Salone dei Pagamenti - 07/11/2019 - MiCo Milano Congressi

Supply Chain e Pagamenti Innovativi

Bitcoin Smart Contracts: abilitatori per la Financial Supply Chain

Lorenzo Giustozzi
lorenzo.giustozzi@chainside.net
CEO at Chainside

chainside

Complessità della supply chain

- tracciabilità materie prime e merci
- garanzia sicurezza/qualità prodotti
- comunicazione tra le parti
- garanzie finanziarie e pagamenti
- gestione inventario e ordini

Complessità della supply chain

- tracciabilità materie prime e merci IoT tracking
- garanzia sicurezza/qualità prodotti
- comunicazione tra le parti
- garanzie finanziarie e pagamenti
- gestione inventario e ordini

Complessità della supply chain

- tracciabilità materie prime e merci — IoT tracking
- garanzia sicurezza/qualità prodotti — IoT monitoring
- comunicazione tra le parti
- garanzie finanziarie e pagamenti
- gestione inventario e ordini

Complessità della supply chain

- tracciabilità materie prime e merci — IoT tracking
- garanzia sicurezza/qualità prodotti — IoT monitoring
- comunicazione tra le parti — Platform integration
- garanzie finanziarie e pagamenti
- gestione inventario e ordini

Complessità della supply chain

- tracciabilità materie prime e merci — IoT tracking
- garanzia sicurezza/qualità prodotti — IoT monitoring
- comunicazione tra le parti — Platform integration
- garanzie finanziarie e pagamenti — Blockchain
- gestione inventario e ordini

Complessità della supply chain

• tracciabilità materie prime e merci	IoT tracking
• garanzia sicurezza/qualità prodotti	IoT monitoring
• comunicazione tra le parti	Platform integration
• garanzie finanziarie e pagamenti	Blockchain
• gestione inventario e ordini	Platform integration

Perchè usare Blockchain solo per i casi d’uso finanziari?

Perché ci servono i soldi?

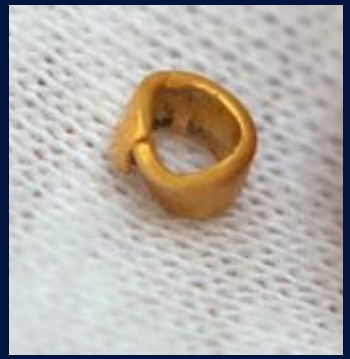
Baratto
n^2-n prezzi

	Meat	Fish	Wood	Iron	Apples
Meat	-	2	0.25	0.2	10
Fish	0.5	-	3	2	8
Wood	4	0.33	-	0.8	6
Iron	5	0.5	1.25	-	20
Apples	0.1	0.125	0.166	0.05	-

Moneta
n-1 prezzi

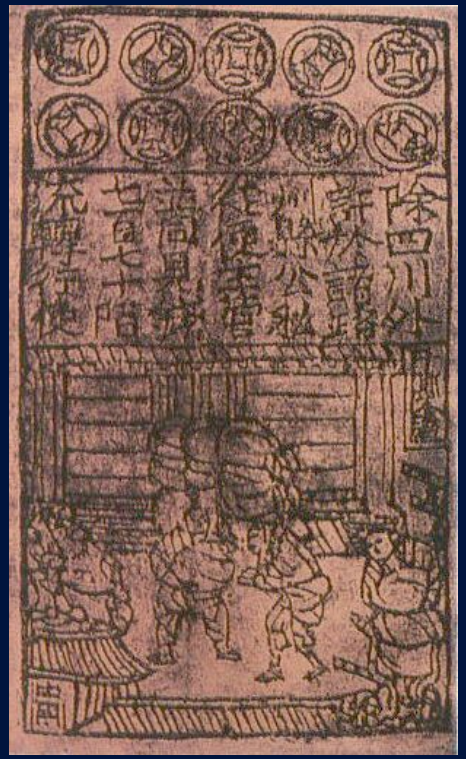
Meat	4
Fish	5
Wood	7
Iron	-
Apples	0.5

Collezionabili come moneta di scambio



Monete di metallo

Note di credito



A Jiaozi credit note, the world first paper money. Sichuan region, Song Dynasty (960–1279 CE)

