Tutto quello che il pubblico ufficiale deve sapere su smart contract, blockchain e firme elettroniche

Gea Arcella

LA FIRMA ELETTRONICA

Per firmare un documento informatico > si utilizza un procedimento informatico

Tale procedimento è l'apposizione > della FIRMA ELETTRONICA

Ogni tipologia di firma non tradizionale deve (continuare ad) essere astrattamente idonea ad assicurare le seguenti funzioni:

a) funzione indicativa, che consiste nell’identificare un soggetto (il firmatario) distinguendolo dagli altri;

b) funzione dichiarativa, ossia l’idoneità a manifestare l’adesione al contenuto del documento da parte del firmatario;

c) funzione probatoria, cioè la capacità della firma di provare la provenienza del documento

LE TIPOLOGIE DI FIRMA ELETTRONICA NEL REG. eIDAS (910/2014)

- «firma elettronica», dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare;

- «firma elettronica avanzata», una firma elettronica che soddisfi i seguenti requisiti (cfr. art. 26):

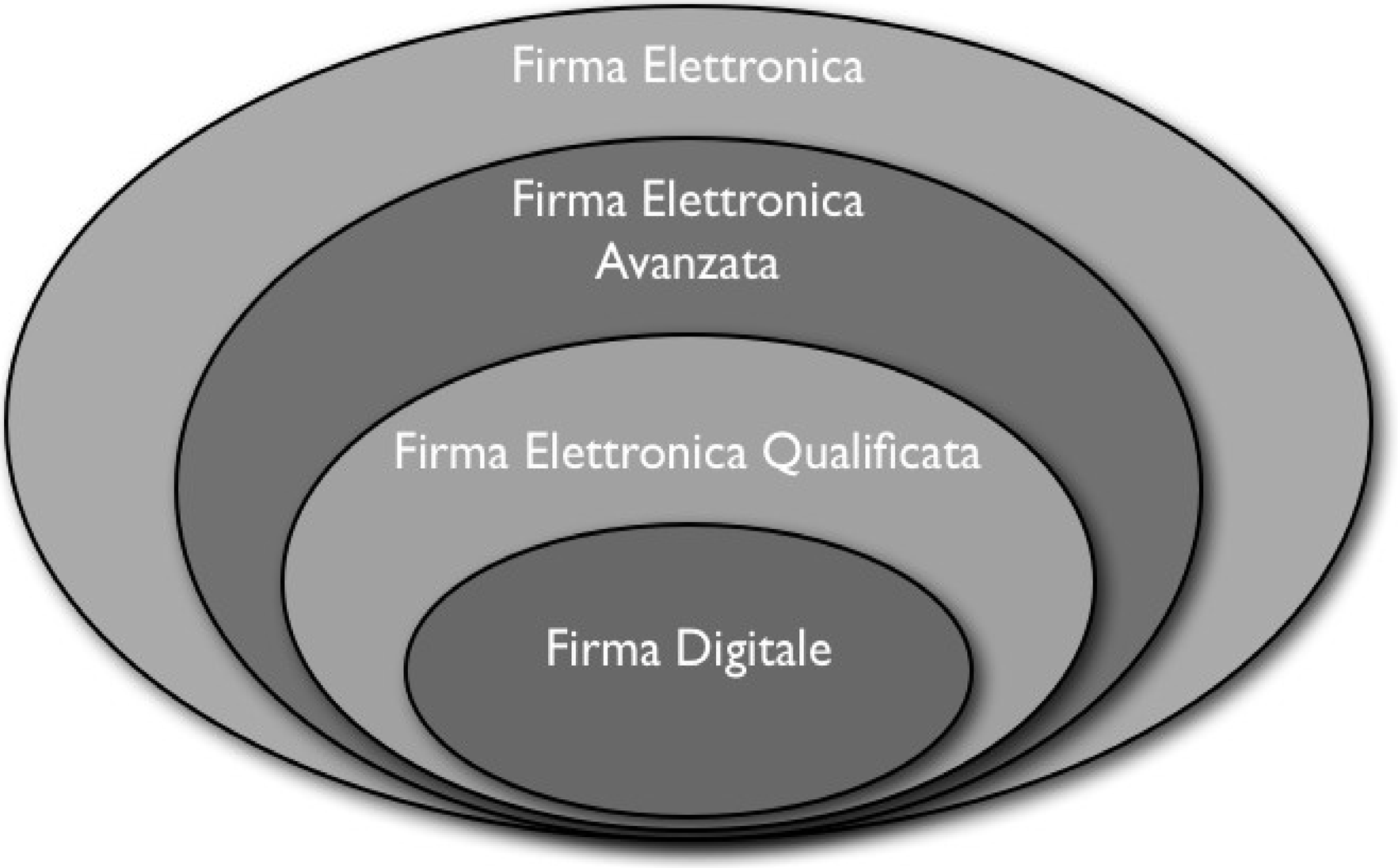
  a) è connessa unicamente al firmatario;

