

Blockchain meets PA: an introduction

Dr. Stefano Capaccioli



Roma, 24 Maggio 2017

Chi sono

- Presidente **Assob.it** (Associazione di Categoria) che si occupa di promozione e difesa delle imprese impegnate nelle criptovalute, con attenzione ai diritti fondamentali digitali.
- **Dottore Commercialista e Revisore Legale** con studio in Arezzo, studioso della frontiera del diritto.
- **Culture della materia** in **Informatica Giuridica (IUS20)** – Prof. G. Ziccardi - Università Statale di Milano.
- **Autore** dell'**unica monografia giuridica sui bitcoin** (*Criptovalute e bitcoin: un'analisi giuridica*, Giuffrè, 2015) e di oltre 20 tra saggi scientifici e articoli su questo argomento.
- **Collaboratore** di *BitcoinMagazine*, *CoinTelegraph*,
- Founder di **Coinlex**.
- Ideatore della prima società italiana con **conferimento di bitcoin** (oraclize.it).

Bitcoin: domande ricorrenti.

- I bitcoin sono illegali?
- I bitcoin sono utilizzati per riciclare?
- I bitcoin sono un « Ponzi Scheme »?
- I bitcoin sono utilizzati esclusivamente dai criminali?

Poi l'ultima domanda

-ma cosa sono i bitcoin?

Cosa dicono del Bitcoin ;-)

La maggior parte delle notizie ed informazioni si basano su errate percezioni, bufale, leggende metropolitane e scarsa comprensione dello strumento.



Più leggende che realtà?

- Bitcoin & **Cryptolocker**

~ Primo ransomware (1998) si pagava (USD) a Ufficio Postale in Panama

- Bitcoin & **ISIS**

~ Giornalista Deutsche Welle si è scusato per la bufala (Europol esclude)

- Bitcoin & **Riciclaggio**

~ bitcoin non è efficace né utile per le attività di riciclaggio

- Bitcoin & **Evasione Fiscale**

~ seguono le normali regole

- Bitcoin & ...

~ Attendiamo la prossima bufala, del resto con il coltello del pane si può commettere un omicidio, ma nessuno lo demonizza. Tutti gli strumenti possono avere un utilizzo criminale, come la diavolina per il piromane.

Demonizzazione di strumento non conosciuto

Leggende

- L'**idea** che il **bitcoin sia funzionale al riciclaggio** è smentito dalle evidenze tecnico-economiche che determinano la sua **inadeguatezza** a servire quale **strumento di riciclaggio**, dato che "bitcoin non è efficace né utile per le attività di riciclaggio".
- Per completezza, secondo i **Quaderni dell'antiriciclaggio – Collana Dati statistici I-2016 dell'UIF**, in Italia (e solo nel primo semestre), sono stati versati (non usati, ma versati) oltre **94 MLD di euro in contanti**, mentre la capitalizzazione mondiale del bitcoin è di circa 30 miliardi di USD.

Tipologia transazione

- Il sistema delle criptovalute comporta un' innovazione nelle metodologie di transazione, con un paradigma ancora da comprendere.

UTENTI	TRANSAZIONE	Tipo
Ignoti	Ignota	Denaro Contante
Nota	Nota	Sistema Finanziario
Ignoti (?)	PUBBLICA	<i>bitcoin</i>

Unbanked e lotta al contante

- Definizione: cittadini europei con più di 15 anni di età che non dispongono di un conto corrente bancario o un conto di deposito.
- In **Italia**, questi **sono quasi 7,8 milioni** (il **13% degli italiani over 15**) (*popolazione totale da 15-18 sono 2,2 M e ultra 80 sono 3,8 M*).
 - Romania 7,8M (39%) e Polonia 8,3M (22%).
 - In Francia (3%) sono poco più di un 1,5M.
 - Germania (1%) e Regno Unito (1%) sono poco sotto Danimarca e Scandinavia (0%).

Fonte: **World Bank, April 2014**

Non esistono dati sugli **underbanked** (accesso solo in parte ai servizi finanziari)

Perché la criminalizzazione?

- L'associazione tra reati e *bitcoin* affonda nel tempo:
 - Alcuni casi giudiziari, quali **Liberty Reserve** e **Silk Road**
 - Difficoltà di comprendere uno strumento nuovo (ed oggettivamente difficile).
- Detta difficoltà porta, mentalmente, al **rifiuto** e alla **stigmatizzazione** dato che, non comprendendo come funziona, nessuno vuol sentirsi “incompetente”!
- La classificazione dello strumento come criminale permette alla nostra mente di trovare una comoda giustificazione per non analizzarlo, collocandolo tra le attività illegali o esclusivamente per attività criminali.

Filosofia – Status Quo

- La società moderna basa quindi le sue transazioni su due pilastri: **FIDUCIA** e **CENTRALIZZAZIONE**.
- Tutte le informazioni sono inserite in **REGISTRI CHIUSI** e **CENTRALIZZATI**, gestiti da **ENTI** in cui è riposta **FIDUCIA** (volontaria o obbligatoria).
 1. **DENARO** (Banche, IMEL, Istituti di Pagamento, Denaro Contante).
 2. **IDENTITÀ** (Reale: registri anagrafe, Digitale: Service Provider quale Facebook, Google, Yahoo).
 3. **DOMINI INTERNET** (ICANN).
- L'utilizzo di tali **REGISTRI CHIUSI** è soggetto a **AUTORIZZAZIONE**, con **PROBLEMI DI INTEROPERABILITÀ (verso terzi)** e **COSTOSO** e necessita di **FIDUCIA CONDIVISA SUL TENUTARIO**,

Origini: Wei Dai (1998), Szabo (2006)

- **Dove:** Mailing List di *Cryptoanarchici*.
(*Cryptoanarchy Manifesto*, Tim May 1988)
- **Obiettivo:** Realizzare un mondo TRUSTLESS
(che non si basi sulla fiducia di un terzo).
- **Finalità:** Creazione di sistema di pseudonimi che possano scambiarsi unità.
- Esercizio Intellettuale di mero studio per realizzare un sistema:
 - **LIBERAMENTE ACCESSIBILE**
 - **NON BASATO SULLA FIDUCIA**
 - **APERTO**
 - **POCO COSTOSO.**

Definizione comune di Criptovaluta

Rappresentazione Digitale di Valore decentralizzata basata sul peer-to-peer, su una *blockchain* condivisa il cui trasferimento è basato sulla crittografia e le cui regole di emissione sono basate su un Algoritmo Open Source.

