualificata** → presunzione di accuratezza della data e dell'ora e di integrità dei dati ai quali data e ora sono associate

## Validazione temporale (2)

A quale validazione temporale intende riferirsi il legislatore?

La norma rinvia agli **standard tecnici individuati dall'AgID** → potrebbero contribuire a sciogliere il nodo interpretativo, anche se tale rinvio rischia di aggravare le problematiche in gioco.

Il reg. (UE) eIDAS n. 910/2014 pone il **principio di non discriminazione**, (primo paragrafo art. 41), secondo cui «alla validazione temporanea elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti della validazione temporanea elettronica qualificata». Il riferimento a quella semplice verrebbe a limitare quanto previsto a livello europeo dal principio di non discriminazione.

Nel caso di interpretazione come validazione temporale elettronica qualificata, gli standard di AgID devono essere interpretati in modo restrittivo soltanto come un ausilio e un mezzo per misurare il rispetto dei requisiti di cui all'art. 42 del reg.(UE) eIDAS, non potendo certo sostituirsi agli stessi.

# Blockchain e data protection

**La funzione di hash e crittografia rientra in pseudonimizzazione** → il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di **informazioni aggiuntive**, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile (art. 4, par. 1, n. 5, reg. UE 2016/679).



**si applica la disciplina in materia di data protection**

di cui al regolamento (UE) 2016/679 e alla normativa italiana (d.lgs. 196/2003, modificato dal d.lgs. 101/2018)



necessario rispetto dei principi,  
individuazione delle figure soggettive previste  
esercizio dei diritti dell'interessato



# Principi

**Principi applicabili al trattamento dei dati personali previsti dal regolamento (UE) 2016/679 (art. 5):**

- **minimizzazione dei dati** → devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati → blockchain per il suo funzionamento replica i dati nei vari nodi
- **limitazione della conservazione** → conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati → nella blockchain i dati sono conservati in modo perpetuo

# Figure soggettive (1)

**Individuazione figure** ai fini di governance, applicazione disciplina ed esercizio diritti interessato (art. 4, par. 1, nn. 7 e 8, reg. UE 2016/679)

- **titolare** → la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, che, singolarmente o insieme ad altri titolari, determina le finalità e i mezzi del trattamento di dati personali
- **responsabile** → soggetto eventualmente preposto dal titolare che tratta dati personali per conto del titolare

**Principio di responsabilizzazione** → titolare è competente per il rispetto dei principi e deve essere in grado di provarlo (art. 5, reg. UE 2016/679)

## Figure soggettive (2)

- **permissioned** → soggetto che governa l'infrastruttura
- **consorzi** → contitolari del trattamento (art. 26)
- **permissionless** → chi?
  - tutti i nodi quali contitolari o responsabili o titolari per sé e responsabili per gli altri? Se titolari difficile individuazione della determinazione “congiunta” delle finalità e dei mezzi del trattamento e se responsabili manca atto di designazione
  - nessun titolare? Difficile applicazione disciplina
  - lo sviluppatore del software? Non sempre determina finalità e mezzi del trattamento

# Diritti dell'interessato

Ampi e rafforzati dal regolamento europeo 2016/679



la stessa difficoltà di individuazione del titolare rischia di tradursi  
nell'ineffettività dell'esercizio dei diritti

(diritto all'accesso a dati e informazioni - art. 15, diritto alla portabilità dei dati - art. 20, diritto di opposizione al trattamento - art. 21)

**Difficoltà ulteriori ad applicare alcuni diritti dell'interessato** in considerazione delle caratteristiche tecniche della blockchain:

- **rettifica e integrazione** (art. 16), **cancellazione** (diritto all'oblio) (art. 17) e **limitazione di trattamento** (art. 18) → difficile applicazione per le caratteristiche di immutabilità, inalterabilità e persistenza dei dati
- **non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato** (art. 22) → blockchain tramite automatismi porta alle conseguenze

# Luogo del trattamento

**Difficile stabilire il luogo del trattamento** e la distribuzione dei nodi può allargarsi fuori dall'ambito territoriale europeo:

- emergono difficoltà concrete nell'applicazione della disciplina, che si estende anche fuori dai confini dell'Unione europea
- dubbi in merito all'applicazione delle norme relative al trasferimento dei dati all'estero, prevista dal regolamento (UE) 2016/679



# Blockchain e data protection

**Le criticità giuridiche esaminate derivano direttamente dalle caratteristiche tecniche distintive della blockchain** → l'approccio concettuale del regolamento europeo in materia di data protection, che prevede un trattamento centralizzato dei dati personali fondato sul controllo e sulla responsabilizzazione, risulta faticosamente adattabile a una tecnologia che si caratterizza invece per decentralizzazione, disintermediazione e distribuzione.