  b) è idonea a identificare il firmatario;

  c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo;

  d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

- «firma elettronica qualificata», una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche;


Firma Elettronica
Firma Elettronica Avanzata
Firma Elettronica Qualificata
Firma Digitale

EFFETTI GIURIDICI DELLE FIRME ELETTRONICHE

1. A una firma 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 per firme elettroniche qualificate. *(principio di non discriminazione)*

2. Una firma **elettronica qualificata ha effetti giuridici equivalenti a quelli di una firma autografa**.

(principio di equivalenza)

3. **Una firma elettronica qualificata** basata su un certificato qualificato rilasciato in uno Stato membro è **riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri**.

(principio del mutuo riconoscimento)

Regolamento eIdas art. 25

IL VALORE GIURIDICO DELLA FIRMA ELETTRONICA

A seconda della sicurezza del procedimento di firma elettronica utilizzato per sottoscrivere il documento informatico, il legislatore italiano ha graduato l’efficacia probatoria del documento medesimo.

2-bis. Salvo il caso di sottoscrizione autenticata» le scritture private di cui all’articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale. Gli atti di cui all'articolo 1350, numero 13), del codice civile «redatti su documento informatico o formati attraverso procedimenti informatici sono sottoscritti, a pena di nullità, con firma elettronica avanzata, qualificata o digitale.».

2-ter. Fatto salvo quanto previsto dal decreto legislativo 2 luglio 2010, n. 110, ogni altro atto pubblico redatto su documento informatico è sottoscritto dal pubblico ufficiale a pena di nullità con firma qualificata o digitale. Le parti, i fidefacenti, l'interprete e i testimoni sottoscrivono personalmente l'atto, in presenza del pubblico ufficiale, con firma avanzata, qualificata o digitale ovvero con firma autografa acquisita digitalmente e allegata agli atti.

Art. 21 CAD

L’autorità di certificazione

- Per garantire un adeguato livello di sicurezza tra due soggetti è necessario che sia assicurata la corrispondenza tra l’identità di ciascuno e la sua chiave pubblica.

- Questo compito viene svolto da una **terza parte fidata** che certifica l’identità del titolare di una chiave pubblica e la sua validità nel tempo attraverso l’emissione di certificati.

- Un **certificato di identificazione** lega il titolare ad una chiave pubblica digitale

Esempio di Certificato Standard X509

Versione
Numero di serie
Identificatore algoritmo
Mittente
Periodo di validità
Oggetto
Informazioni chiave pubblica
Firma digitale dell'Autorità di Certificazione

Lo standard X509 evolve in 3 versioni

ver.1 nel 1988

ver.2 nel 1993

ver.3 nel 1996

IL VALORE GIURIDICO DELLA FIRMA ELETTRONICA

Solo la firma elettronica qualificata viene direttamente equiparata dal Regolamento eIdas alla sottoscrizione autografa e gode del riconoscimento reciproco tra Stati membri se accompagnata da un certificato qualificato.

