



Avv. Paolo Lessio
studioclass

Commissione Intelligenza Artificiale e
Processo Telematico Ordine degli Avvocati di
Milano

Avv. Giovanni Rocchi

Componente FIIF del Consiglio Nazionale
Forense



2008

12, 13, 14 settembre

LEHMAN
BROTHERS

2008
12, 13, 14 settembre

BANKRUPTCY

2008

1 novembre



Una versione decentralizzata e puramente elettronica della moneta consentirebbe di inviare i pagamenti on-line da una parte ad un'altra senza passare attraverso le istituzioni finanziarie.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.

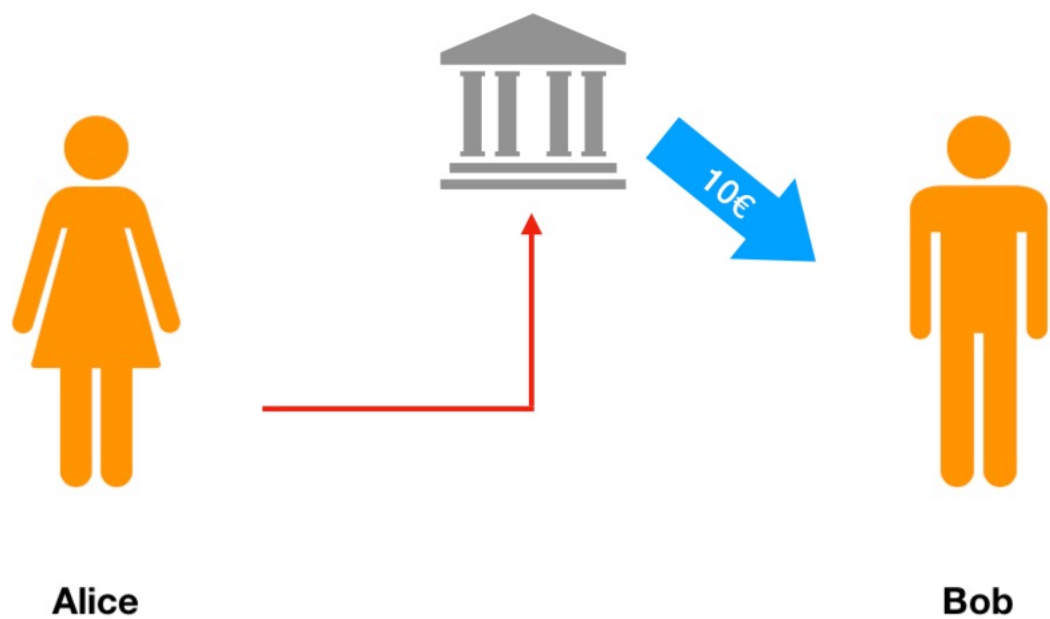
2008
1 novembre



Le principali proprietà:

- ❖ La doppia spesa è prevenuta con una rete decentralizzata
- ❖ Non serve una zecca o altri terzi garanti
- ❖ I partecipanti possono essere anonimi
- ❖ La nuova moneta viene generata da un algoritmo proof-of-work
- ❖ La proof-of-work alimenta la rete che previene la doppia spesa