Monete FIAT


100 000 000 000 000 RESERVE BANK OF ZIMBABWE
100 000 000 000 000
I promise to pay the bearer on demand
ONE HUNDRED TRILLION DOLLARS
for the Reserve Bank of Zimbabwe
AA0777821
100 000 000 000 000 HARARE
AA0777821


B
EGYMILLIÁRD B-PENGŐ
1
MILLIÁRD
B
BUDAPEST, 1946. ÉVI JÚNIUS HÓ 3-ÁN
MAGYAR NEMZETI BANK
ELNÖK
A BANKJEGYHAMISÍTÁST A TÖRVÉNY BÜNTETI


República Bolivariana de Venezuela
100
CIEN BOLÍVARES
D57965488
D57965488
100


٢٥
خمسة وعشرون دينارا
٢٥

100 SHILIN
BANKIGA DHEXE EE SOOMAALIYA
100 SHILLINGS
D137
100
SHILIN
SOOMAALI
074941
D137
100 SHILLINGS
074941
MUQDISHO 1988
100 SHILIN

Bitcoin!

Goal: ricreare nel digitale una esperienza simile a quella del contante

Goals

- transazioni p2p

Goals

- transazioni p2p
- resistente alla censura

Goals

- transazioni p2p
- resistente alla censura
- libero accesso (permission-less)

Goals

- transazioni p2p
- resistente alla censura
- libero accesso (permission-less)
- riserva di valore (store of value)

Goals

- transazioni p2p
- resistente alla censura
- libero accesso (permission-less)
- riserva di valore (store of value)
- rispettoso della privacy

Decomponiamo il problema

Decomponiamo il problema

CHI sta transando?

Decomponiamo il problema

CHI sta transando?

DOVE teniamo traccia delle transazioni?

Decomponiamo il problema

CHI sta transando?

DOVE teniamo traccia delle transazioni?

QUALE è l’oggetto della transazione?

Decomponiamo il problema

CHI sta transando?

DOVE teniamo traccia delle transazioni?

QUALE è l'oggetto della transazione?

QUANDO è avvenuta una transazione?

CHI sta transando?

SISTEMA CENTRALIZZATO

Un coordinatore gestisce le identità di tutti i partecipanti con un sistema di credenziali.

CHI sta transando?

SISTEMA
DECENTRALIZZATO

Nessun coordinatore “sulla collina”, sistema di identità basato su firma digitale.

Digital signatures

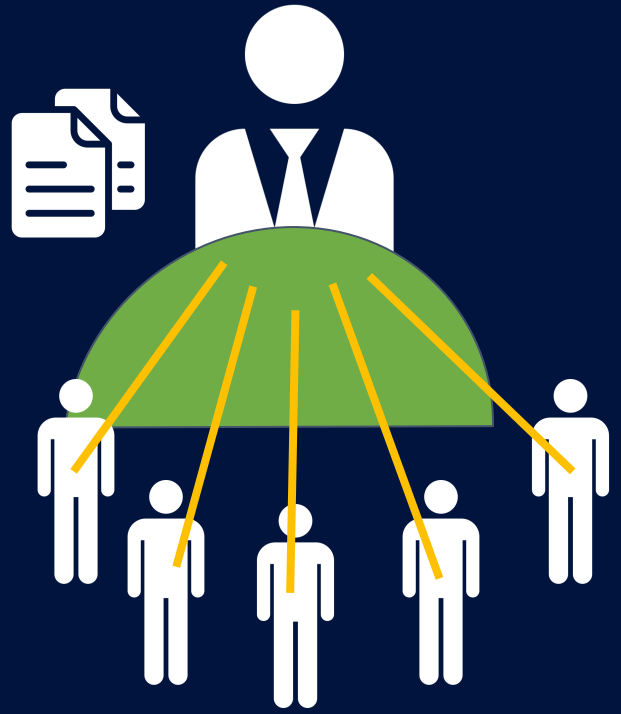
PRIVATE KEY

PUBLIC KEY

DOVE teniamo traccia delle transazioni

SISTEMA CENTRALIZZATO

Un coordinatore mantiene un libro mastro su cui ha pieno controllo per gestire i movimenti.



