

Lecture 10 dicembre 2014 – Dipartimento di Economia – La Sapienza

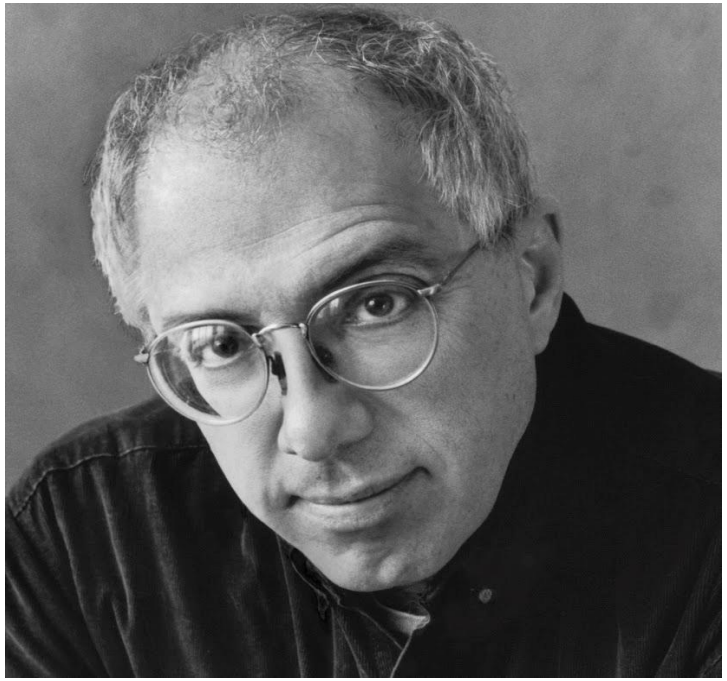
Bitcoin: la moneta digitale «downloadable» e nuovi pagamenti

(analisi Law and Economics)

Avv. Giulia Arangüena

© ADLP Studio Legale 2014 – All Rights Reserved

Un passo indietro



1994 – Steven Levy per Wired

“The killer application for electronic networks isn't video-on-demand. It's going to hit you where it really matters - in your wallet. It's, not only going to revolutionize the Net, it will change the global economy”.

© ADLP Studio Legale 2014 – All Rights Reserved

Gli antenati del Bitcoin



Illustrazione: Martin Venezky

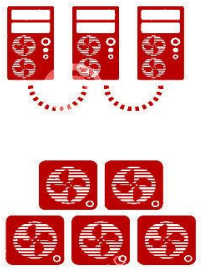
- Digi Cash (David Chaum)
- Web Money
- E-Gold
- B-Money

Il concetto di una moneta *online* decentralizzata esiste da quando si è approdati ad una visione di Internet come una risorsa pubblica; e ci sono stati nel tempo vari tentativi di creare una moneta *online* unica e globale.

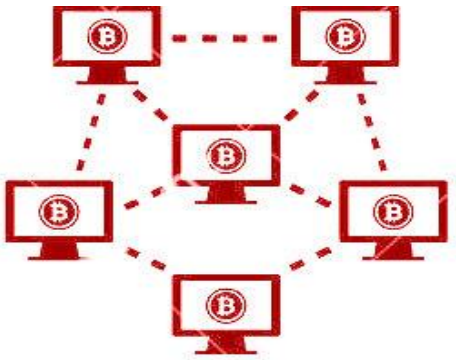
© ADLP Studio Legale 2014 – All Rights Reserved