Blockchain condivisa

Sistema distribuito di tenuta delle transazioni in forma **incrementale**, liberamente **accessibile** e basato sul consenso **decentralizzato**.

Un **libro giornale a blocchi** legati uno all'altro con un sistema di **hash**

L'hash di **un blocco** è il **primo elemento del blocco successivo** per legare tutta la catena in maniera indissolubile.

Bitcoin: problemi di inquadramento.

- Natura della criptovaluta che ha le seguenti caratteristiche:

- Virtuale
- Polimorfa
- Ibrida
- Pseudonima
- Ubiqua

***N.B.** Nel caso di Bitcoin: Bitcoin (B) protocollo e bitcoin (b) unità di conto. Ciò ingenera confusione in molti autori.*

- Mezzo di scambio, bene immateriale (?) che include una unità di valore.

- Proprietà:

- Destinazione alla circolazione in maniera tracciabile
- Pseudonominatività
- Unità di conto

Unità di conto

- L'unità di conto costituisce un grattacapo.
- È rivoluzione copernicana perché riesce a eliminare centralizzazione e fiducia.
- È ubiqua, polimorfa e virtuale, tale per cui la scelta di un paese comporta reazioni
- Non è controllabile.

Bitcoin: definizione giuridica.

I *bitcoin* possono essere considerati (a seconda del contesto senza definizione condivisa o condivisibile), anche se è **pacifico che la valuta virtuale «bitcoin» non abbia altre finalità oltre a quella di un mezzo di pagamento e che essa sia accettata a tal fine da alcuni operatori.** (Sentenza CGUE C-264/14).

- **Moneta**, in quanto rispondono alle definizioni classiche economiche.
- **Valuta estera**, in quanto non ha corso legale nel territorio.
- **Bene Immateriale**, dato che non esistono fisicamente.
- **Commodity**, in quanto bene fungibile prodotto da un'attività umana e riconosciuto da una determinata comunità quale valore.
- **Strumento Finanziario** (*Securities*), in quanto la propria valutazione dipende dalla domanda ed offerta ed è scambiato in un mercato.
- **Diritto di Baratto**, dato che possono essere barattate con beni e servizi espressi in quella data unità di conto.
- **Sistema di Pagamento**, dato che svolge quella funzione.
- **Obbligazione Naturale**, dato che sono accettati su base volontaria e non è possibile forzare un'esecuzione.

Italia: solo monete a corso legale?

Documento di legittimazione



Documento di legittimazione



Titolo di credito



Frammentazione

- Ogni paese/ordinamento giuridico ha le sue regole
- Le norme nascono per rispondere a determinate esigenze sociali e per determinate finalità
- L'algoritmo è REGOLAMENTATO dalle sue regole («Code is law»)
- Le soluzioni quindi VALGONO per quell'ordinamento (inteso come ambito territoriale/comunità) e per quella normativa (intesa sulle finalità della stessa) e **NON POSSONO ESSERE ESTESE AD ALTRO!**
- Diffidate quindi dalla risposta semplice a un domanda complessa, perché è SBAGLIATA! Su tutte HashFast v Lowe

HashFast v Lowe

HashFast Technologies LLC è fallita ed il curatore ha revocato il pagamento di 3.000 bitcoin, ma doveva essere:

1. *Restituito i bitcoin (oggi ~700 \$/BTC).*
2. *Restituito il valore dei bitcoin al momento della transazione (~120 \$/BTC).*
3. *Restituito il valore dei bitcoin data fallimento (~448 \$/BTC).*

Secondo la Bankruptcy Law, il bitcoin è moneta o no?

Tesi 1: Curatela. IRS (Internal Revenue Service) e della CFTC (Commodity Future and Trade Commission) considerano bitcoin come una **commodity** e quindi non una moneta.

Tesi 2: Dr Lowe. FinCEN, SEC e Sentenze US v. Faiella e US v. Ulbricht, considerano bitcoin come **moneta**.

Il Giudice Dennis Montali ha sentenziato che il bitcoin non può essere assimilato a valuta a corso legale e quindi non è moneta per la Bankruptcy Law dello Stato della California.

Miti da sfatare / Potenzialità

- **Non è anonimo** (riservatezza senza anonimato o pseudonimo)
- È tracciabile ~ investigazioni come qualsiasi reato informatico
- Transazioni sono **IMMUTABILI, LIBERAMENTE ACCESSIBILI** e **ETERNE**
- Possibilità di **creazione protocolli** (*multisig, smart contracts*) che agevolano le transazioni
- Possibilità di **completare la transazione on line** in maniera totalmente decentralizzata.

Grazie per l'attenzione

Stefano Capaccioli

Dottore Commercialista

Revisore Legale

Via de' Cenci 15 - 52100 Arezzo (AR)

Mail s@capaccioli.net

Twitter: @s_capaccioli

Website: www.capaccioli.net / www.assob.it / www.coinlex.it

Blog: coinlex.wordpress.com (bitcoin)

Blog: www.aurumlex.it (metalli preziosi)