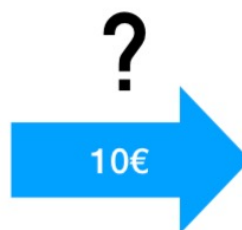
TRANSAZIONE



TRANSAZIONE



Alice



Bob

TRANSAZIONE



Alice



Bob



TRANSAZIONE



~~Alice~~

1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa



~~Bob~~

3M4fso45ujGu38u09Jge34Wn9i10jKa



TRANSAZIONE



Alice



Bob

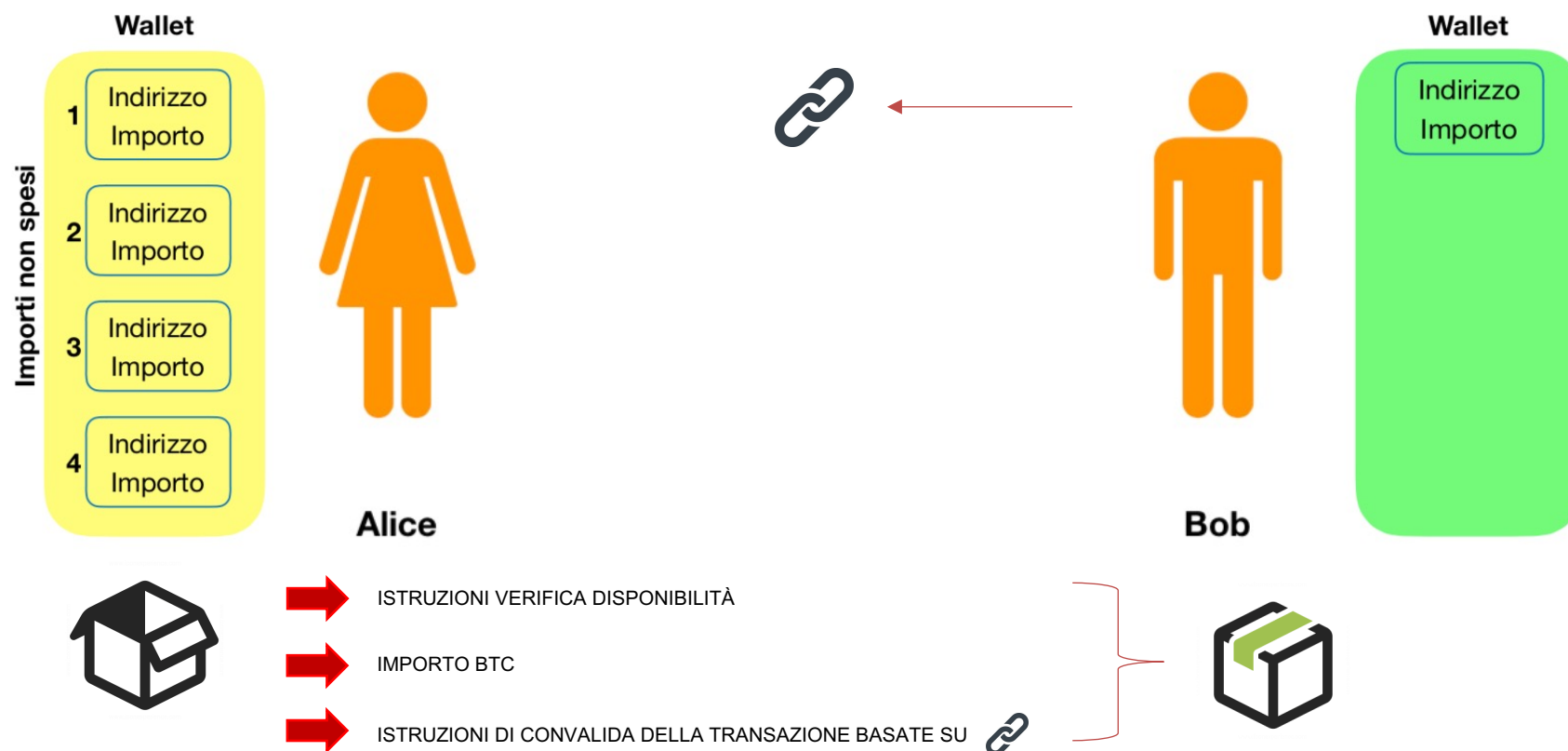
TRANSAZIONE



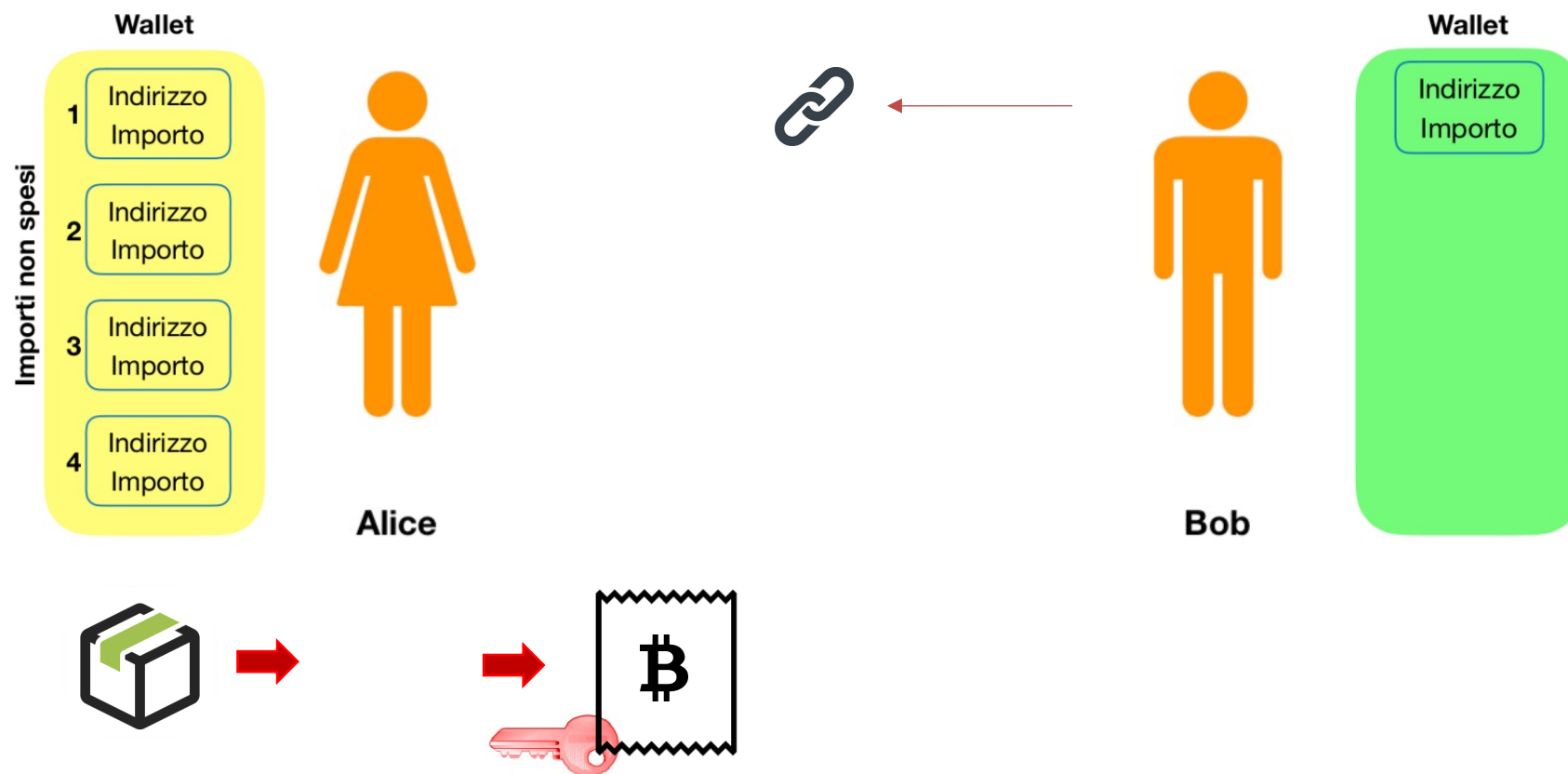
TRANSAZIONE



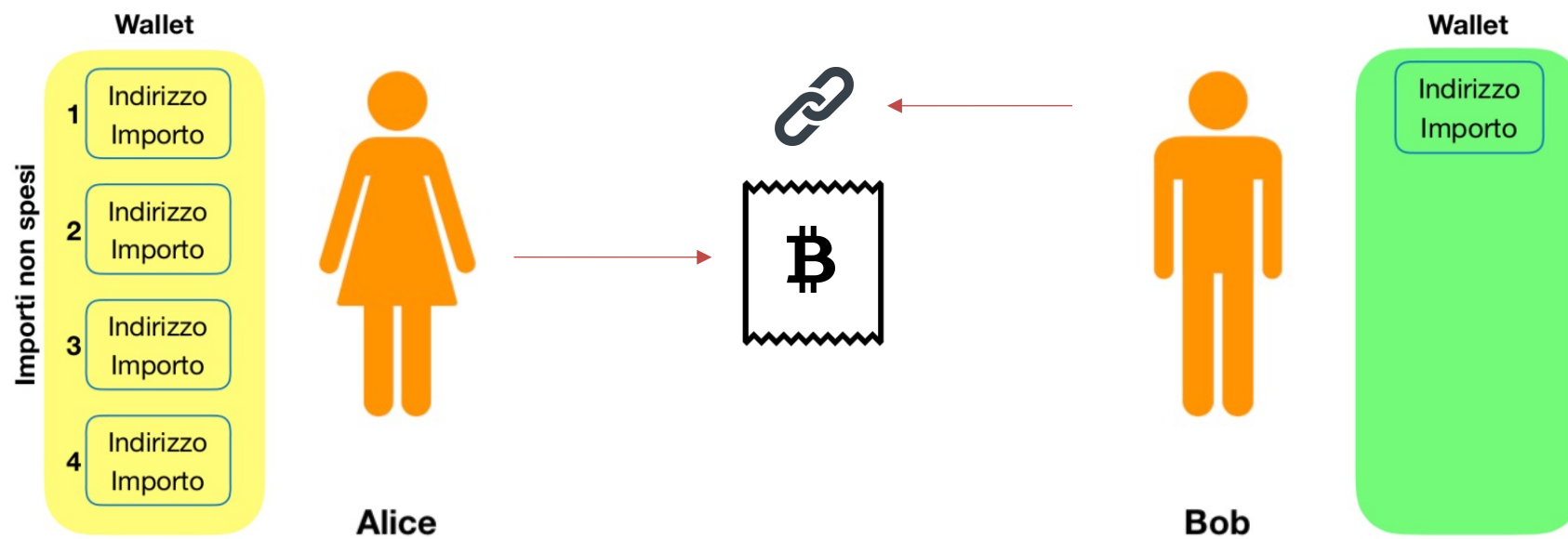
TRANSAZIONE



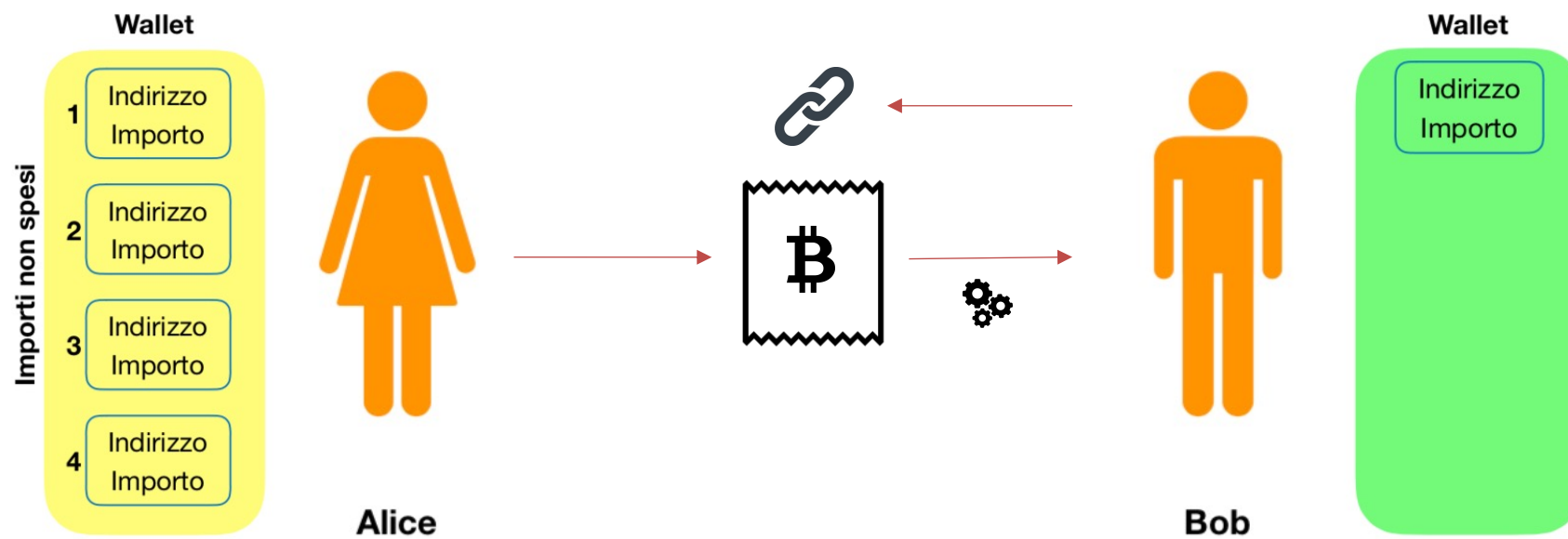
TRANSAZIONE



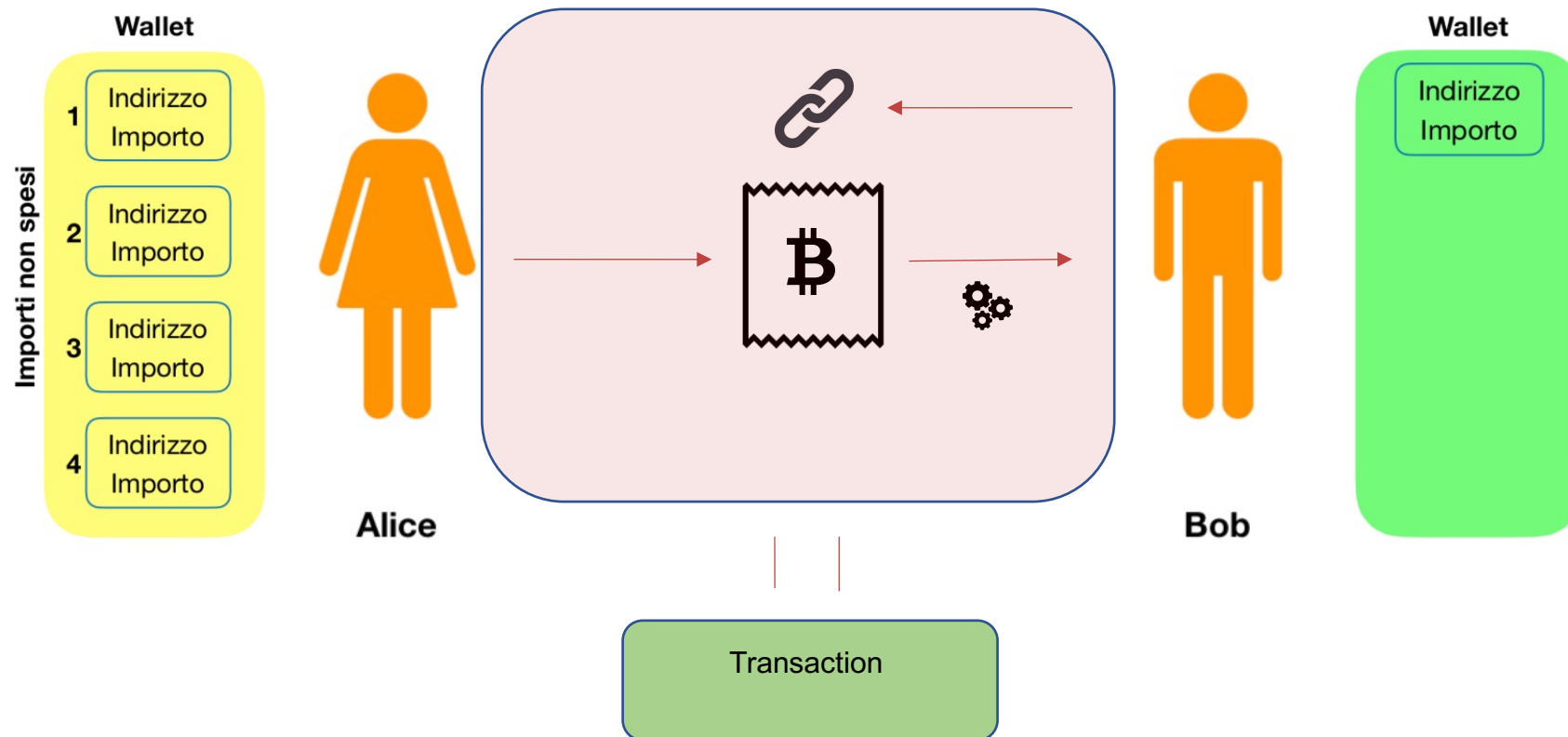
TRANSAZIONE

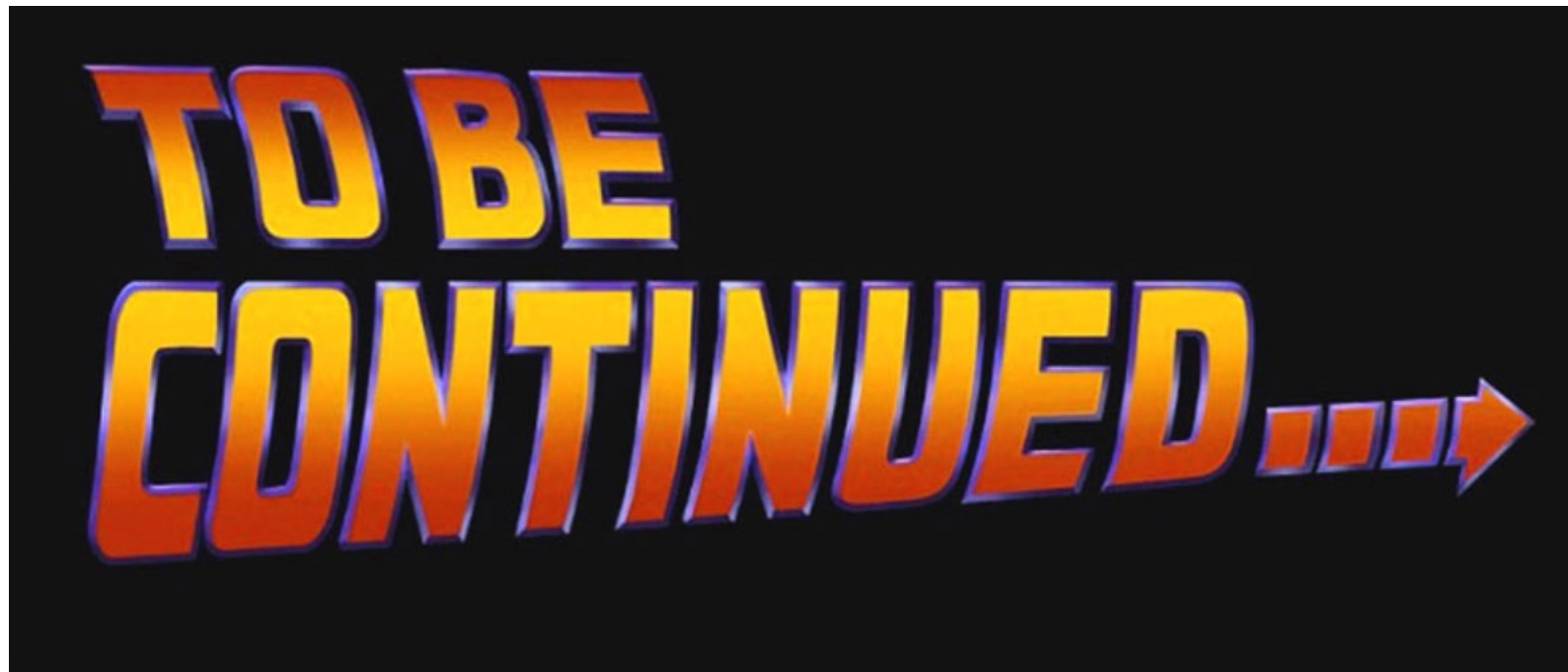


TRANSAZIONE



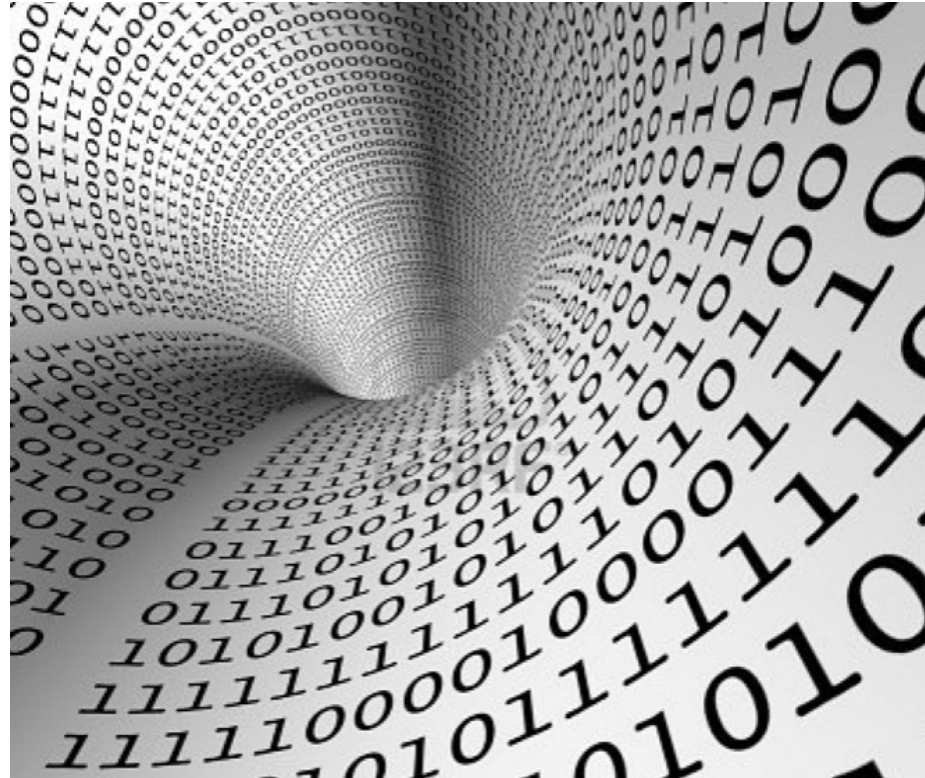
TRANSAZIONE





Il Documento Informatico

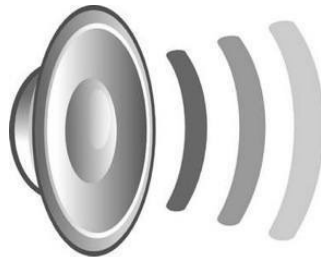
IRTI	CARNELUTTI
<i>res signata</i> , non volatile, dotata di durevolezza tale da poter essere letta a distanza di tempo	la ricorrenza dell'elemento materiale costituisce la principale differenza tra documento e testimonianza