Tecnologia + Infrastruttura = Valore Digitale

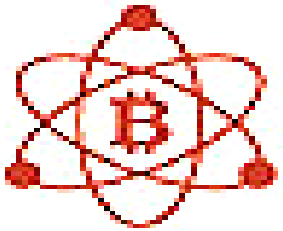
Mining Subnetwork



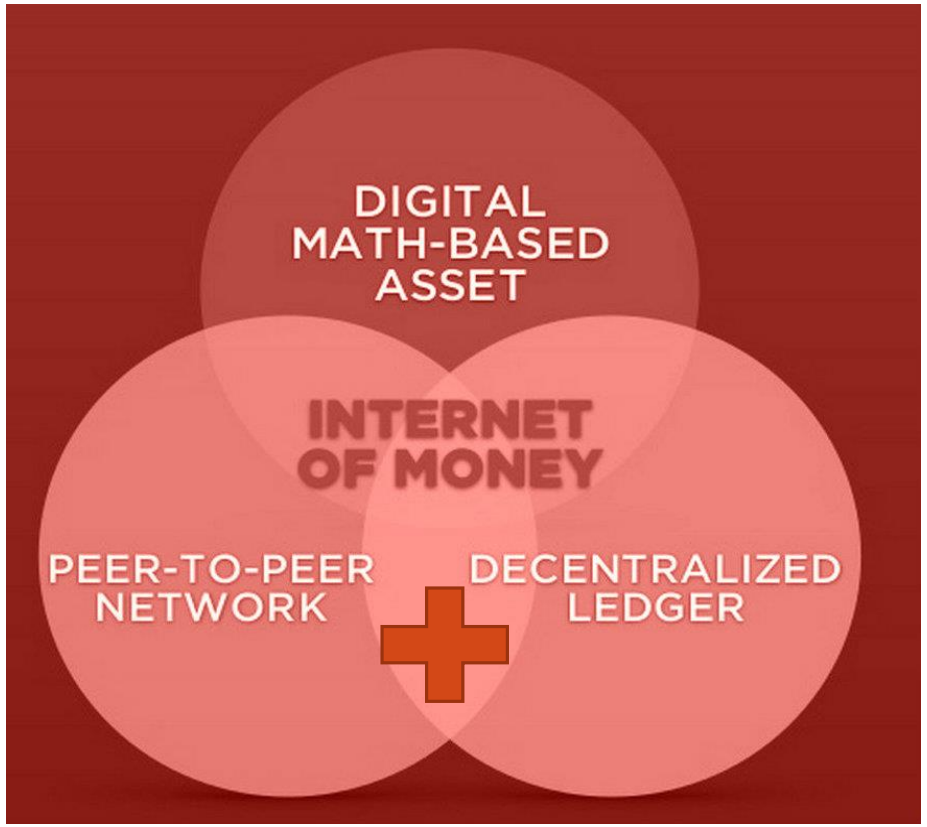
2 funzioni:
- Estrarre e mettere in circolazione nuova unità di valore digitale
- Validare (autenticare) i trasferimenti di esso nella rete



Rete P2P



Blockchain o catena dei blocchi



bitcoin

Bitcoin

© ADLP Studio Legale 2014 – All Rights Reserved

Come funziona

1454A2geTxaJwF8eqry7oLECdomgDSj62x

Public Key ("Address")
34 characters starting with **1** or **3**
Represents a possible destination for payment

Private key
51 characters starting with 5
Usata nei trasferimenti



Blocco – encripted data container

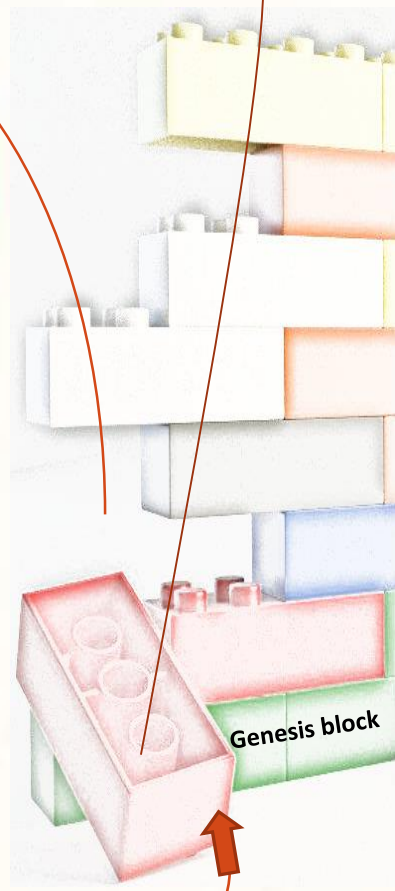
Combination

Proof of Work

Potenza di calcolo: combina tutti i caratteri alfanumerici possibili finché non si trova il «codice» per decifrare il messaggio/dati del blocco

Autenticazione dei dati contenuti nel blocco





© ADLP Studio Legale 2014 – All Rights Reserved

Ledger

Dave	12.5
Alice	323
Bob	6.2
Carol	10
Eve	100
Scott	.00000001
Kristin	45
...	...

+5.2

-5.2





Bob



Carol

© ADLP Studio Legale 2014 – All Rights Reserved

Che cos'è il bitcoin?

Empiricamente:

- è la ricompensa che traggono i minatori per il lavoro di estrazione dei dati e di autenticazione dei trasferimenti (*reward* fisso + commissioni)

Funzionalmente

- è la **rappresentazione informatica certificata** di dati presenti nella Blockchain, decifrati, autenticati e resi trasferibili – in rete – attraverso l'apposizione di una sequenza di firme digitali

© ADLP Studio Legale 2014 – All Rights Reserved

Le idee di base



E’ moneta qualunque oggetto che sia accettato in un determinato paese/contesto sociale come pagamento per beni, servizi o debiti (funzione di intermediazione di Keynes)

Tale oggetto/valore può essere anche un qualsiasi dato informatico

L’uso della crittografia per controllare la creazione e il trasferimento del valore può sostituire enti centrali e altri intermediari

© ADLP Studio Legale 2014 – All Rights Reserved

«Rarità digitale»

Il bitcoin ha la **medesima** struttura economica della moneta: si basa sul **principio di scarsità e rarità** (preziosità).

