



BITCOIN

tra

Legge e mercato

Lodi, 6 marzo 2018

## Introduzione

Problema 1

Problema 2

Bitcoin (cenni)

Conclusione

- **Bitcoin** è di fatto una soluzione **tecnica** e **strategica** a **due problemi**. Questi due problemi *non* sono tecnici ma **politici** ed **economici**
- Sono problemi **generali** ma bitcoin li risolve nel settore **particolare** del **denaro**:
  1. problema di **libertà**: violazione sistematica del principio di non aggressione (PNA). P. es. della libertà di scelta nel settore del denaro
  2. problema **economico**: le conseguenze della violazione sistematica, da parte dello stato (& Co.), delle leggi economiche
- Nell'informazione *mainstream*, questi due problemi vengono **accuratamente evitati**
- Capire questi due problemi aiuta a filtrare le **baggianate** che si sentono su bitcoin

## Introduzione

Problema 1

Problema 2

Bitcoin (cenni)

Conclusione

- Lo scopo di questo intervento è:
  - a. **ricordare** brevemente **questi due problemi**
  - b. in chiusura, dare un'idea **estremamente rapida e superficiale**, da **non esperto**, di:
    - **cos'è bitcoin**
    - **come funziona**
    - **in che modo risolve**, nel settore particolare del denaro, i due problemi di cui sopra

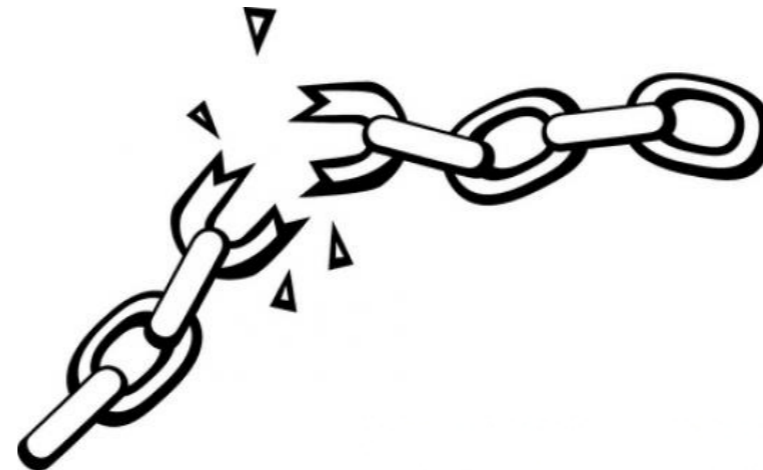
Introduzione

**Problema 1**

Problema 2

Bitcoin (cenni)

Conclusione



Introduzione

**Problema 1**

Problema 2

Bitcoin (cenni)

Conclusione

- Il **primo problema** non consiste tanto nel fatto che lo stato violi il PNA (p. es. la libertà di scelta), quanto nel fatto che lo **possa fare legalmente**
- In altre parole, il problema è la **violazione legale della Legge**. Paradossoso?
- No: **inversione del concetto di legge**
  - da: **limite non arbitrario** a **ogni** potere coercitivo (**Legge**): principio (regola **generale** di **comportamento individuale**) esiste **indipendentemente** dalla volontà di chiunque
  - a: **strumento** di potere coercitivo arbitrario di alcuni su altri ('legge' **fiat** o **positiva**): provvedimento **particolare** che esiste in quanto **decisione** di un'autorità

Introduzione

**Problema 1**

Problema 2

Bitcoin (cenni)

Conclusione

- Legge e 'legge' fiat sono due **strutture di pensiero**:  
(→ differenze fra partiti o fra sistemi di governo sono irrilevanti)
- **alternative**
- che **non hanno pari dignità**:
  - una trova il **limite alla coercizione** di alcuni su altri nella **coerenza logica** e nell'**assenza di privilegio**,
  - l'altra nell'**arbitrarietà** e nel **privilegio**
- cioè: una è **scientifica** e l'altra no
- p. es. una è compatibile con l'idea di **uguaglianza davanti alla legge**, l'altra no