eIDAS	CAD
«documento elettronico», qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva;	documento informatico: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

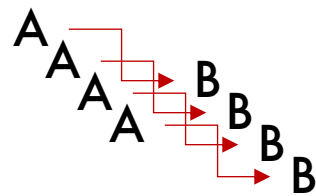
che cos'è il documento informatico???

Il Documento informatico



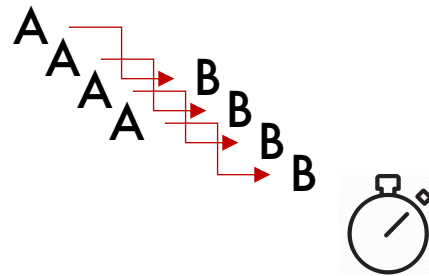
A → B





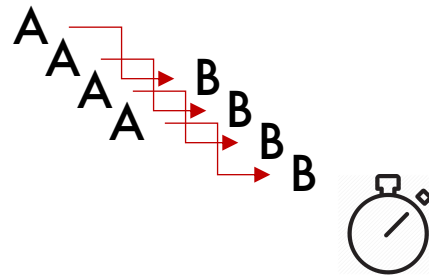
HASH N-1

NONCE (?)



HASH N-1

NONCE (?)



Il presente regolamento dovrebbe stabilire il principio secondo cui a un documento elettronico non dovrebbero essere negati gli effetti giuridici per il motivo nella sua forma elettronica al fine di assicurare che una transazione elettronica non possa essere respinta per il solo motivo che un documento è in forma elettronica.



Si ma a cosa serve?!?

Art. 8-ter.

(Tecnologie basate su registri distribuiti e smart contract)