Ma nel sistema Bitcoin, la «**rarità**» non si fonda su riserve di metalli preziosi, o su altri elementi rari (monopolio della forza, potenza militare, etc.), ma è «**digitale**».

Tale «rarità digitale» è **indotta artificialmente** attraverso un algoritmo a casualità programmata che pone «**difficoltà crescenti**» (*challenge*) che richiedono una dimostrazione del lavoro svolto per risolverle (*proof of work*), costosa da produrre (energia impiegata nel calcolo) ma attendibile e veloce da verificare.



© ADLP Studio Legale 2014 – All Rights Reserved

Quasi-money

Dal punto di vista economico il bitcoin è denaro (quasi).

Sebbene in maniera imperfetta e non del tutto equivalente, svolge tutte e tre le tipiche funzioni della moneta:

- Mezzo di scambio
- Unità di conto
- Riserva di valore

Per questo il bitcoin è stato definito come una «*quasimoney*»

© ADLP Studio Legale 2014 – All Rights Reserved

Limiti costituzionali generali

Nella definizione giuridica della totalità delle monete legali esistenti nel mondo, le stesse sono intese come emanazione monopolistica del potere sovrano degli ordinamenti statali, sostenuto dalle rispettive **capacità di raccolta dei tributi**.

Moneta è solo la moneta legale degli Stati, emessa dalle Banche Centrali per conto degli stessi.



© ADLP Studio Legale 2014 – All Rights Reserved

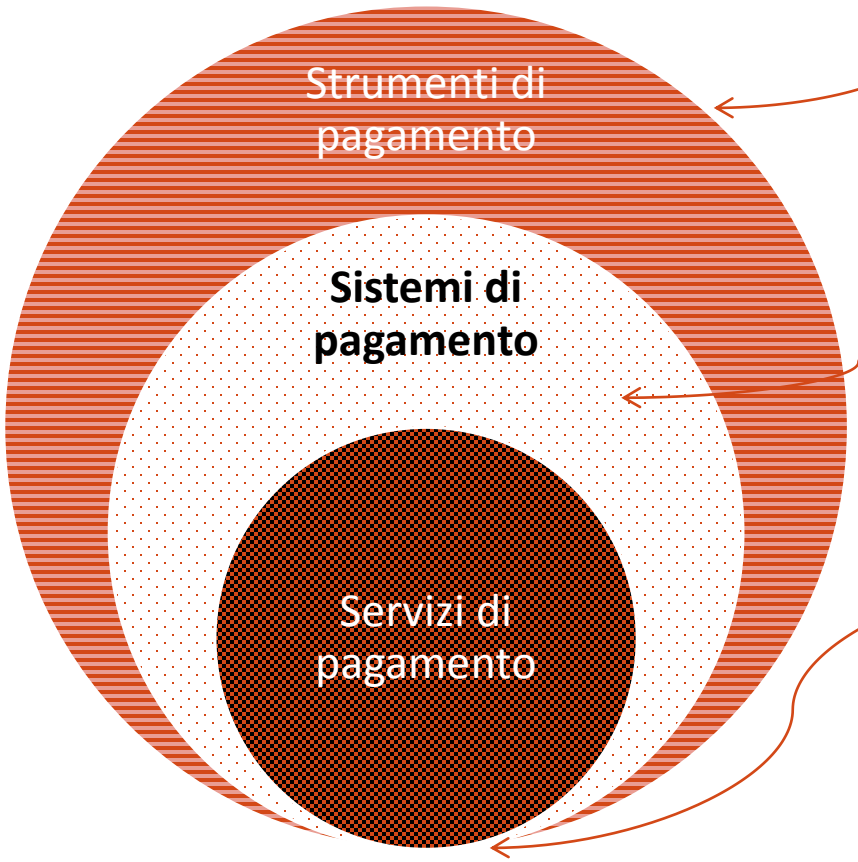
Temperamento del principio monetario

- Nel nostro ordinamento i debiti pecuniari si estinguono con moneta avente corso legale nello Stato al tempo del pagamento e per il suo valore nominale (art. 1227 c.c.)
- Secondo la Cassazione esiste però un fenomeno di progressiva «smaterializzazione» del denaro che risponde ad esigenze di sicurezza e di velocizzazione dei rapporti.
- Necessità di un'interpretazione evolutiva del **principio monetario** per adeguarlo alla mutata realtà.
- L'oggetto del pagamento non è più la moneta nella sua entità materiale, ma **il suo valore.**

Cass. Civ. Sez. Un. 18 dicembre 2007 n.26617

© ADLP Studio Legale 2014 – All Rights Reserved

Smaterializzazione della moneta



Strumenti alternativi alla moneta di rappresentazione monetaria, ugualmente capaci di trasferire valore tra soggetti e soddisfare obbligazioni pecuniarie