Introduzione

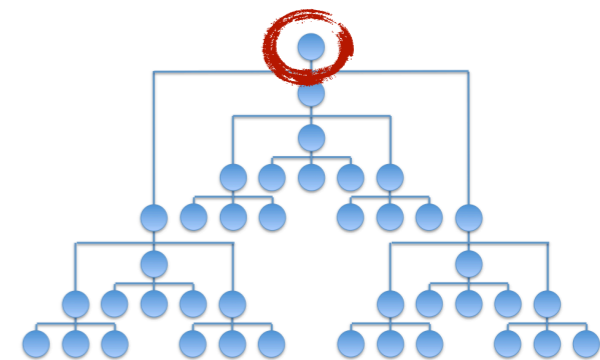
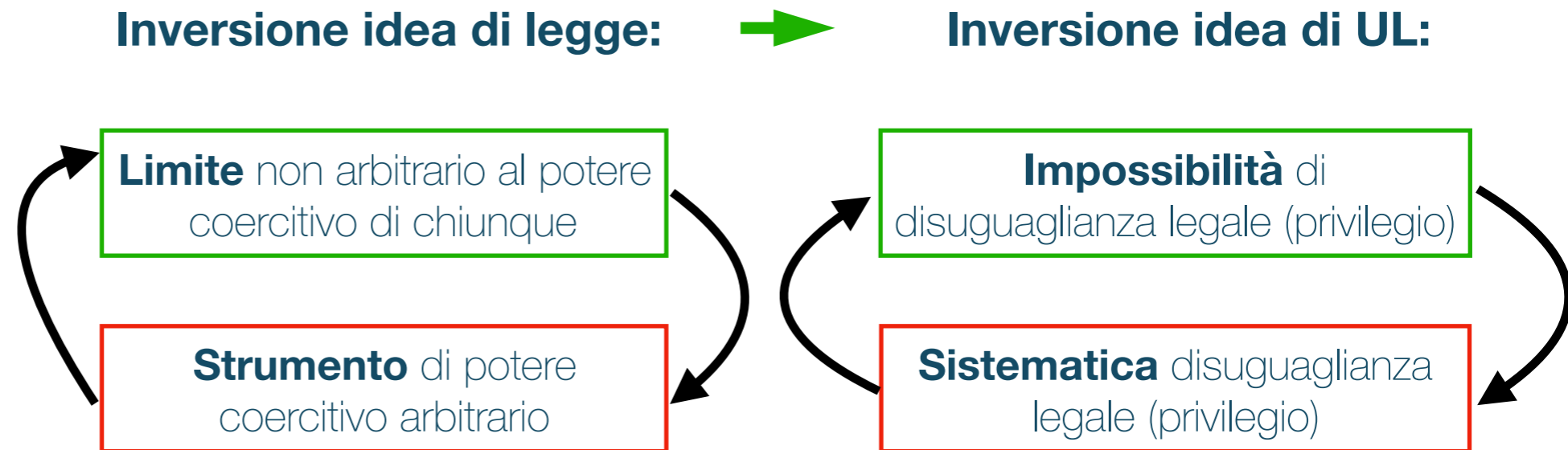
**Problema 1**

Problema 2

Bitcoin (cenni)

Conclusione

- All'inversione dell'idea di legge si accompagna infatti l'inversione dell'idea di **uguaglianza davanti alla legge (UL)**:



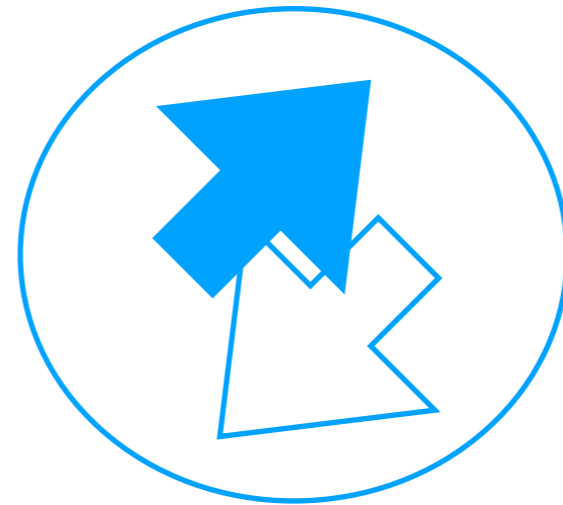
Introduzione

Problema 1

**Problema 2**

Bitcoin (cenni)

Conclusione





Introduzione

Problema 1

**Problema 2**

Bitcoin (cenni)

Conclusione

- Problema economico è costituito da:
  - A. le **crisi economiche cicliche**, es. 2008
  - B. le **misure** che le autorità monetarie e politiche impongono **per 'risolvere'** queste crisi
- Bitcoin **non** risolve questo problema cercando di impedire A e B, ma offrendo alle persone una **via di uscita individuale** (e **non censurabile**) ad almeno parte delle conseguenze di questi problemi, e perfino un modo per trasformarle in **opportunità**



Introduzione

Problema 1

**Problema 2**

Bitcoin (cenni)

Conclusione

- **Premessa**, esistono **due soli** tipi possibili di **ordine economico** (e sono **incompatibili** fra loro):