DOVE teniamo traccia delle transazioni

SISTEMA
DECENTRALIZZATO

Ognuno tiene traccia di tutte le transazioni del sistema.

QUALE è l'oggetto della transazione

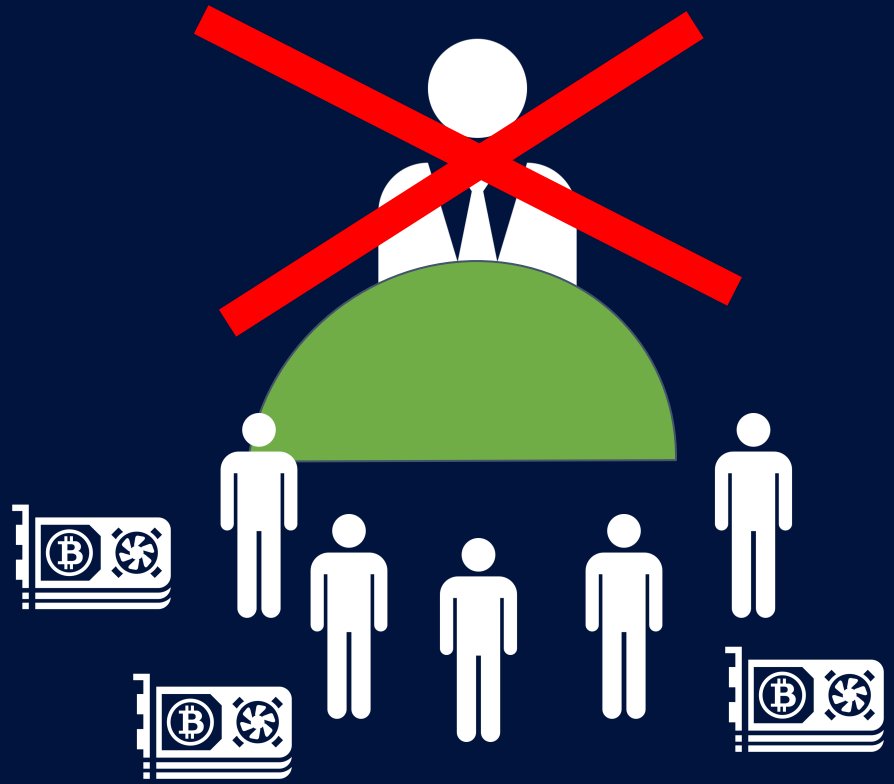
SISTEMA CENTRALIZZATO

Un issuer centralizzato ha il potere di creare moneta per tutti (es. banca centrale)