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.

Art. 8-ter.

(Tecnologie basate su registri distribuiti e smart contract)

Si definiscono « tecnologie basate su registri distribuiti » le tecnologie che usano un registro distribuito

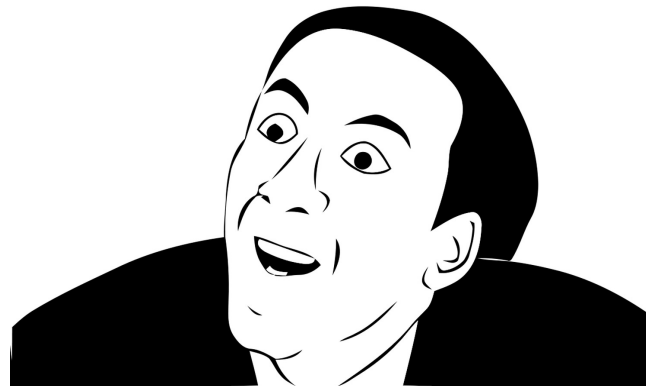
Art. 8-ter.

(Tecnologie basate su registri distribuiti e smart contract)

Si definiscono « tecnologie basate su registri distribuiti » le tecnologie
registro distribuito

che usano un

YOU DON'T SAY?



Art. 8-ter.

(Tecnologie basate su registri distribuiti e smart contract)

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.

Art. 8-ter.

(Tecnologie basate su registri distribuiti e smart contract)

Si definiscono « tecnologie basate su registri distribuiti » le tecnologie e i protocolli informatici che usano un registro architetturealmente decentralizzato su basi crittografiche

Art. 8-ter.

(Tecnologie basate su registri distribuiti e smart contract)

Si definiscono « tecnologie basate su registri distribuiti » le tecnologie e i protocolli informatici che usano un registro

basi crittografiche



La norma sembra suggerire l'uso
dell'algoritmo di consenso

MA

non lo dice...

architetturalmente decentralizzato su



HARDWARE O SOFTWARE?

Art. 8-ter.

(Tecnologie basate su registri distribuiti e smart contract)

Si definiscono « tecnologie basate su registri distribuiti » le tecnologie e i protocolli informatici

tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati

non alterabili e non

modificabili.

Art. 8-ter.

(Tecnologie basate su registri distribuiti e smart contract)

Si definiscono « tecnologie basate su registri distribuiti » le tecnologie e i protocolli informatici

tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati

non alterabili e non

modificabili.