### ordine spontaneo

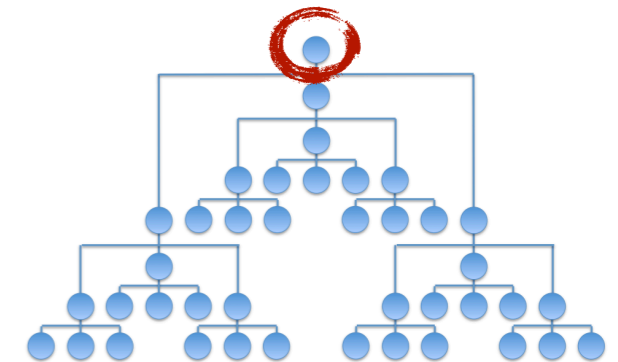
- **non c'è gerarchia unitaria di fini**: le singole persone agiscono in funzione dei loro **fini individuali**
- agiscono sulla base di una **conoscenza dispersa** (p. es. delle loro preferenze, situazione, ecc.) che possiedono **solo loro** e che **non è disponibile** ad autorità centrali



- Se la **conoscenza rilevante è dispersa** capillarmente, **può prosperare**.

### ordine positivo

- **c'è gerarchia unitaria di fini**: le persone agiscono (in misura variabile) in funzione dei fini **imposti arbitrariamente** da chi controlla l'ordine positivo
- agiscono sulla base della **conoscenza centralizzata** di quest'ultimo



- Se la **conoscenza rilevante è dispersa** capillarmente, **deve necessariamente fallire** **crisi ec.**

Introduzione

Problema 1

**Problema 2**

Bitcoin (cenni)

Conclusione

- Bitcoin nasce in risposta all'ultima crisi ciclica (2008). **Il punto di partenza** per capire le **crisi cicliche** è il **tasso d'interesse ( $i$ )**:

$i$  di mercato ( $iM$ )



componente **primaria**

**Pref. fra tempo futuro (risparmio R) e tempo presente (consumo C):**

> R  $\rightarrow$  > risorse disponibili per gli investimenti (RDI)  $\rightarrow$  < il loro prezzo ( $i$  = 'prezzo del tempo')

E viceversa.

$\rightarrow iM =$

$i$  arbitrario ( $iA$ )



$i$  = **decisione** banche centrali

$\rightarrow iA =$

Introduzione

Problema 1

**Problema 2**

Bitcoin (cenni)

Conclusione

Prezzi **di mercato** = “**bussola**”  
del processo economico



- Quindi anche il **tasso d'interesse ( $i$ )**: il prezzo delle RDI (o 'prezzo del tempo')
- La funzione di  $iM$  è quella di **coordinare risparmi e investimenti nel tempo** (rilevanza **systemica**)
- Questo coordinamento **richiede una conoscenza** (quella delle preferenze temporali delle singole persone in ogni momento) che è **dispersa capillarmente** fra le persone e che non è conoscibile da alcun “manager del sistema monetario” i.e. banchiere centrale

$$(iM = \text{[Network Diagram]} )$$

Introduzione

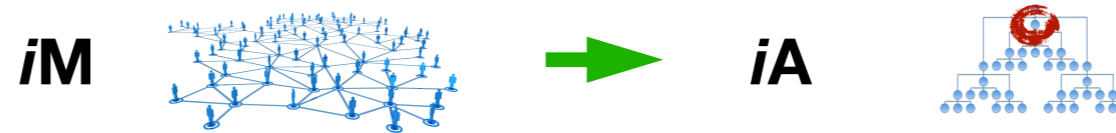
Problema 1

**Problema 2**

Bitcoin (cenni)

Conclusione

- **Inflazione monetaria** sistema bancario:



- Avviene per **tre vie**:

- **banche commerciali** (BC):

- ❖ riserva frazionaria (RF): dep **1k**, CRO=1% > "thin air" (TA) **99k**

- **banca centrale** (banca delle banche):

- ❖ riduz. coeff. di ris. obb.ria (CRO) dep **1k**, CRO=0,5% > TA **199k**

- ❖ aumento riserve totali delle BC (amplif. RF)

- \* prestiti a BC ris. in. **1k**, CRO 1%, CRBC 10% > TA **990k**

- \* riduz. tasso d'int. su prestiti a BC **idem** (TUS < i BC a clienti)

- \* operazioni di mercato aperto (es. "QE") TA **illimitato**

- **stato**:

- ❖ divieto uso del contante (amplif. RF)

Introduzione

Problema 1

**Problema 2**

Bitcoin (cenni)