Complesso degli strumenti e delle procedure volti ad agevolare lo scambio di risorse

Insieme di procedure tecniche e operazioni svolte da un soggetto qualificato professionalmente e specializzato, atte a consentire l'esecuzione di pagamenti

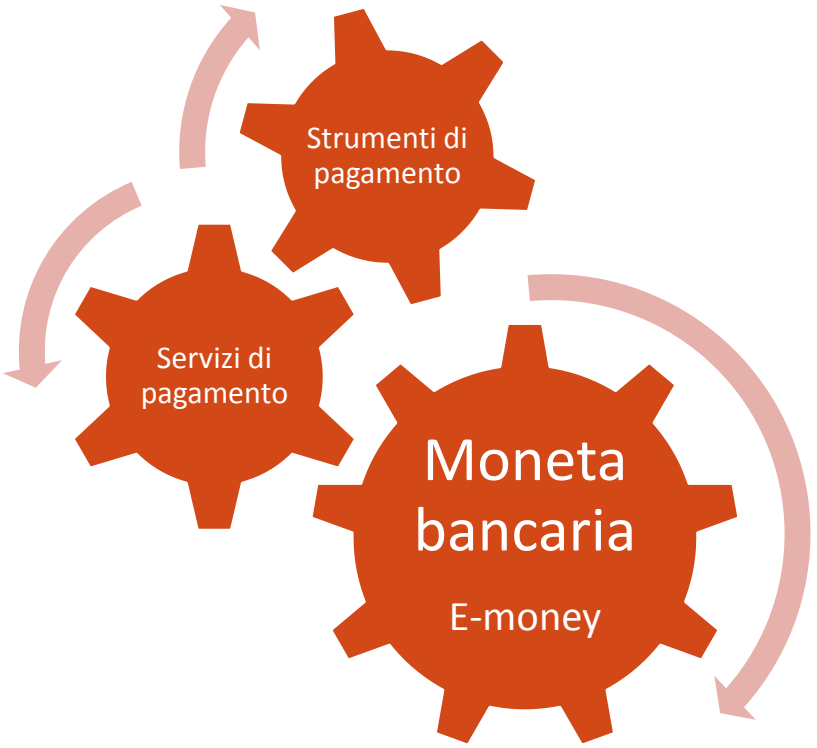
© ADLP Studio Legale 2014 – All Rights Reserved

Attuale centralità della moneta bancaria

Attualmente, dal punto di vista legale ed economico, tanto la categoria degli strumenti di pagamento quanto quella dei servizi di pagamento poggia sulla **moneta bancaria**.

La moneta bancaria, inizialmente sviluppata coi titoli bancari (assegni) , è un **surrogato della moneta legale** che offre forme alternative di circolazione del denaro.

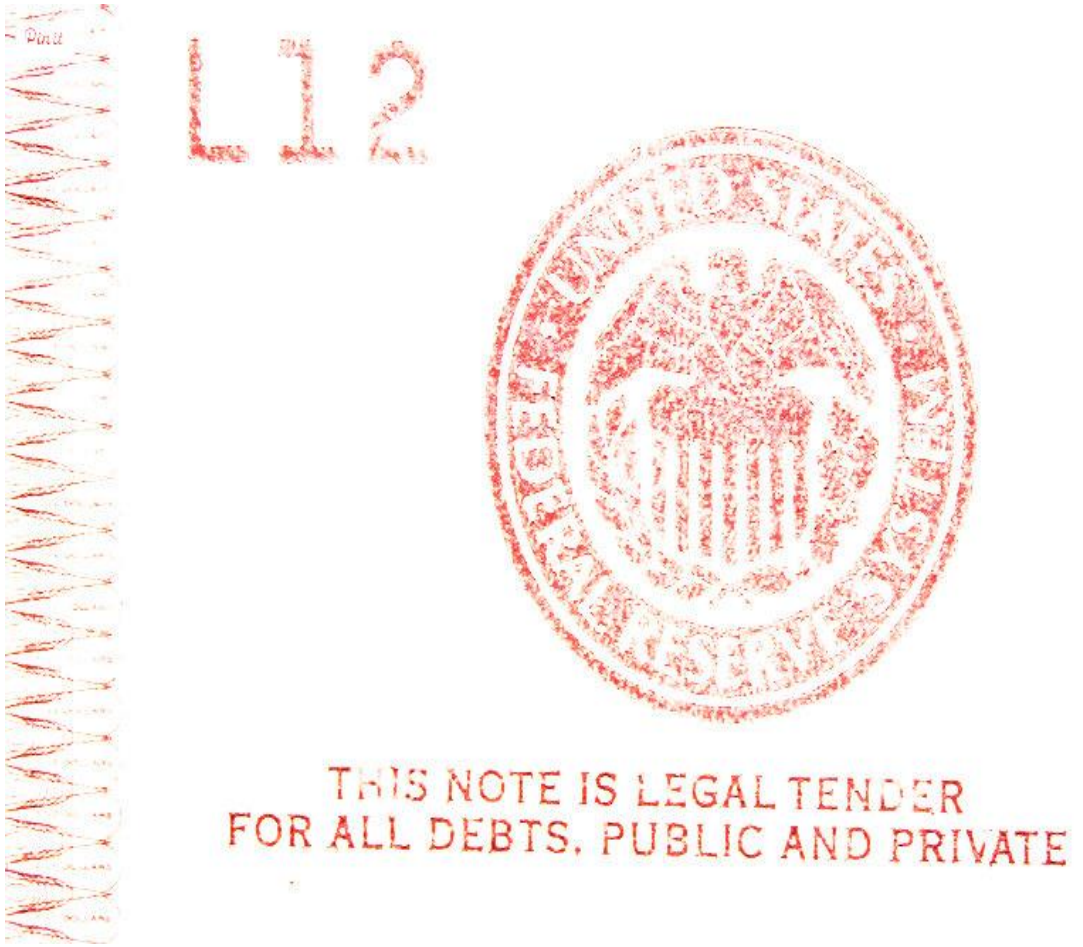
E' un «**sistema di trasporto**» del denaro che ora ha assunto caratteristiche sempre più digitali ed innovative con l'**e-money**, o moneta elettronica. [Fonte, Giorgianni – Tardivo, Manuale di diritto bancario]