Azione preventiva sul design dell'architettura tecnologica, adattandola e adeguando alcune caratteristiche distintive della blockchain, quali disintermediazione e immutabilità.

**Possibilità in incorporazione del diritto nella tecnica** → data protection by design e by default (art. 25) → soluzioni in grado di conciliare la tecnologia con i principi della data protection, quali la memorizzazione dei dati personali off-chain, memorizzando sulla stessa un mero riferimento o tecniche atte a prevenire la re-identificazione dei soggetti che non permettano di ricondurre i dati a un solo soggetto o coppie di chiavi diverse per ciascuna transizione.

# SMART CONTRACTS



# Cosa sono?

Nel momento in cui sono soddisfatte le condizioni contrattuali tradotte dal codice informatico nel linguaggio macchina, si attivano automaticamente gli effetti conseguenti con le caratteristiche della blockchain (immutabilità e irreversibilità)



gli effetti contrattuali si eseguono automaticamente al verificarsi delle condizioni predeterminate dalle parti e descritte nel software sotto forma di codice informatico secondo la logica “if this then that” → **self-enforcement delle regole**

Ideatore Nick Szabo

**Evoluzione “intelligente” del contratto** (capace di eseguirsi automaticamente in modo deterministico), è un’applicazione significativa della blockchain, in cui regole informatiche e norme giuridiche si intersecano significativamente, determinando esigenze e problematiche inedite → muta il linguaggio di riferimento e si compie una piena automazione, in cui la tecnologia è capace di sostituirsi all’uomo

# Vantaggi

- eliminazione del rischio di inadempimento
- eliminazione del ricorso a intermediari e dei costi in termini economici e di tempo
- sicurezza della relazione contrattuale
- evitare insorgere di controversie



vantaggi potenziali, suscettibili di sfumare a fronte di esigenze concrete da perseguire, che determinano la necessità della presenza di quegli elementi che in teoria gli smart contracts permettono di superare

# Definizione normativa

**Art. 8-ter, comma 2, d.l. 135/2018 conv. in l. 12/2019**

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'AgID con linee guida da adottare entro 90 giorni dalla data di entrata in vigore della legge di conversione del decreto.

## **Evoluzione dei contratti automatici**

(es. distributore automatico di bevande o vending machine):

**qualificazione normativa tra software e documento informatico**

# Inquadramento e qualificazione giuridica (1)

## Due ricostruzioni

1. **veri e propri accordi negoziali**, capaci di sostituirsi completamente ai contratti tradizionali → il codice informatico costituirebbe l'accordo, nel quale si esprime la volontà contrattuale, con forza di legge tra le parti (art. 1372 c.c.), dotato della capacità di essere automaticamente eseguito



diversa modalità di manifestazione del consenso, formazione e conclusione dell'accordo

2. **meri strumenti idonei a gestire gli accordi e a eseguire una volontà espressa altrove** in un precedente accordo contrattuale, capaci di garantire l'automazione dell'adempimento e dell'esecuzione, riguardando solo adempimento e fase esecutiva



non riguarda la fase di formazione del contratto, costituita dall'accordo delle parti (esterno o off-chain), ma la fase dell'adempimento, che avverrebbe in modo automatico al verificarsi delle condizioni espresse nel codice informatico



## Inquadramento e qualificazione giuridica (2)

L'appartenenza all'una o all'altra ipotesi dipende strettamente dalla specifica fattispecie, ossia da quale delle due ipotesi lo smart contract realizzi in concreto e dal rapporto tra accordo e codice informatico



definizione normativa parrebbe alludere alla seconda ricostruzione

# Criticità nel rispetto della normativa civilistica (1)

- applicazione delle disposizioni in materia di **inadempimento** → adempimento è automatico e prescinde dal comportamento delle parti



Al riguardo rileva l'art. 1375 c.c. ai sensi del quale l'esecuzione del contratto deve avvenire secondo **buona fede** → non significa sempre un'esecuzione letterale dell'accordo, come nel caso dell'esecuzione automatica, ma può doversi declinare in una valutazione qualitativa

- **interpretazione** e norme degli artt. 1362-1371 c.c., che “secondo buona fede” portano l'interprete a dover cercare “la comune intenzione delle parti” → difficile applicazione, codice informatico esegue in modo rigido senza margini di interpretazione
- applicazione strumenti di **fase patologica**, quali vizi del consenso (errore, violenza e dolo), nullità e annullamento, risoluzione, attivazione di rimedi in autotutela o inibizione dell'esecuzione a seguito di un provvedimento giudiziale → servono come legittimo rimedio a patologie del negozio o a tutelare la parte debole, interessi meritevoli di tutela per l'ordinamento, che subirebbero un'inevitabile compressione