Attualmente l’unico procedimento tecnologico che assicura tutti i requisiti previsti per la firma qualifica è quello basato sulle chiavi asimmetriche che si sostanzia nella firma digitale.

DEFINIZIONE FIRMA DIGITALE

un particolare tipo di firma elettronica «qualificata» basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario 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. 1, lett. S, CAD

La firma digitale: tecnologia

cifrari asimmetrici o

“a chiave pubblica”

Mittente

chiave privata

per cifrare

Destinatario

chiave pubblica

per decifrare

LA LEGGE NOTARILE ED IL CAD

1. Le parti, i fidefacenti, l'interprete e i testimoni sottoscrivono personalmente l'atto pubblico informatico in presenza del notaio con firma digitale o con firma elettronica, consistente anche nell'acquisizione digitale della sottoscrizione autografa.

2. Il notaio appone personalmente la propria firma digitale dopo le parti, l'interprete e i testimoni e in loro presenza.

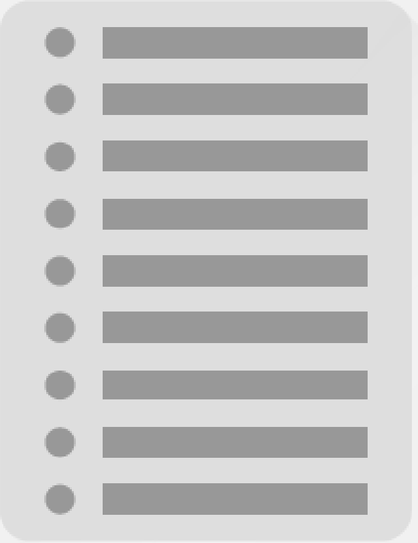
art. 52-bis l.not.

Firma autenticata. - 1. Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma elettronica o qualsiasi altro tipo di firma avanzata autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato. 2.L'autenticazione della firma elettronica, anche mediante l'acquisizione digitale della sottoscrizione autografa, o di qualsiasi altro tipo di firma elettronica avanzata consiste nell'attestazione, da parte del pubblico ufficiale, (...omissis)

art.25 CAD

il perchè di un registro

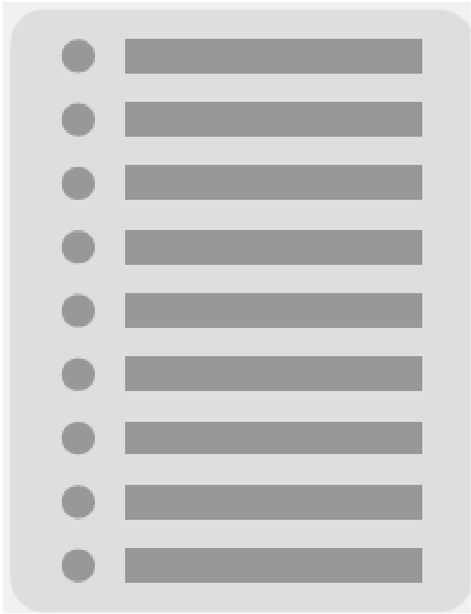
i paradossi della comunicazione inter absentes



IL VALORE DEL REGISTRO

vale per le parti

vale per i terzi



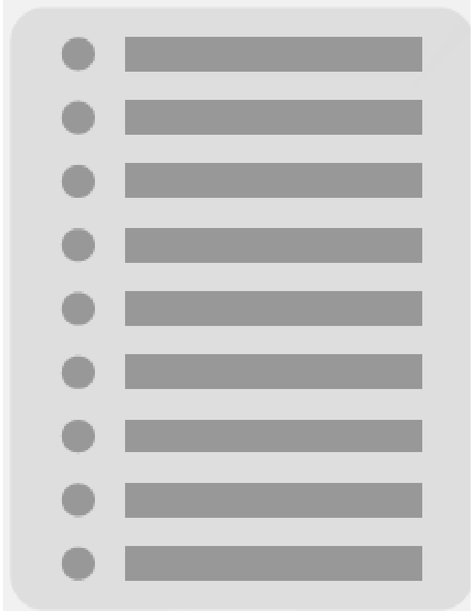
IL VALORE DEL REGISTRO

Il registro Pubblico

Registri accentrati

versus

Registri distribuiti



Il sistema blockchain

- database distribuito in cui la garanzia della registrazione è data dal fatto che più sistemi riportano in modo coerente la registrazione dell'avvenuta transazione;