© ADLP Studio Legale 2014 – All Rights Reserved

Caratteristiche della moneta bancaria

- La moneta bancaria è **moneta di conto**
- Equivale, dal punto di vista economico, al valore della moneta legale
- E' moneta fiduciaria ma non è moneta legale
- Soggiace al rischio di conversione (difficoltà della banca di rimborsare l'equivalente in moneta a corso forzoso)



© ADLP Studio Legale 2014 – All Rights Reserved

Che cos'è la moneta bancaria?

- Prestiti in corso di utilizzo regolati in conto corrente
- Depositi dei clienti
- Somma dei saldi creditore dei conti correnti



La moneta bancaria è **l'insieme delle passività delle banche** messe a disposizione del pubblico e regolate in conto corrente

© ADLP Studio Legale 2014 – All Rights Reserved

Fattori di sviluppo della moneta bancaria

- Funzione monetaria delle banche commerciali che si affianca alla funzione istituzionale delle tutela del risparmio
- Proporzione inversa tra il numero di operazioni collegate al conto concorrente e ai depositi regolate il moneta bancaria, e utilizzo di scorte di liquidità (**abbattimento costi di utilizzo del contante**)
- Capacità di utilizzare le passività in bilancio per produrre redditi
- Possibilità di gestione di massa di operazioni di raccolta e operazioni di impiego
- **Scambio tra un debito a vista della banca** (i saldi creditore dei depositi e c/c) **con un debito altrui a scadenza differita**

© ADLP Studio Legale 2014 – All Rights Reserved

Bitcoin vs. moneta elettronica

Secondo la Direttiva n. 2009/110/CE, la moneta elettronica deve:

- essere memorizzata elettronicamente;
- essere **emessa dietro ricezione di fondi** di importo non inferiore al valore monetario memorizzato; e
- essere accettata come mezzo di pagamento da imprese diverse dall'emittente.

Il bitcoin è conforme al primo ed al terzo dei requisiti posti dalla normativa europea sulla moneta elettronica.

Ma, limitatamente all'attività di Mining che porta alla creazione di moneta, in quanto svincolato dalla ricezione di fondi di valore equivalente al valore monetario emesso (o estratto), il **bitcoin non è qualificabile come moneta elettronica**, pur comportandosi come tale negli scambi

© ADLP Studio Legale 2014 – All Rights Reserved

Il paradosso del lavoro vs. il debito



Il Bitcoin non si fonda sul debito ma sulla c.d. *proof of work*

L'e-money, fondandosi sul debito, non rispetta il principi di «scarsità»