# Criticità nel rispetto della normativa civilistica (2)

**Codice informatico** genera significative problematiche nelle diverse fasi:

- **predisposizione del contratto** → traduzione in codice informatico di clausole generali, espressioni valoriali e principi interpretabili (buona fede, correttezza, diligenza, ragionevolezza, giusta causa etc.) → non misurabili, di difficile traduzione informatica
- **attuazione del contratto** → **barriera semantica, problemi di comprensione e intelligibilità** del contenuto per le parti e il giudice, che avrà bisogno di un interprete → in forma diversa riemerge necessità di intermediario
- **insorgenza problematiche** → **divergenze tra l'accordo** (e volontà delle parti) **e la traduzione nell'algoritmo**, per difficile traduzione o per **errori tecnici** → conseguenti vizi → necessità di solide competenze trasversali di natura giuridica e informatica

# Criticità nel rispetto della normativa civilistica (3)

Vantaggio della blockchain consistente nell'eliminazione di intermediari sostanzialmente annullato dal fatto che è **necessario comunque avvalersi di un terzo cui riporre fiducia, un soggetto con competenze informatiche**, cruciale nella fase di predisposizione del contratto, ma anche nel momento dell'attuazione o in caso di problematiche



più propriamente un **mutamento della tipologia di intermediario**, che in tal caso è chiamato a svolgere la funzione tecnica di tradurre in linguaggio informatico l'accordo, invece che quella giuridica di seguirne la genesi, la vita e l'esecuzione

**Discutibile che l'automatismo renda evitabile il ricorso a figure terze a livello giuridico** → in questi casi sono necessarie diverse figure di intermediari, dotate di competenze informatiche e giuridiche, chiamate a collaborare in modo sinergico al fine di garantire risultati scevri da criticità ed errori

# Possibili soluzioni

**Incorporazione del diritto nella tecnica** → utile per applicare **disciplina civilistica** prevedendo clausole, misure correttive e strumenti rimediali proattivi e reattivi

- funzione di autodistruzione “**kill switch**” o “**self destruct**” disciplinata dalle parti, al fine di garantire l’attuazione di eventuali pronunce di risoluzione, nullità o annullabilità
- **operazioni multi-signature (multi-sig)**, che prevedono un meccanismo di risoluzione delle controversie, avvalendosi di un utente terzo interno al sistema con funzione di arbitro
- ricorso a **meccanismi alternativi** di risoluzione delle controversie, quali la procedura di mediazione o un arbitrato

**Preventiva gestione del rischio** operata con la scelta del tipo contrattuale e delle condizioni contrattuali può costituire uno strumento efficace

# Problematica inerente la firma (1)

Art. 8-ter → smart contracts soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'AgID con linee guida



ai fini della riconducibilità del documento informatico al soggetto, può qualificarsi come “**firma elettronica avanzata identificata**” (art. 20, comma 1-bis, d.lgs. 82/2005) → il documento informatico quando è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dalle linee guida di AgID con modalità tali da garantire sicurezza, integrità e immodificabilità del documento e in maniera manifesta e inequivoca, ha valore di documento con firma avanzata



**si affianca a firma avanzata, della quale condivide valore giuridico e probatorio** (in dottrina qualificata come firma avanzata identificata)



## Problematica inerente la firma (2)

Partecipanti sono identificati nelle blockchain permissioned,  
ma non nelle permissionless → in tal caso

**firma elettronica (cosiddetta semplice)**



Idoneità a soddisfare il requisito della forma scritta e valore probatorio di documento informatico a cui è apposta firma semplice → **liberamente valutabili ex post dal giudice**, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità

(art. 20, comma 1 bis, d.lgs. 82/2005)

# Blockchain e firma

**Idoneità ad assolvere il requisito della forma scritta può mutare** a seconda della tipologia di blockchain impiegata e, anche in tal caso, scaturisce strettamente dalle caratteristiche tecniche concrete



valore giuridico ed efficacia probatoria sono diversi  
in conformità alla differente capacità tecnologica  
di garantire sicurezza e affidabilità  
circa l'identità dei soggetti e l'integrità dei dati

# STRATEGIA NAZIONALE



*Ministero dello Sviluppo Economico*

# BC

Blockchain

Verso una strategia nazionale



# Gruppo di esperti ed obiettivi

## 30 profili multidisciplinari

- mondo dell'impresa e delle associazioni di categoria
- accademia, mondo della ricerca e pubblica amministrazione
- società civile, organizzazioni sindacali, terzo settore, associazioni dei consumatori
- insieme a rappresentanti del MISE

## Elaborazione policy e strumenti

- iniziative e buone prassi esistenti
- use case relativi all'utilizzo delle DLT nel settore pubblico
- condizioni per promuovere ricerca, sviluppo, impiego e adozione
- creare e favorire condizioni economiche, politiche e regolatorie
- strumenti tecnici e normativi volti a diffondere applicazione di smart contract