Conclusione

- Alcune **conseguenze inflazione monetaria**:
  - a. **diminuzione potere di acquisto del denaro di stato**
  - b. **trasferimento risorse dai creditori ai debitori** (quindi **allo stato**: il debitore maggiore)
  - c. trasferimento di risorse da chi riceve il nuovo denaro **prima** (es. banche commerciali) a chi lo riceve **dopo**
  - d. **soprattutto, crisi economiche cicliche** (es. 2008)

Introduzione

Problema 1

**Problema 2**

Bitcoin (cenni)

Conclusione

- Alcune **conseguenze inflazione monetaria**:
  - a. **diminuzione potere di acquisto del denaro di stato**
  - b. **trasferimento risorse dai creditori ai debitori** (quindi **allo stato**: il debitore maggiore)
  - c. trasferimento di risorse da chi riceve il nuovo denaro **prima** (es. banche commerciali) a chi lo riceve **dopo**
  - d. **soprattutto, crisi economiche cicliche** (es. 2008)

Introduzione

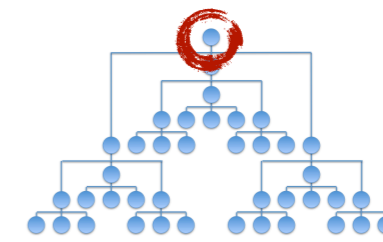
Problema 1

**Problema 2**

Bitcoin (cenni)

Conclusione

- Bitcoin nasce nel 2009 a seguito (e anche in risposta) alla **crisi economica del 2008**, che è stata **solo l'ultima** delle crisi cicliche prodotte dall'inflazione monetaria
- In estrema **sintesi** e **intuitivamente\***, queste crisi cicliche sono prodotte dalla seguente **dinamica**:
  - a. ***i* artificialmente basso** ( $iA$ ) indica la presenza di **molte** RDI
  - b.  incoraggia **investimenti ambiziosi** a lungo termine: distorce la **struttura produttiva** ("**malinvestments**"): salta coord.to R e I nel tempo
  - c. inizialmente  $iA$  produce **fase espansiva**
  - d. tuttavia, l'informazione data da  $iA$  è **sbagliata**: le risorse disponibili per completare quei progetti ambiziosi **non ci sono** ( $iM > iA$ ). Nuova struttura produttiva **non sostenibile**.
  - e. quando questo fatto diventa **evidente** si ha una fase di **crisi** economica





Introduzione

Problema 1

**Problema 2**

Bitcoin (cenni)

Conclusione

\*Biblio:

- Mises L., 1998 [1949], *Human Action*
- Rothbard M.N., 2004 [1962], *Man, Economy and State*
- Hayek F.A., 1967[1931], *Prices and Production*
- De Soto J.H., 2006, *Money, Bank Credit and Economic Cycles*
  
- Murphy R.P., 2010, *Lessons for the Young Economist*
- Murphy R.P., 2008, *Study Guide to Human Action*
- Carbone F. De Soto J.H., 2012, *A scuola di economia*
- Hazlitt H., 2008 [1946], *Economics in One Lesson*

Mie sintesi teoria ciclo economico:

- *Indipendenza, denaro e credito*
- *Crescita strutturale e ripresa ciclica*
- *Law, Money, Banking and the Business Cycle*

Introduzione

Problema 1

**Problema 2**

Bitcoin (cenni)

Conclusione

- La crisi ciclica viene di solito curata con le **stesse misure** che la hanno prodotta:

*“Combattere la depressione economica attraverso l’espansione forzata del credito vuol dire curare il male attraverso le **stesse misure** che lo hanno prodotto; dato che il problema è causato dalla distorsione della struttura produttiva noi vogliamo creare ancora maggiore distorsione” (F.A. Hayek)*

*“Se elencassimo logicamente i vari modi nei quali lo stato può **impedire il processo di aggiustamento di mercato**, troveremmo che abbiamo elencato **esattamente** l’arsenale di politiche economiche ‘anti-depressive’ dei governi:*

- |   |  |
|---|--|
| 1) <i>Impedire o ritardare i fallimenti*</i>              | [es. “Too Big to Fail”, ... n.d.r.]          |
| 2) <i>Inflazionare ulteriormente la moneta</i>            | [es. “QE”, ... n.d.r.]                       |
| 3) <i>Mantenere alti i salari</i>                         | [es. “salario minimo”,... n.d.r.]            |
| 4) <i>Mantenere alti i prezzi</i>                         | [es. ob.vo BCE, protez.mo, ... n.d.r.]       |
| 5) <i>Stimolare il consumo e scoraggiare il risparmio</i> | [es. “bonus cultura”, ... n.d.r.]            |
| 6) <i>Sussidiare la disoccupazione</i>                    | [es. “reddito citt.za, dignità”, ... n.d.r.] |
| 7) [Ulteriore spesa ‘pubblica’                            | es. “Inv.ti pubblici”, “pubbl. impiego” ...  |
| 8) Impedire i licenziamenti                               | es. art. 18, ...                             |
| 9) ... n.d.r.]”   |  |
- (M.N. Rothbard)

(\*) Nel caso dei fallimenti bancari, ora c’è il “bail in” ma...