- ogni volta che si voglia registrare una transazione la conferma che essa è avvenuta validamente deve provenire almeno dal 51% dei nodi che partecipano a network mediante una votazione che contemporaneamente comporta anche la risoluzione di un problema matematico (proof off work)

- La non modificabilità dei registri è data dal numero delle repliche coerenti del registro e da sistemi di crittografia.

Il sistema blockchain

- pluralità di soggetti diversi, meglio se estranei rispetto alla transazione da tracciare, che gestiscono copie dei registri anche ai fini della affidabilità e sicurezza in caso di guasti , possono costituire una rete qualificata mantenendo la propria indipendenza

- volontarietà del registro: i registri da gestire debbono essere volontari, ovvero non sono sotto il controllo e gestione di un Ente unico definito da una norma, altrimenti ricadremmo nello schema del registro accentrato.

La block chain dei bitcoin

La catena chiamata “block chain” è un repository di dati, costituito da una lista di record in continuo aumento,

una copia totale o parziale è memorizzata su **tutti i nodi del network**

I record contenuti in un singolo “blocco” della catena sono di due tipi:

- le transazioni, che sono semplici dati
- i blocchi, che sono “raccolte di transazioni” tra loro concatenate attraverso un particolare meccanismo informatico; essi costituiscono la registrazione di quali transazioni sono state inserite nel database e del loro ordine.

Il registro distribuito

- Le transazioni sono create dagli utenti del network che effettuano singole operazioni (per esempio, trasferimento di valuta ad un altro utente)

- I blocchi sono generati da una speciale categoria di partecipanti (i “miners”), che utilizzano software e a volte hardware specializzato per creare i blocchi.

Il registro distribuito: le caratteristiche

- il nuovo blocco contiene sempre al suo interno l'impronta (c.d. hash) del blocco precedente
-
- In questo modo si crea un collegamento indissolubile tra i blocchi (di qui l'immagine della catena) che rende al tempo stesso la blockchain "immutabile"

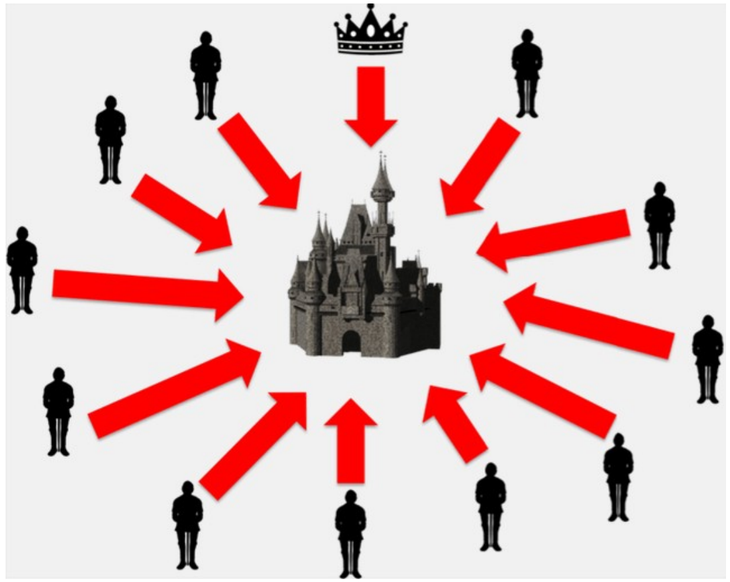
- è un registro informatico, che può essere letto "in automatico" ed interpretato sempre in automatico da un computer