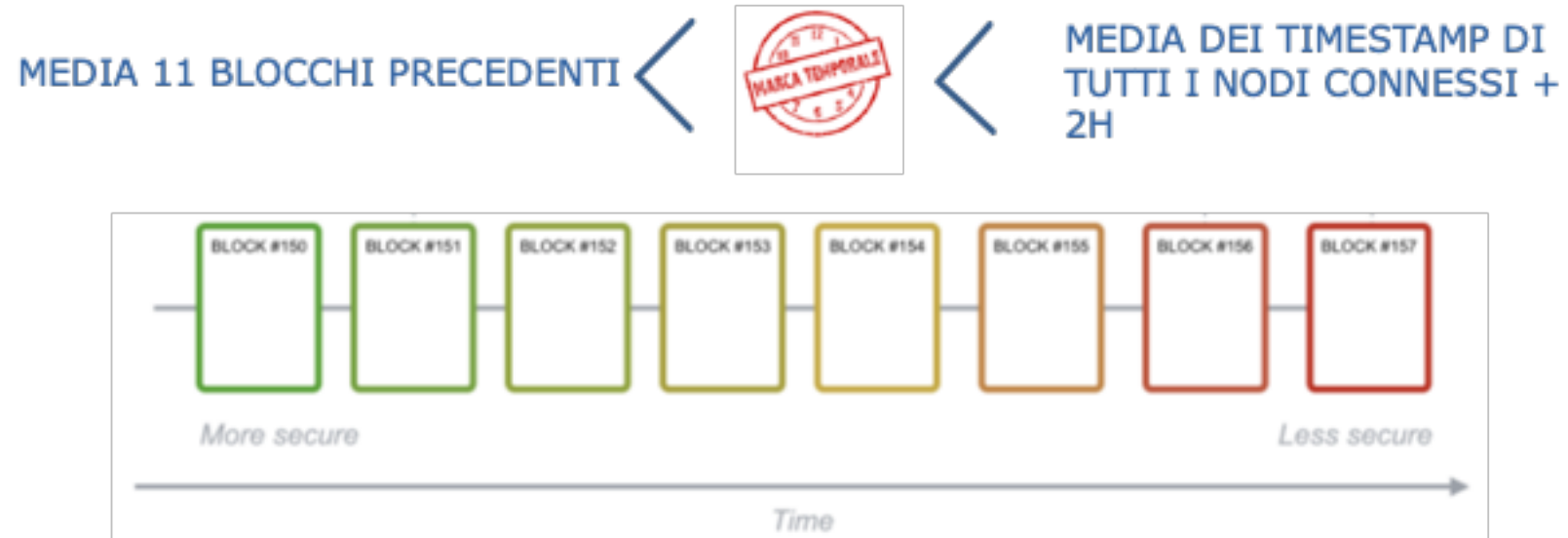
3. La memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all'articolo 41 del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014.

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.





Come funziona il timestamping



Each block contains a Unix time timestamp.

In addition to serving as a source of variation for the block hash, they also make it more difficult for an adversary to manipulate the block chain. A timestamp is accepted as valid if it is greater than the median timestamp of previous 11 blocks, and less than the network-adjusted time + 2 hours.

"Network-adjusted time" is the median of the timestamps returned by all nodes connected to you.

As a result, block timestamps are not exactly accurate, and they do not even need to be in order.

Block times are accurate only to within an hour or two.

Blockchain:
la sua funzione consiste nel
certificare l'esistenza di un
determinato «oggetto informatico»
in un determinato tempo (anche in
via indiretta)

The diagram features a central title, "Sistema di Validazione Temporale Elettronica", which is underlined. Above the title is a simple blue arc. Below the title, a vertical line descends to a horizontal line, which then branches into two vertical lines extending downwards towards the two text blocks at the bottom of the slide.

Sistema di Validazione Temporale Elettronica

dati in forma elettronica che collegano
altri dati in forma elettronica a una
particolare ora e data, così da provare
che questi ultimi esistevano in quel
momento

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

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.

validazione temporale elettronica: dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento.

Effetti giuridici della validazione temporale elettronica

1. Alla validazione temporanea elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziari per il solo motivo della sua forma elettronica o perchè non soddisfa i requisiti della validazione temporanea elettronica qualificata.

[...]

LA NORMA APPARE INAPPLICABILE!!!

**TO BE
CONTINUED...** →

moneta elettronica

“il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso dietro ricevimento di fondi per effettuare operazioni di pagamento ... e che sia accettato da persone fisiche o giuridiche diverse dall'emittente di moneta elettronica”

moneta elettronica

“il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso dietro versamento di fondi per effettuare operazioni di pagamento ... e che sia creato da persone fisiche o giuridiche di cui l'emittente è moneta elettronica”

moneta elettronica

“il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso dietro versamento di fondi per effettuare operazioni di pagamento ... e che sia emesso da persone fisiche o giuridiche di cui l'emittente è moneta elettronica”



valuta virtuale

la rappresentazione digitale di valore, non emessa 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 e trasferita, archiviata e negoziata elettronicamente