Introduzione

Problema 1

Problema 2

**Bitcoin (cenni)**

Conclusione



Introduzione

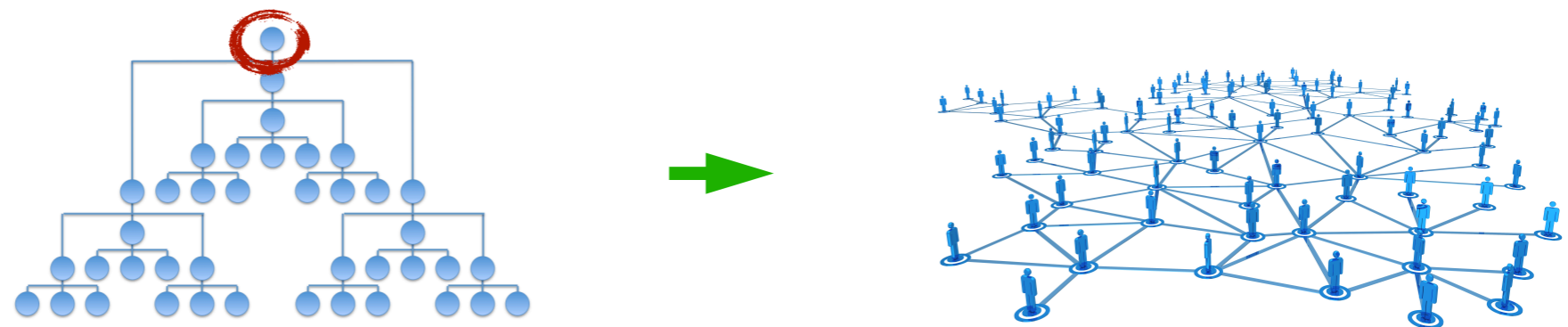
Problema 1

Problema 2

**Bitcoin (cenni)**

Conclusione

- Abbiamo visto che la sistematica violazione, da parte dello stato, della libertà (**Problema 1**) e delle leggi economiche (**Problema 2**) producono **ulteriori** violazioni della libertà e crisi economiche cicliche: **circolo vizioso**
- Abbiamo anche visto che la natura dei due problemi è **strutturale**: i due problemi possono essere risolti solo modificando la **struttura** del sistema politico (**idea di legge**) ed economico (**interventismo**, specie monetario)



Introduzione

Problema 1

Problema 2

**Bitcoin (cenni)**

Conclusione

- Questa **struttura** tuttavia **non può** essere modificata:
  - **né attraverso la politica** (la politica - lo stato - è il problema, non la soluzione)
  - **né attraverso l'esperienza storica** (se le atroci esperienze storiche del nazismo e del comunismo non sono bastate a far capire alle persone che quella **struttura** andava cambiata, quale esperienza può riuscire a farlo?)
  - **né**, almeno nel "futuro prevedibile", **attraverso la diffusione della cultura** (modificare la struttura di pensiero che si è imparato a dare per scontata fin dalla nascita è molto difficile: è ragionevole pensare che solo una minoranza possa/voglia farlo - anche se Internet...)
  - Situazione **senza speranza**

Introduzione

Problema 1

Problema 2

**Bitcoin (cenni)**

Conclusione

## Ma poi...

- Qualcuno ha capito che **non serviva** modificare o sostituire la struttura, ma bastava **forkarla**
- *“Non cambierai mai le cose **combattendo la realtà esistente**. Per cambiare qualcosa, costruisci un modello nuovo che renda la realtà esistente **obsoleta**” (B. Fuller)*