Il registro distribuito: i problemi

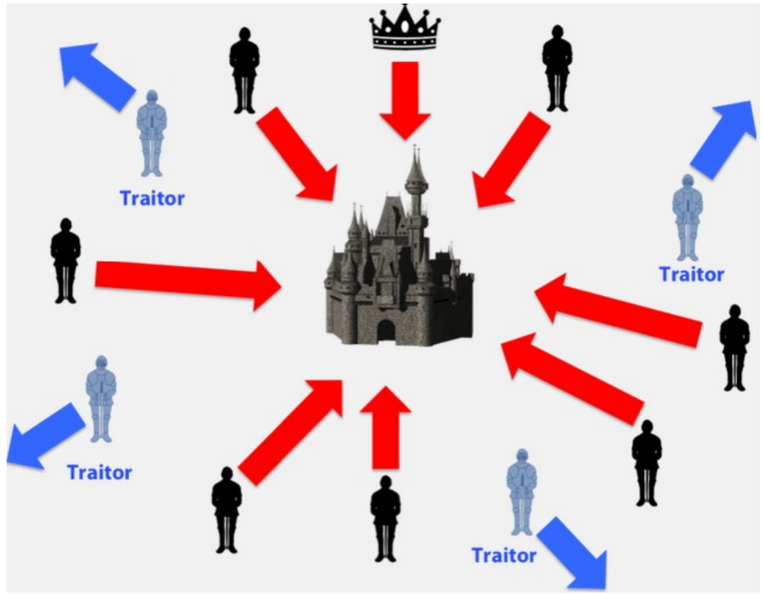
- L’esistenza di più repliche di uno stesso registro rischia di far incorrere i suoi utilizzatori in quello che - tecnicamente - viene definito il problema del “double spending” (letteralmente “doppia spesa”): una stessa risorsa viene contemporaneamente impiegata da due o più soggetti

- I registri distribuiti pongono il difficile problema della creazione di un meccanismo di consenso altrettanto distribuito, ma univoco, che consenta di evitare che singole registrazioni si accavallino oppure che si disponga più volte delle medesime utilità.

IL PROBLEMA DEI REGISTRI DISTRIBUITI
o dei Generali Bizantini



Attacco coordinato: vittoria



Attacco non coordinato: sconfitta

LA SOLUZIONE PER I BITCOIN

Proof ok work:
problema matematico complicatissimo da risolvere ma facilissimo da verificare, costantemente aggiornato all’interno della rete specifica dei bitcoin

tipi di blockchain

Pubbliche (permissionless)

Tutti possono eseguire delle transazioni o partecipare alla verifica e creazione di un nuovo blocco

Pubbliche + private (permissioned)

Si determina chi possa accedere alla rete, si definisce quali sono i ruoli che un utente può ricoprire all'interno della stessa e la visibilità dei dati registrati.

Le Blockchain permissioned

Basate sui concetti di governance e centralizzazione in una rete che nasce come assolutamente decentralizzata e distribuita

Ha diversi livelli di accesso che riguardano:

* La lettura del registro, che può essere soggetta a diverse restrizioni come ad esempio poter visionare solo le transazioni che coinvolgono direttamente l'utente specifico.

* La possibilità di proporre ed effettuare nuove transazioni che vengano poi validate ed inserite nella Blockchain.

* La possibilità di partecipare attivamente alla rete svolgendo l'attività di mining per la creazione di nuovi blocchi.

.

Le Blockchain permissioned

ritenute più sicure di quelle pubbliche

Hanno un livello di segretezza più alto controllando chi può accedervi e chi può visualizzare i dati registrati.

sono più performanti, veloci, scalabili e meno costose di quelle pubbliche, dato che hanno una dimensione e diffusione minore e che le transazioni vengono verificate da un limitato numero di utenti.

Deformazione dell'approccio originario della blockchain il cui elemento caratterizzante è determinato dall'assenza di una autorità

.

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.