L'attività di *mining* è una attività lavorativa altamente specializzata

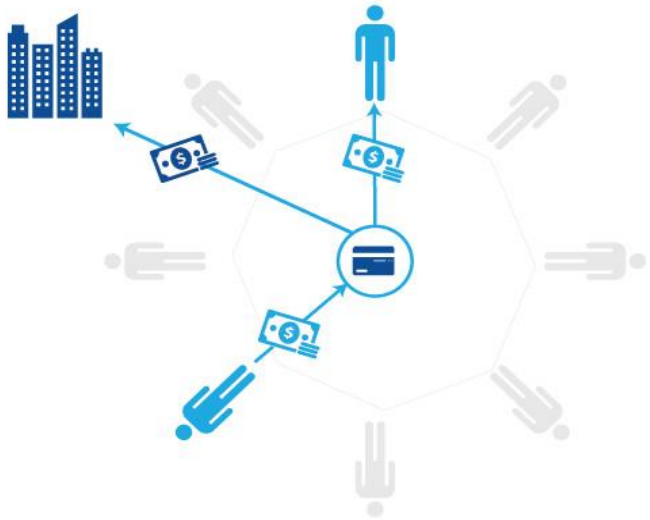
La forza probatoria e l'autenticità della Blockchain è distribuita all'interno *network* e non si fonda sull'affidabilità di un unico soggetto

I costi di energia elettrica necessari per il computo a difficoltà crescenti sono trasformati per conferire «rarità» digitale alle unità di conto e aumentare la potenza di calcolo della rete

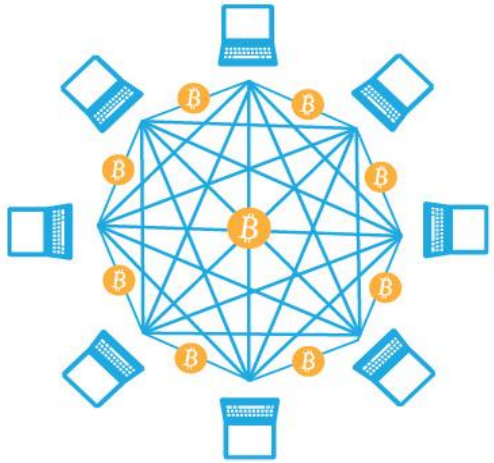
Avv. Giulia Arangüena

© ADLP Studio Legale 2014 – All Rights Reserved

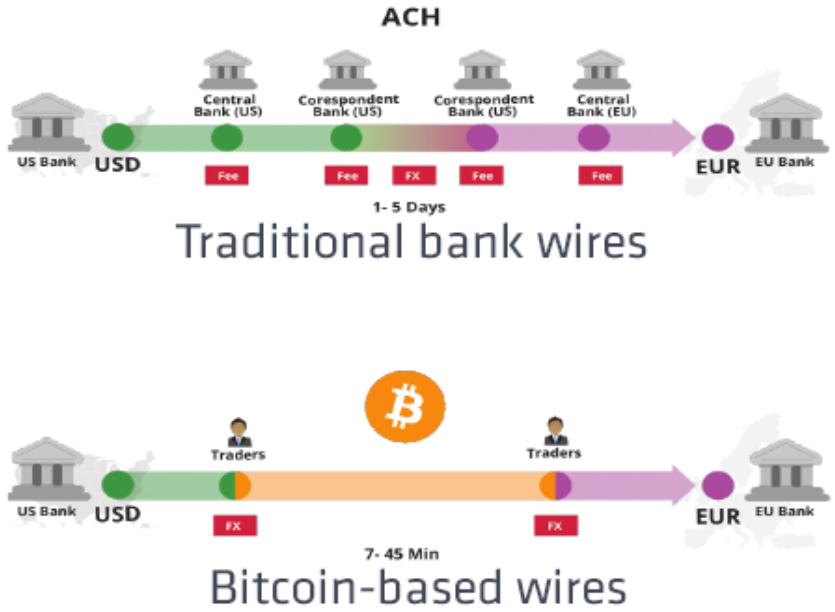
Servizi Bitcoin di e-payment



Current payment systems require third-party intermediaries that often charge high processing fees ...



... but machine-to-machine payment using the Bitcoin protocol could allow for direct payment between individuals, as well as support micropayments.