QUALE è l'oggetto della transazione

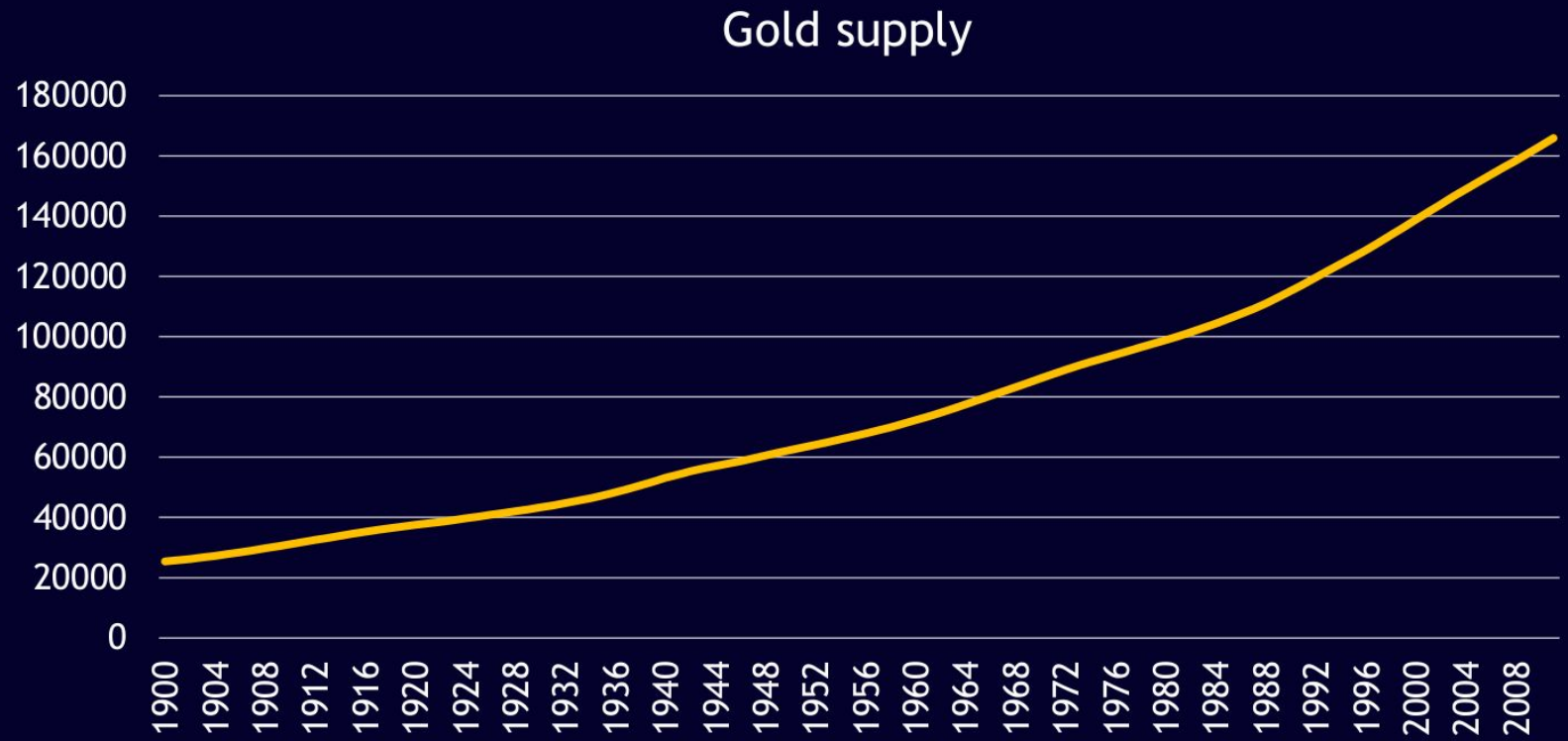
SISTEMA
DECENTRALIZZATO

Chiunque possa "bruciare" energia elettrica è in grado di creare moneta (con alcuni limiti).