D.L. 14 dicembre 2018, n. 135 convertito con modificazioni dalla L. 11 febbraio 2019, n. 12

REGISTRI DISTRIBUITI E SMART CONTRACT

Scopo dichiarato della norma è consentire, attraverso l'utilizzo di una blockchain e dei processi c.d. di tokenizzazione, di poter dimostrare in futuro la paternità e l'anteriorità di un token digitale dal contenuto più disparato (dal semplice hash di un documento ad un identificativo di un oggetto reale).

Il dato contenuto nella blockchain non dipende da un dato pregresso e **la blockchain diventa unicamente un registro, sicuro, ma con solo funzioni di contenitore.**

BIT COIN E SMART CONTRACT

Caratteristica della blockchain è la sua capacità di essere un registro informatico, che può essere letto ed interpretato in automatico da un computer

Il sistema dei Bitcoin ha inserito nel proprio meccanismo di funzionamento un'ulteriore "condizione" operativa, che consiste nel seguente comando: "autorizzo la transazione di X bitcoin solo se ... dopo aver interrogato la blockchain ... emerge che il disponente Tizio ha X, o più, bitcoin".

Questa caratteristica di lettura ed interpretazione dei dati contenuti nel registro caratterizza (attualmente) le criptovalute e non la blockchain e prefigura il funzionamento degli smart contracts.

SMART CONTRACT

Attraverso lo smart contract non ci si limita ad inserire nella blockchain un dato, ma quel dato contiene ulteriori istruzioni, che la blockchain stessa eseguirà in modo del tutto indipendente dalla (successiva) attività delle parti.

La capacità di eseguire comandi secondo un logica “If /Then” caratterizza gli smart contracts

SMART CONTRACT

Il termine “smart contract” è stato coniato negli anni '90 da Nick Szabo, un informatico statunitense, con studi legali e di crittografia:

“L'idea di base dello smart contract è che molti tipi di clausole contrattuali (come la garanzia, l'assunzione dell'obbligazione, la delimitazione di un diritto di proprietà, ecc.) possono essere incorporati nell'hardware e nel software che trattiamo, in modo da rendere la violazione del contratto costosa (se desiderato, addirittura proibitiva) per il soggetto inadempiente”.

SMART CONTRACT

Lo smart contract, come elaborato da Szabo, dovrebbe essere una sorta di integrazione tra un software (che contiene le istruzioni), ed un hardware (che tali istruzioni è chiamato ad eseguire materialmente) o un punto di destinazione (cioè il luogo - fisico o virtuale - ove sono destinate ad agire le istruzioni automatizzate) che manca totalmente nella definizione normativa italiana

La norma definisce lo smart contract esclusivamente come un “programma per elaboratore” (quindi come un software) che per indurre una modificazione del mondo reale avrà comunque bisogno di una ulteriore e separata disciplina contrattuale.

La diffusione degli scambi in criptovalute contante digitale o nuovi strumenti "finanziari"?

LE CRIPTOVALUTE IN SENSO STRETTO

gettoni digitali (digital tokens) privati

senza diritti incorporati

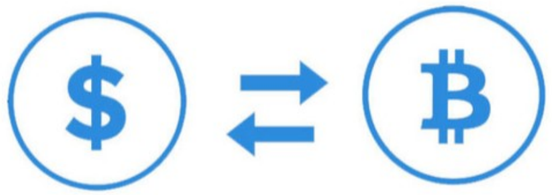
convertibili, a prezzo variabile

che operano attraverso registro gestito in modo decentrato

denominato blockchain o DLT (distributed ledger technology)

ALTRI DIGITAL TOKENS

- payment tokens, rappresentazioni digitali di valore emessi da una entità giuridica a fronte di una quantità di moneta tradizionale;
- utility tokens, che rappresentano diritti amministrativi non trasferibili e non negoziabili;
- security tokens, rappresentazioni digitali di diritti trasferibili e negoziabili quali: diritti di voto, diritti su flussi di cassa, diritti di proprietà su attività finanziarie o quote su beni reali standardizzabili (commodities) più spesso oggetto di ICOs
- NFT, (non-fungible token) è un tipo speciale di token crittografico che rappresenta il titolo di proprietà di un bene unico (digitale o fisico); non sono reciprocamente intercambiabili, diversamente dalle criptovalute, come bitcoin e molti token di rete o di utilità, che sono per loro stessa natura fungibili.