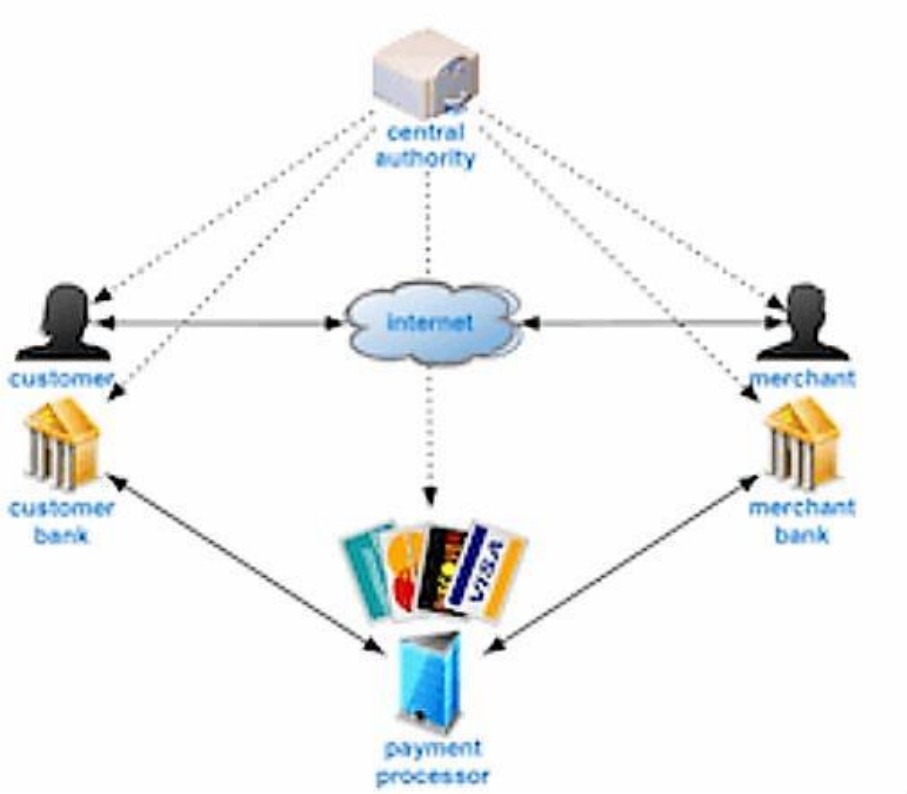


Graphic: Deloitte University Press | DUPress.com

I servizi di pagamento offerti dal protocollo Bitcoin sono immediati e diretti tra i soggetti interessati ad una determinata transazione. Il *settlment* avviene in assenza di intermediari

© ADLP Studio Legale 2014 – All Rights Reserved

Impatto *disruptive* sul commercio elettronico



Il Bitcoin si fonda sulla creazione e funzionamento della Blockchain.

Tale sistema è caratterizzato dal processo mediante il quale i suoi utenti "conciliano" le modifiche da apportarvi e cioè le operazioni accettate come valide e annotabili su di esso.

La Blockchain e la rete p2p consentono operazioni commerciali e transazioni economiche **senza la necessità di un terzo di fiducia** che garantisca la corretta esecuzione dello scambio.

Il protocollo elimina gli attuali sistemi fondati sulla fiducia, cioè "*trust-less*", professionalmente garantita dal sistema bancario e finanziario tradizionale

© ADLP Studio Legale 2014 – All Rights Reserved

Vincoli legali attuali

- La Direttiva n. 2007/64/UE (c.d. PSD) stabilisce norme relative all'esecuzione dei pagamenti qualora i fondi siano costituiti in moneta elettronica (non disciplina l'emissione, né modifica la regolamentazione prudenziale, né consente ai prestatori dei servizi - istituti di pagamento - di emettere moneta elettronica).
- Il bitcoin non è moneta elettronica e quindi il sistema di pagamento Bitcoin non rientra nel campo di applicazione della PSD.
- Il D.lgs. N. 11/2010 , modificando il TUB, ha inserito:

  - art. 114 *sexies* che riserva in esclusiva l'attività di prestazione dei servizi di pagamento alle banche, IMEL e ai soggetti iscritti all'albo degli istituti di pagamento;

  - art. 131 *ter* che punisce l'esercizio abusivo dell'attività di prestazione dei servizi di pagamento.

E' in atto processo di negoziazione della proposta della Commissione (luglio 2013) di riforma ed emanazione PSD2, a seguito del Libro Verde (gennaio 2012) sull'e-payment

© ADLP Studio Legale 2014 – All Rights Reserved

Natura sociale e relazionale del denaro

Sebbene i processi storici di istituzione della moneta siano legati all'intervento dello Stato nelle relazioni private e si basino sulla forza pubblica, **l'ontologia del denaro è** rimasta tanto **relazionale, astratta e cogente quanto quella dei contratti** in generale.

E le **possibilità di formulare contratti sono molteplici** …
(nei limiti della c.d. autonomia privata, quale espressione della libertà originaria dei soggetti, preesistente a qualsiasi riconoscimento giuridico).