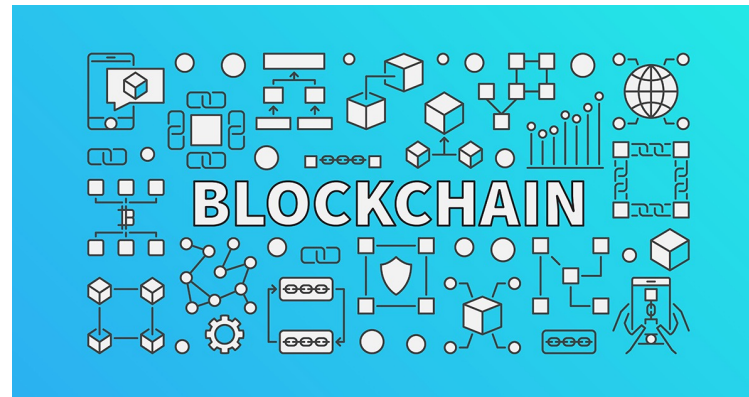
TRANSAZIONE

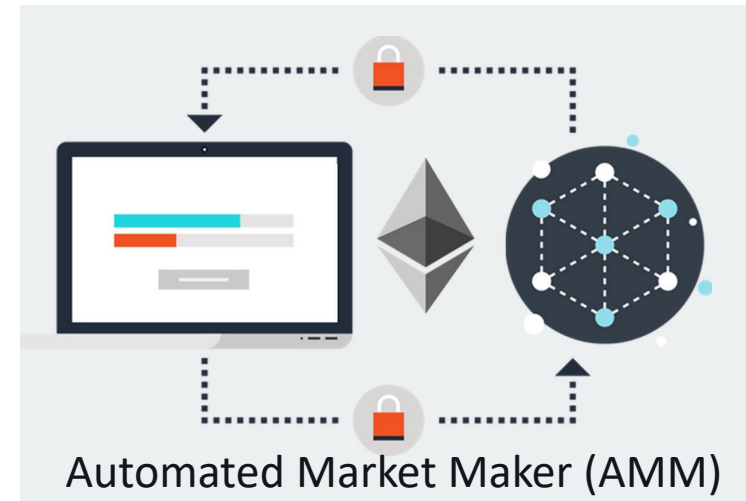


Alice



EXCHANGE





DeFi

DeFi

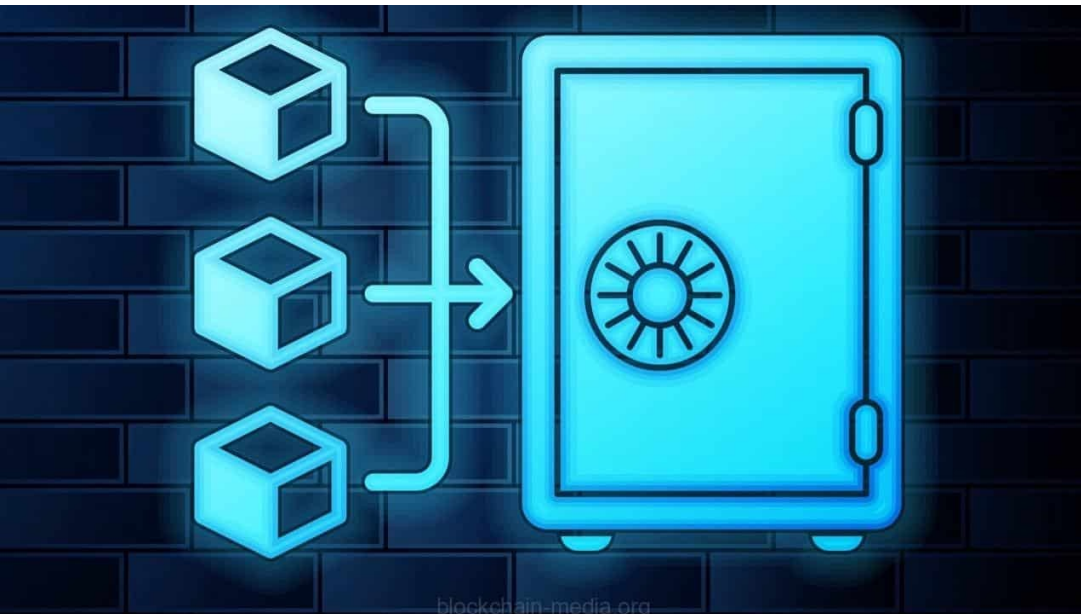
Automated Market Maker (AMM) - POOL



- Conferimento di 2 asset;
- Attivazione SC : $A \times B = K$
- Scambio
- Regolamento in aumento della moneta scambiata

DeFi

Automated Market Maker (AMM) - STAKING



- Conferimento ASSET;
- Aumento reward
- Ridistribuzione

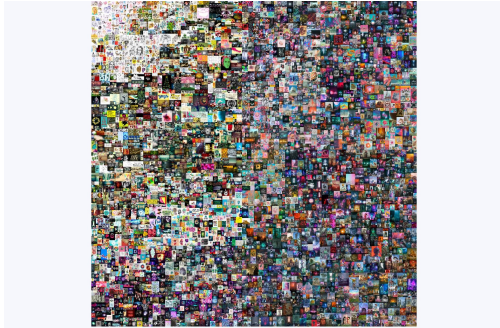
DeFi

Automated Market Maker (AMM) - Lending

A graphic with a dark blue background. On the left, the text 'DEFI LENDING' is written in white, with 'DEFI' in bold. On the right, there is a stylized globe with a network of glowing blue lines and dots overlaid on it. The word 'DeFi' is written in a large, light blue font across the center of the globe.

DEFI LENDING

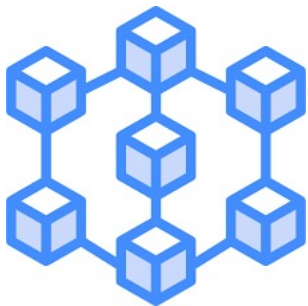
- Conferimento ASSET;
- Prestito a terzi e reward
- Cash collateral (stable coin)