criptovalute e tracciabilità

exchanges e wallet providers

Gli operatori in valute virtuali secondo il D.LGS 231/2007

persona fisica o giuridica che

fornisce a terzi,

a titolo professionale,

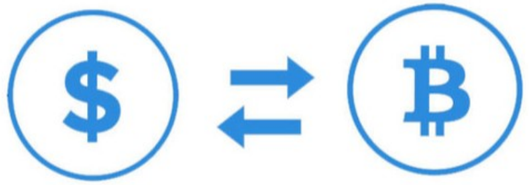
servizi funzionali

all'utilizzo, allo scambio,

alla conservazione di “valuta virtuale” e alla loro

conversione da ovvero in valute aventi corso legale

art. 1, comma 2, lett. ff



criptovalute ed anonimato

L'utilizzo della tecnologia c.d. blokchain con il registro distribuito

garantisce:

- l'impossibilità una double spendig

- il tracciamento informatico della transazione

Le chiavi crittografiche che consentono l'utilizzo

delle criptovalute rimangono anonime.

Registrazioni senza **transazione**

Transazioni senza **registrazione**

criptovalute ed anonimato

Possibilità di trasferire le criptovalute fuori dai circuiti regolamentati: -

tramite il mero trasferimento del wallet fisico che le contiene, o

-mediante prestatori di servizi che hanno il loro stabilimento in paesi che

non prevedono nessun obbligo

di identificazione dei propri utenti

Scambi in criptovalute:

vendita o permuta?

LE CRIPTOVALUTE: MONETA O BENE IMMATERIALE?

2 teorie:

- strumenti finanziari o come **beni immateriali**
- **strumenti di pagamento (moneta)**

“moneta virtuale”:

alternativa a quella tradizionale la cui circolazione si fonda sull’accettazione volontaria da parte degli operatori del mercato che, sulla base della fiducia, la ricevono come corrispettivo nello scambio di beni e servizi, riconoscendone, quindi, il valore di scambio indipendentemente da un obbligo di legge

LE VALUTE VIRTUALI SECONDO IL D.LGS 231/2007

rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un’autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l’acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente

art. 1, comma 2, lett. qq

criptovalute: vendita o permuta?

1) E' permuta e non vendita lo scambio di due monete, qualora queste siano considerate per il loro valore intrinseco o artistico.
2) E' permuta e non vendita il cambio di monete di taglio grosso, con monete di taglio più piccolo.

Cottino in "Del riporto. Della permuta."

criptovalute: vendita o permuta?

1470 C.C. La vendita è il contratto che ha per oggetto il trasferimento della proprietà di una cosa o il trasferimento di un altro diritto verso il corrispettivo di un prezzo

1277 C.C. I debiti pecuniari si estinguono con moneta avente corso legale nello Stato al tempo del pagamento e per il suo valore nominale

1278 C.C. Se la somma dovuta è determinata in una moneta non avente corso legale nello Stato, il debitore ha facoltà di pagare in moneta legale, al corso del cambio nel giorno della scadenza e nel luogo stabilito per il pagamento

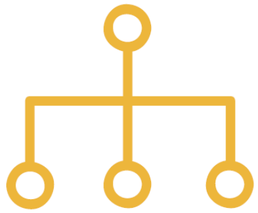
1279 C.C. La disposizione dell'articolo precedente non si applica, se la moneta non avente corso legale nello Stato è indicata con la clausola "effettivo" o altra equivalente