© ADLP Studio Legale 2014 – All Rights Reserved

Autonomia privata

L'autonomia privata costituisce un concetto fondamentale del diritto: in generale, è il potere dei privati di regolare liberamente i propri interessi e di decidere della propria sfera giuridica, nel rispetto dei limiti e degli obblighi stabiliti dall'ordinamento. In base al rapporto tra soggetto privato e ordinamento giuridico, l'autonomia privata viene definita di volta in volta o come *potere riconosciuto* ai privati ovvero come *libertà originaria*, fenomeno anzitutto sociale e preesistente a qualunque tipo di riconoscimento giuridico. La Costituzione non la menziona espressamente ma la tutela indirettamente all'art. 3 (come strumento necessario al pieno sviluppo della persona umana) e all'art. 41 (come iniziativa economica privata). All'interno del concetto generale di autonomia privata occorre distinguere varie categorie: si parla di *autonomia contrattuale* (art. 1322 c.c.) con riferimento specifico al potere di determinare liberamente il contenuto del contratto nei limiti imposti dalla legge, sia in caso di contratti il cui schema astratto è previsto dal legislatore (contratti tipici), sia in caso di contratti che non appartengano a nessuno schema astratto previsto dal legislatore (contratti atipici), purché, in questo secondo caso, siano diretti a realizzare interessi meritevoli di tutela secondo l'ordinamento giuridico. Si parla altresì di *autonomia negoziale* come categoria più generale dell'autonomia contrattuale perché riferita a tutti i negozi giuridici, benché occorra precisare che l'autonomia privata non si possa esplicare per tutti i negozi con la stessa ampiezza.

© ADLP Studio Legale 2014 – All Rights Reserved

Qualificazione giuridica generale

Il Bitcoin è giunto ad avere una sua **rilevanza giuridica**.

Ancorché privo di materialità e senza disciplina legale nel nostro ordinamento, il Bitcoin rappresenta un **"bene giuridico"**, una «res» che conferisce diritti e facoltà rientranti nella nozione della proprietà art. 810 c.c.).

Il Bitcoin è già in grado, cioè di attribuire utilità a chi lo possiede grazie al suo valore di scambio ed alla "**meritevolezza**" di fatto (giuridica ed economica) **degli interessi e dei bisogni economici che soddisfa.**

© ADLP Studio Legale 2014 – All Rights Reserved

Punti deboli

- La nozione di "*property*" – presente negli ordinamenti di *common law* – si scontra con la nostra tradizione giuridica.
- Il nostro ordinamento e la stessa nozione dell'art. 810 c.c. sono improntati su un concetto di cosa materiale, cioè su un'idea di cosa/bene fisico dotato di una sua propria corporalità.
- Difficoltà a ricomprendere nel diritto proprietario le *new properties* e necessità di elaborazione dottrinale.
- La tutela conseguente alla sola qualificazione giuridica generale sarebbe demandata al solo (mutevole) giudizio *ex post* sulla meritevolezza degli scopi economici conseguibili, da farsi caso per caso.
- Non elimina il problema della regolazione delle attività economiche fatte con il suo impiego

© ADLP Studio Legale 2014 – All Rights Reserved

Non è property ma «smart property»

Il primo teorico della *smart property* o *smart contract*, sin dalla fine degli anni ’90, è **Nick SZABO**, della George Washington University.

Questo A. si riferisce ai c.d. contratti “intelligenti”, in quanto incorporati direttamente nei software o nell’hardware necessari al funzionamento di talune applicazioni, al fine di consentire una loro esecuzione automatizzata e correlata alla stessa tecnologia impiegata, **abbattendo i rischi legali della transazione e costi di sicurezza e fiducia nelle capacità di adempimento del contraente**

© ADLP Studio Legale 2014 – All Rights Reserved

Esempi di smart contract

Precursore degli *smart contracts* è il distributore automatico, tant'è che quando l'utente interagisce con tale macchina l'intera transazione è disciplinata ed eseguita dalla stessa infrastruttura tecnica del distributore.

- bracci meccanici all'uscita dai parcheggi o ai caselli autostradali
- disconnessione automatica dalla fornitura di servizi offerti dalle industrie a rete
- tassametri montati sui taxi
- DRM, *Digital rights management*, cioè nei sistemi di protezione elettronica incorporati in alcuni dispositivi di lettura di file recanti opere di ingegno e contenuti soggetti alle limitazioni del diritto d'autore, a protezione dei titolari dei diritti

© ADLP Studio Legale 2014 – All Rights Reserved

Natura giuridica della «smart money»

staticamente

- **Rappresentazione informatica di dati** (atti, fatti e dati giuridicamente vincolanti) muniti di autenticità digitale attraverso l'apposizione di firme elettroniche - non certificate da autorità centrali - attestanti l'avvenuta validazione crittografica degli stessi e la loro trasferibilità.

funzionalmente

- **Documento informatico** incorporante **titoli/certificati digitali nominativi** basati su identità pseudonime, rappresentativi dei dati informatici iscritti sulla Blockchain.

strutturalmente

- «**Digital baerer**» negoziabile, rappresentativo di dati/informazioni muniti di valore e recanti la certificazione della propria e l'altrui legittimazione e affidabilità a compiere una determinata transazione (a possedere, avere, spendere, trasferire, acquistare o vendere)

© ADLP Studio Legale 2014 – All Rights Reserved

A PRESTO!



Giulia Arangüena

Avvocato specialista di diritto dell'innovazione

giulia.aranguena@adlpstudio.it

Su twitter @maiameraime

© ADLP Studio Legale 2014 – All Rights Reserved