Introduzione

Problema 1

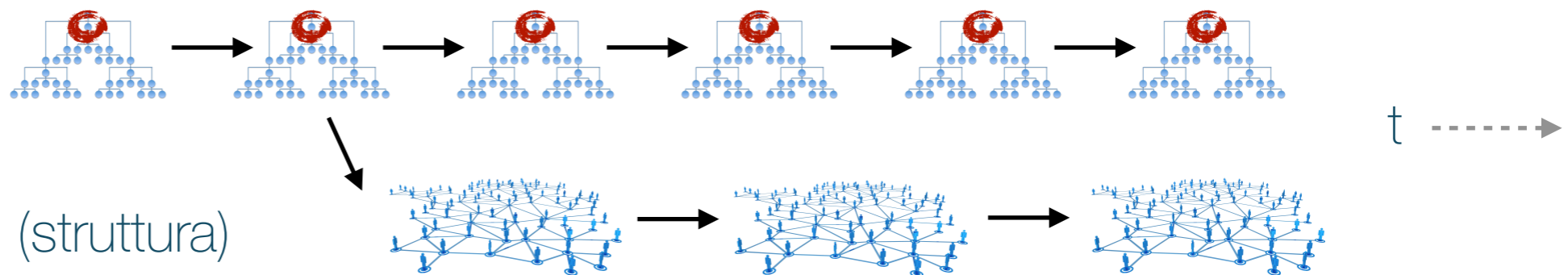
Problema 2

**Bitcoin (cenni)**

Conclusione



dal film "Interstellar", 2014 - video [qui](#) ([link](#))



- Esperimento bitcoin: **forkare il sistema monetario**

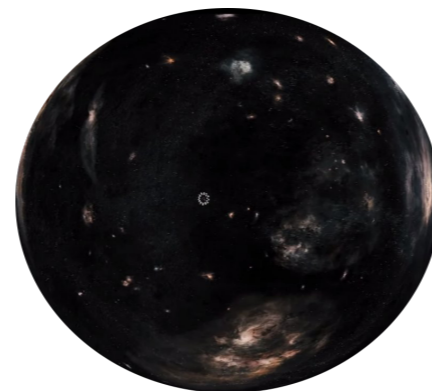
Introduzione

Problema 1

Problema 2

**Bitcoin (cenni)**

Conclusione

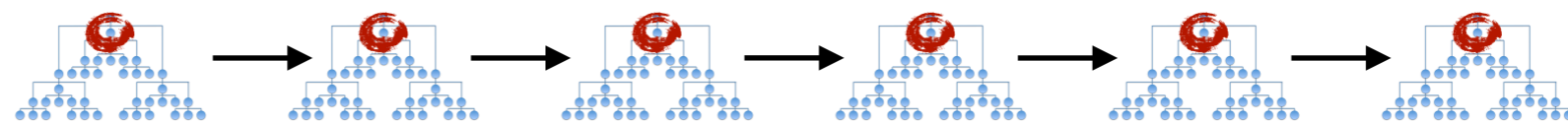


(metafora)

=



(wormhole in Interstellar)



t ----->

(struttura)