# Temi della strategia nazionale

- **caratteristiche** della tecnologia e **modelli di governance**
- **scenario** globale ed europeo
- principali **casi d'uso** in Italia e in ambito internazionale
- **definizioni** di riferimento
- **contesto normativo** internazionale, UE e nazionale
- **indirizzi** strategici
- **ricerca e sperimentazione** su blockchain e registri distribuiti
- **educazione, skills e apprendimento** permanente
- **settori strategici e use case abilitanti**

Tra giugno e luglio 2020 [consultazione pubblica](#) svolta dal Ministero dello Sviluppo economico sulla sintesi del documento elaborato dal Gruppo di esperti.

# Applicazioni

- ambito finanziario e monetario (prima applicazione pratica, il Bitcoin)
  - supply chain → farmaceutica, agrifood & beverage, automotive, abbigliamento, contratti di franchising
  - processi aziendali
  - settore agroalimentare
  - settore assicurativo
  - pubblica amministrazione
  - identità digitale
  - gestione dei diritti di proprietà intellettuale
  - brevetti
  - settore energetico
  - proprietà di asset
- etc.

# Supply chain e blockchain (1)

- **certificazione, tracciabilità, fiducia e decentralizzazione** → prodotti, merci (da origine a consegna), processi, scambi, riducendo errori e frodi e prevenendo contraffazioni grazie a tracciamento
- **automazione e sicurezza** → logistica e trasporti, gestione inventario, controllo circa esistenza e completezza dei documenti di spedizione
- **smart contracts** → eliminazione dei dubbi di interpretazione su quanto stabilito dai contratti, semplificazione e riduzione costi, minor litigiosità e disintermediazione



## **vantaggi**

in termini di trasparenza, qualità, riduzione di costi e tempi, sicurezza, crescita dei ricavi, automazione e ottimizzazione processi, identificazione e riduzione dei problemi, monitoraggio in tempo reale, fiducia clientela

[https://www.osservatori.net/it\\_it/osservatori/blockchain-distributed-ledger](https://www.osservatori.net/it_it/osservatori/blockchain-distributed-ledger)



# Supply chain e blockchain (2)

- **IBM Food Trust** → blockchain permissioned Hyperledger Fabric → certificazione qualità del prodotto, trasparenza e tracciabilità di tutta la filiera agro-alimentare evitando casi di contaminazione, contraffazioni e richieste da parte dei consumatori di maggiori informazioni sulla provenienza del cibo
- **Nestlé** → blockchain per tracciabilità e sicurezza della catena di approvvigionamento (ingredienti nella purea di patate)
- **Coop Chain** → trasparenza e visibilità dei vari attori coinvolti nella filiera della produzione delle uova a marchio Coop
- **Carrefour** → blockchain per tracciare la produzione di polli ruspanti

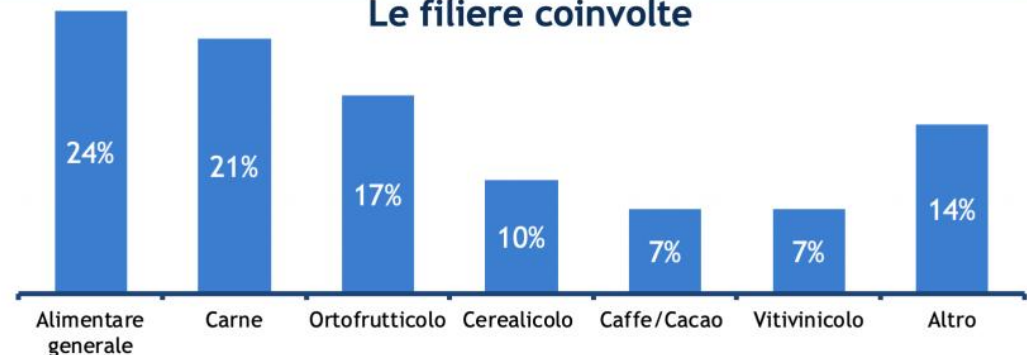
## Blockchain per la tracciabilità alimentare

**42 casi internazionali e italiani**

*di progetti blockchain nel food tra il 2016 e il 2018*

- Più che **raddoppiati** nell'ultimo anno
- Particolarmente interessate le **filiere della carne e dell'ortofrutta** (cfr. recenti «crisi alimentari» che hanno coinvolto i settori)

### Le filiere coinvolte



*Base: 42 casi applicativi*

***Grazie per l'attenzione***



**Fernanda Faini**

Research Fellow e docente in diritto dell'informatica – Università di Pisa

**email**                      fernanda.faini@jus.unipi.it

**Linked in**                      fernandafaini