3 caveat sulla blockchain

Il registro e la blockchain

L'impronta non è il documento

Gli smart contract



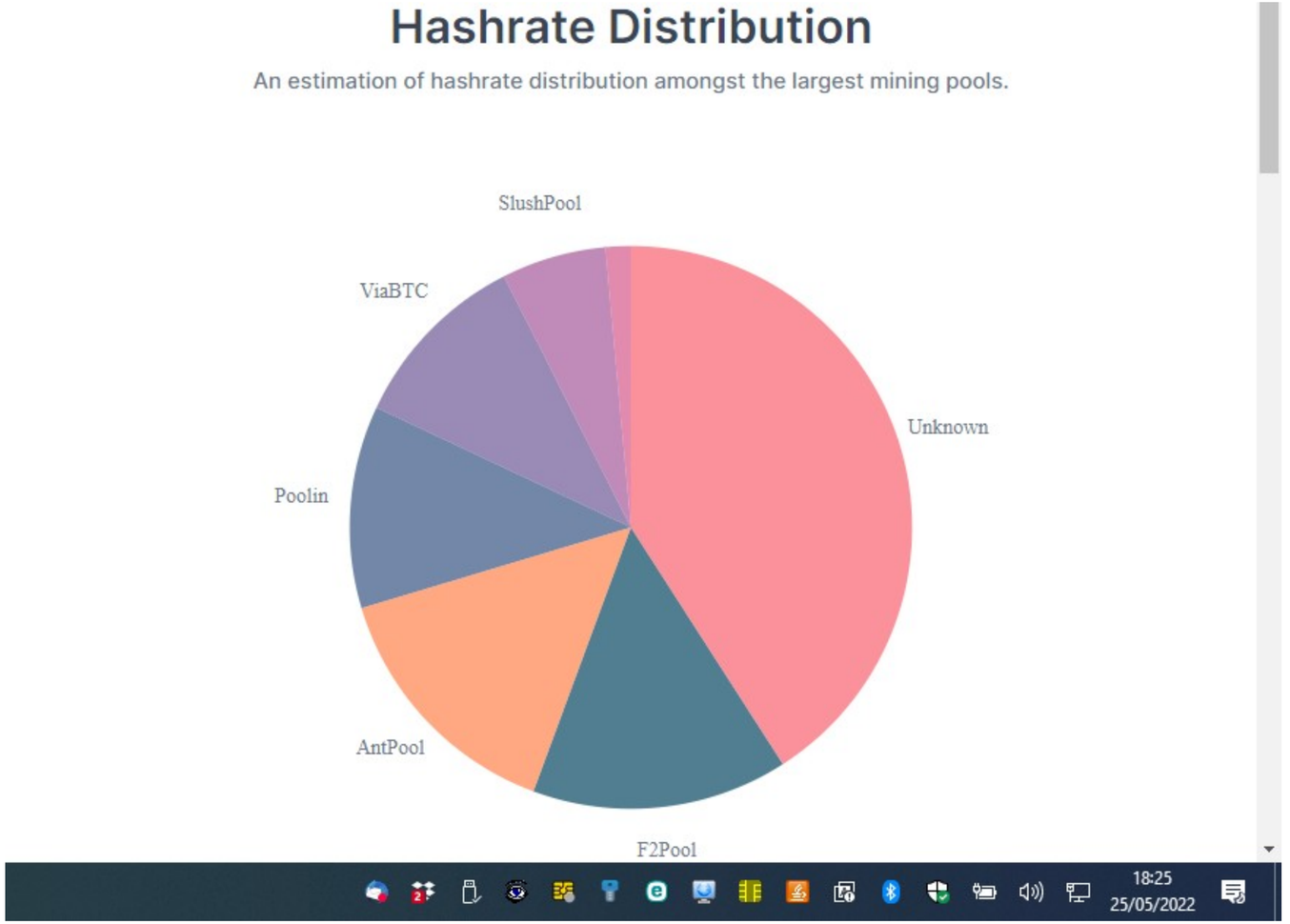
Lo smart contract non è il contratto

criptovalute

Chi paga il sistema?
la rete bitcoin consuma quanto l'Eire

Chi controlla chi?
blockchain permissioned o permissionless?

https://blockchain.info/pools



Grazie per l'attenzione

garcella@notariato.it