Everydays: the First 5000 Days



HASH: 8bd78d028008aa7d15cbc1093d69e1f3b745092b0a988b227712e0c3543dfabc

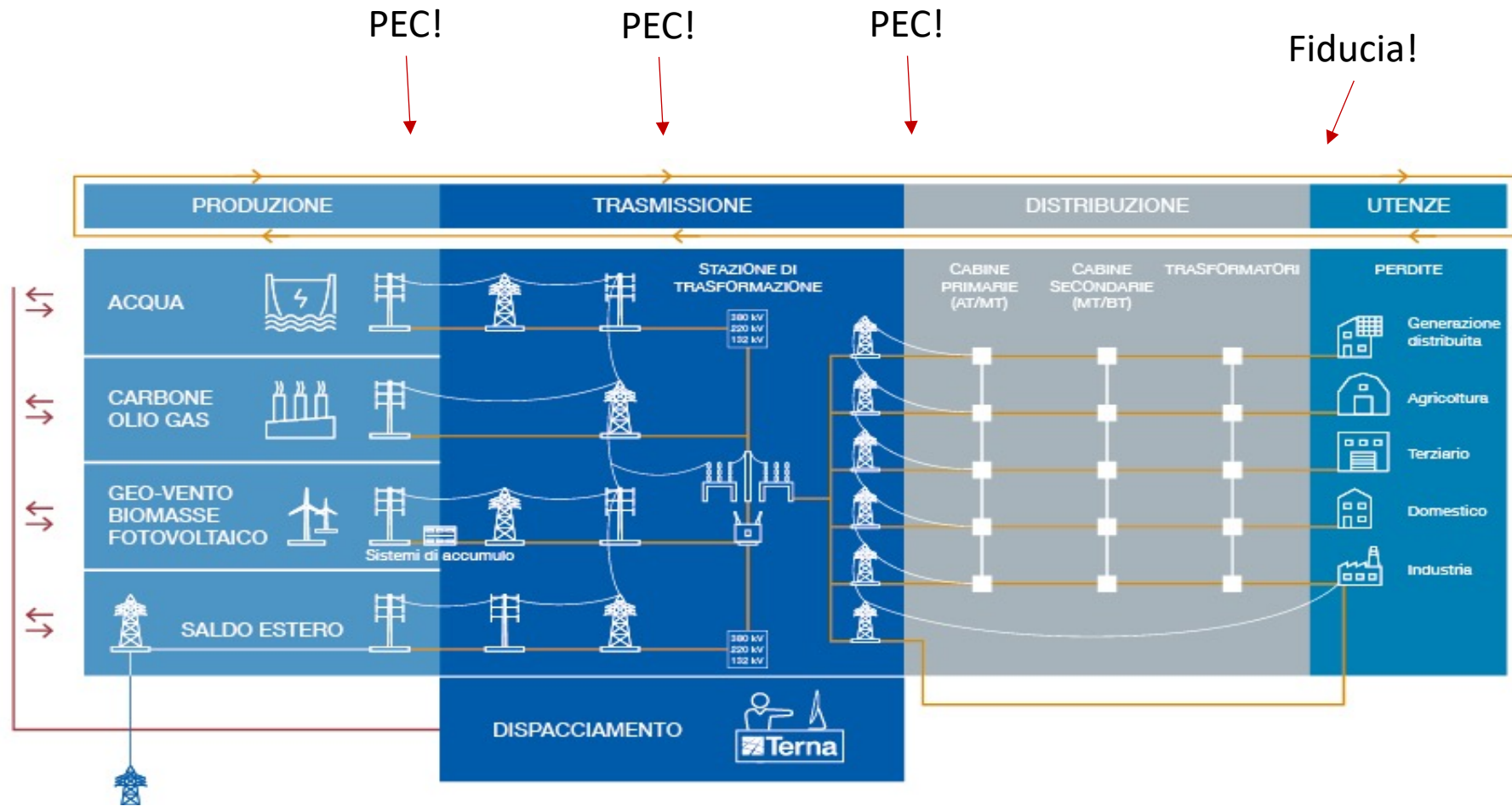


NFT

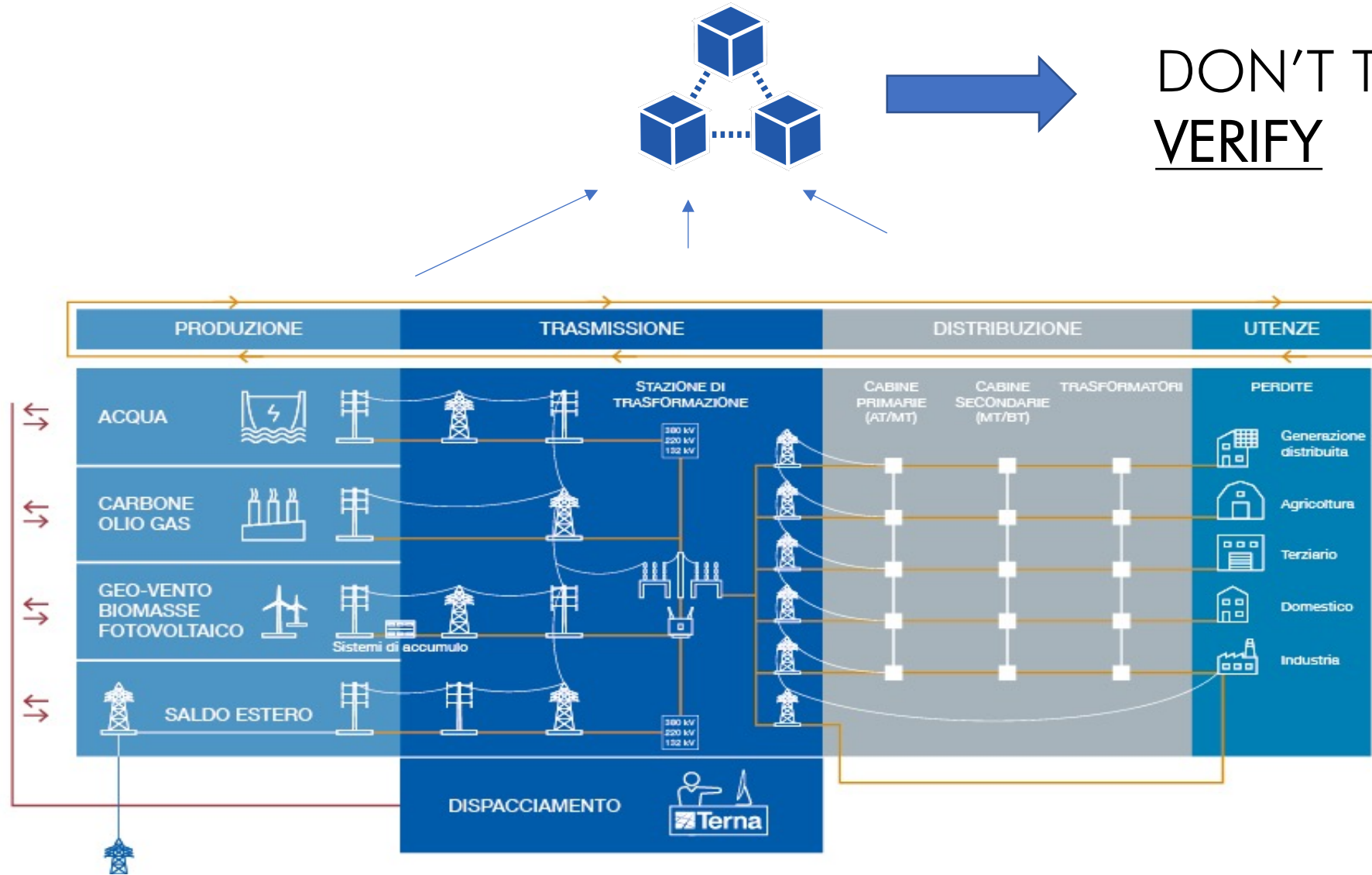
**Titolo che incorpora il
diritto su un bene
immateriale (e non?)**

**TO BE
CONTINUED...** →

Facciamo un'ipotesi: come funziona oggi il mercato dell'energia elettrica?



Facciamo un'ipotesi: come potrebbe funzionare il mercato dell'energia elettrica?



**TO BE
CONTINUED...** →



Avv. Paolo Lessio

studiolegale cislighi lessio associati

Corso di Porta Nuova, 20 - 20121 Milano tel: +39 02 94392452

fax: +39 02 89877637 e-mail: segreteria@studioclass.it