- Esperimento bitcoin: **forkare il sistema monetario**



Introduzione

Problema 1

Problema 2

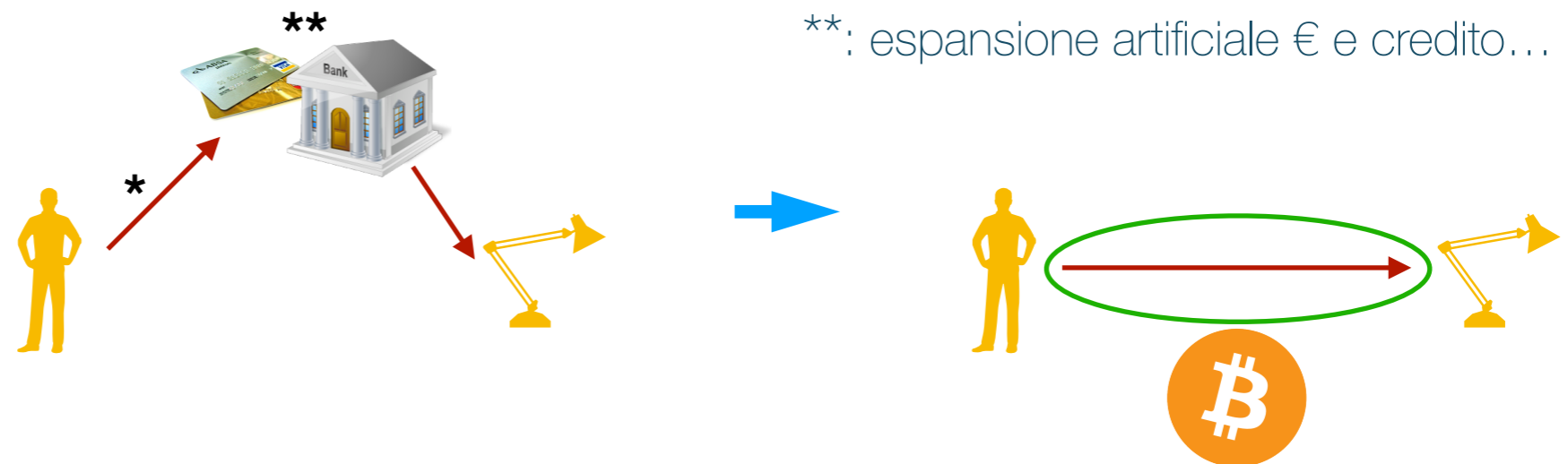
**Bitcoin (cenni)****3.1 Cos'è**

3.2 Come funziona

3.3 Problemi 1 e 2

Conclusione

- Il sistema **bitcoin-blockchain** ("bitcoin") è un sistema di **certificazione decentralizzato** e **non censurabile** (**blockchain**) che funziona grazie a una **struttura di incentivi economici di mercato** costituita da un asset scarso e **non inflazionabile** (**bitcoin**)
- In altri termini, questo sistema è **non solo una moneta** di mercato non inflazionabile (bitcoin) **ma anche un sistema di pagamento** decentralizzato (*peer to peer*) e non censurabile (blockchain)



- Bitcoin = **Internet (del denaro) + non cens.tà + privacy**

Introduzione

Problema 1

Problema 2

## Bitcoin (cenni)

3.1 Cos'è

### 3.2 Come funziona

3.3 Problemi 1 e 2

Conclusione

- La **blockchain** è un **registro** completo di **transazioni in bitcoin**
- Si chiama “blockchain” (“catena di blocchi”) perché le transazioni vi vengono registrate in **“blocchi” consecutivi** (ogni “blocco” è come una pagina del registro)
- Questo registro non è centralizzato. Al contrario, è **decentralizzato: distribuito** fra molti “nodi” in giro per il mondo
- **Chiunque**, scaricando l'apposito software, può essere uno di questi nodi
- In questo registro sono annotati i **trasferimenti di proprietà** di alcuni “numeri”: i **bitcoin** (l'**analogia** fra i “numeri” e i bitcoin è tratta da “Understanding Bitcoin” di Barta S. e Murphy R.P., 12/17 - [understandingbitcoin.us](http://understandingbitcoin.us))

Introduzione

Problema 1

Problema 2

## Bitcoin (cenni)

3.1 Cos'è

**3.2 Come funziona**

3.3 Problemi 1 e 2

Conclusione

- La **proprietà di questi “numeri”** è **determinata univocamente: non** attraverso documenti di identità, ma attraverso **tecniche crittografiche**
- In altri termini: questi “numeri” sono **scarsi e proprietà privata** di qualcuno
- L'**innovazione rivoluzionaria** della blockchain sta nel fatto che **“garantisce”** che le informazioni contenute nei vari registri siano **le stesse** ovunque (impedisce il **“double spending”** dei bitcoin)
- Questo risultato, che sarebbe banale ottenere attraverso **copie** di un registro centralizzato, è **“meccanicamente” impossibile** da ottenere in un registro **distribuito**
- La blockchain ottiene questo risultato non “meccanicamente” ma attraverso una **struttura di incentivi** (cioè attraverso un **processo di mercato**)

Introduzione

Problema 1

Problema 2

## Bitcoin (cenni)

3.1 Cos'è

### 3.2 Come funziona

3.3 Problemi 1 e 2

Conclusione

- **Tutti** coloro che aggiornano per primi una copia del registro (i “contabili” o “**minatori**”) hanno un incentivo **economico** a che **tutti gli altri** abbiano sul **loro** registro le **stesse** informazioni, e viceversa
- Questo **incentivo economico** è dato dal fatto che, per il loro lavoro di **registrazione e verifica**, i contabili ottengono in cambio dei “numeri” scarsi (cioè dei **bitcoin**) di cui quindi diventano proprietari. In questo modo i bitcoin “entrano in circolo” (virgolette perché **il denaro non circola** ma si trova sempre nei conti di liquidità di qualcuno).
- Questa ricompensa in bitcoin per blocco registrato e verificato (*block reward*) **si dimezza ogni 210.000 blocchi minati** (cioè ogni circa quattro anni): era 50 BTC nel gennaio del 2009; è diventato 25 BTC nel novembre 2012; dal luglio 2016 è di 12,5 BTC e nel marzo 2020 sarà di 6,25 BTC)

Introduzione

Problema 1

Problema 2

## Bitcoin (cenni)

3.1 Cos'è

### 3.2 Come funziona

3.3 Problemi 1 e 2

Conclusione

- **Da chi** i minatori ottengono questo compenso in bitcoin? **Non** da una società con nome, indirizzo, p. IVA e nr. di telefono, ma da un **protocollo software open-source**, costantemente aggiornato da una comunità di **sviluppatori** e **non arbitrariamente modificabile**, neanche da chi lo ha inventato
- I bitcoin che il protocollo mette a disposizione sono **21 milioni**, non un centesimo di più. Ogni bitcoin è **divisibile** fino all'ottava cifra decimale
- Per ottenere ("**estrarre**") questi bitcoin, quindi per verificare la proprietà dei bitcoin e che le informazioni sui registri siano le stesse ovunque, i "contabili" ("minatori") devono risolvere complicati **problemi di calcolo** usando dei computers
- La **difficoltà** di questi problemi di calcolo **aumenta all'aumentare della potenza di calcolo** (e diminuisce al diminuire di questa)

Introduzione

Problema 1

Problema 2

## Bitcoin (cenni)

3.1 Cos'è

**3.2 Come funziona**

3.3 Problemi 1 e 2

Conclusione

- Questo serve a fare in modo che, in condizioni normali, il **tempo di registrazione di ogni blocco** (“pagina” del registro) sia di circa **10 minuti** (l'ultimo bitcoin sarà “estratto” nel 2140; il 99% dei bitcoin sarà minato entro il 2030: oggi siamo a circa l'80%)
- Questo è un fatto importante che **distingue economicamente bitcoin dall'oro**: all'aumentare della domanda di oro, ne aumenta il prezzo. L'aumento di prezzo dell'oro produce un aumento degli investimenti in **nuove tecnologie** che rendono estrazione dell'oro **più “facile”**, e quindi producono un **aumento dell'offerta** di oro sul mercato (quindi una spinta del prezzo al ribasso).
- Nel caso di bitcoin, **al contrario**, la **difficoltà** di estrazione **aumenta** con l'aumentare della potenza di calcolo (e quindi della domanda): **l'offerta di bitcoin** quindi **non sale** all'aumentare della domanda (**sale il prezzo**) e il suo andamento nel tempo è (molto) **più prevedibile** di quello dell'offerta dell'oro

Introduzione

Problema 1

Problema 2

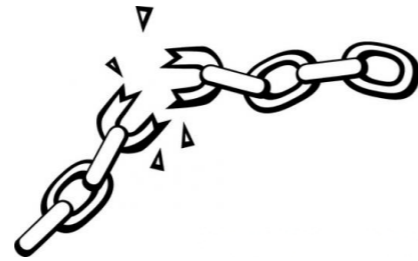
## Bitcoin (cenni)

2.1 Cos'è

3.2 Come funziona

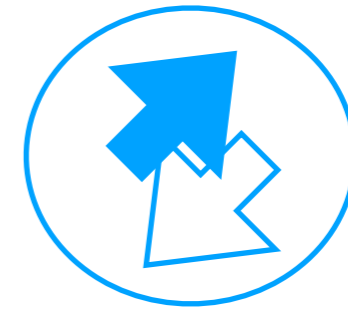
### 3.3 Problemi 1 e 2

Conclusione



Problema 1

- Libertà di scelta
- Più in generale, difesa PNA nei settori attinenti al denaro
- Uguaglianza davanti alla Legge
- Proprietà del denaro
- (Discreta) privacy



Problema 2

- Libero mercato nel settore del denaro
- Uso di conoscenza dispersa
- No inflazione monetaria
- No perdita potere d'acquisto del denaro fiat
- Via d'uscita individuale da crisi cicliche
- Via di uscita individuale dalle 'cure' delle crisi cicliche da parte di governi e banche centrali

Introduzione

Problema 1

Problema 2

## Bitcoin (cenni)

2.1 Cos'è

3.2 Come funziona

### 3.3 Problemi 1 e 2

Conclusione

*Food for thought:* ha senso sostenere che

- i governi **possono** vietare e impedire bitcoin?
- bitcoin **dovrebbe** essere vietato in quanto renderebbe la vita più facile al **crimine** o al **riciclaggio** di denaro?
- bitcoin dovrebbe essere vietato in quanto è una **“bolla”**?
- bitcoin dovrebbe essere vietato in quanto è un **fattore di instabilità monetaria**?
- bitcoin è una cattiva moneta perché è **“deflazionistica”**?
- l'aumento di prezzo di bitcoin **scoraggia gli investimenti produttivi**?
- l'aumento di prezzo di bitcoin incoraggia l'**hoarding** (il denaro “sotto il materasso”) e che questo sarebbe un problema per l'economia?
- bitcoin, a causa dell'energia che richiede, **danneggia l'ambiente**?

Risposta breve: **no**

- **Bitcoin è denaro?** Opin. diverse, ma in fondo chisseneimporta



Introduzione

Problema 1

Problema 2

Bitcoin (cenni)

**Conclusione**

not without a fight

(and this time the good guys could win)