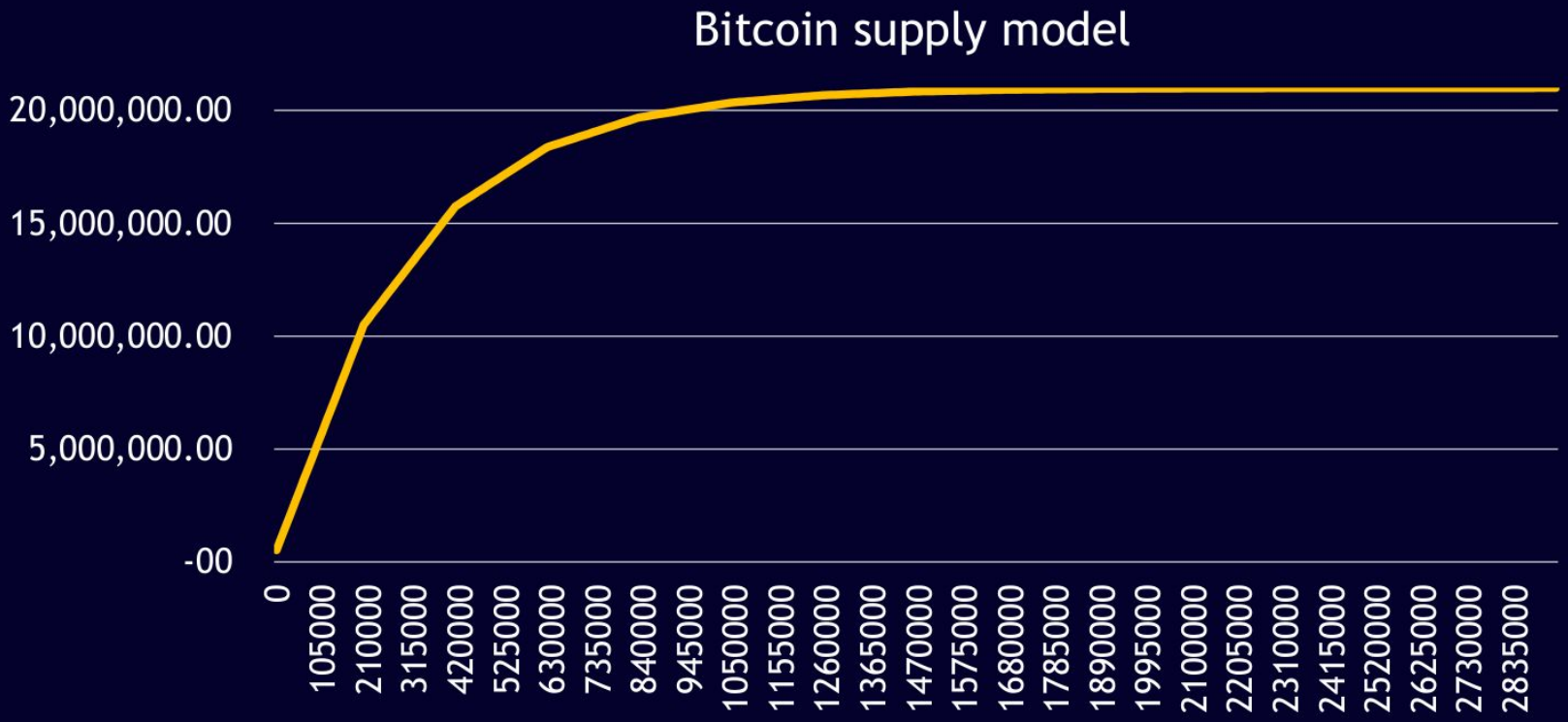



BITMAIN

Store of value



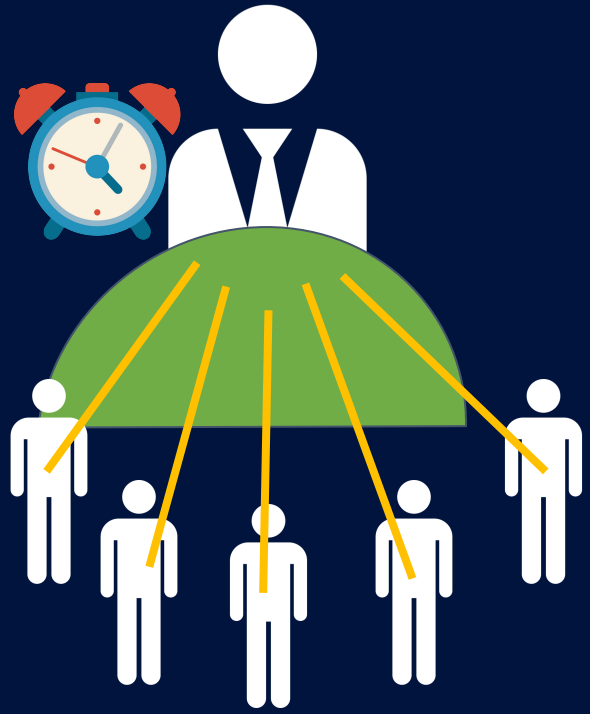
Store of value



QUANDO è avvenuta la transazione

SISTEMA CENTRALIZZATO

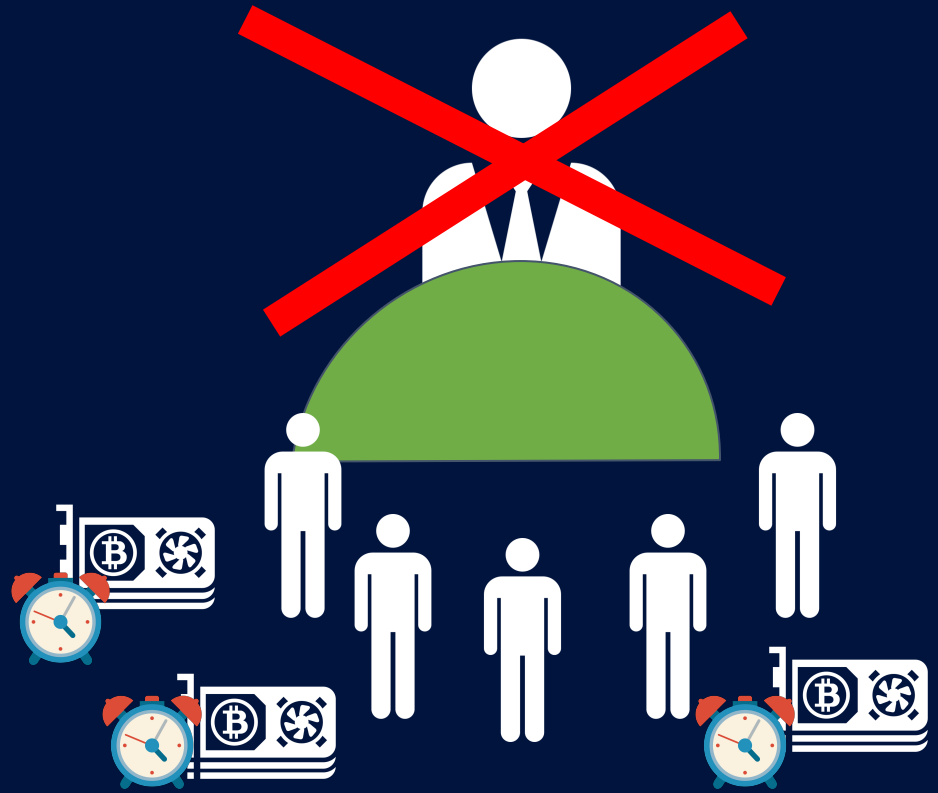
Un coordinatore tiene traccia dei timestamps delle transazioni e le ordina cronologicamente.



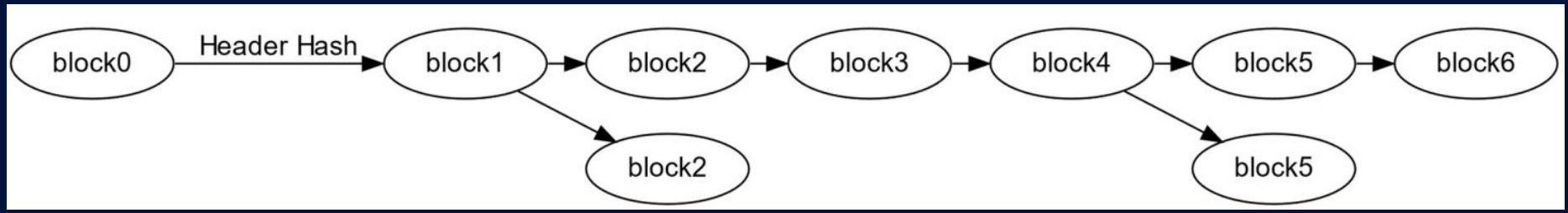
QUANDO è avvenuta la transazione

SISTEMA
DECENTRALIZZATO

Tutti quelli che partecipano alla creazione di nuova moneta, implicitamente aiutano nell'ordinamento delle transazioni.



The blockchain



Recap

- transazioni p2p
- resistente alla censura
- libero accesso (permission-less)
- riserva di valore (store of value)
- rispettoso della privacy

Recap

- transazioni p2p
- resistente alla censura
- libero accesso (permission-less)
- riserva di valore (store of value)
- rispettoso della privacy

Recap

- transazioni p2p
- resistente alla censura
- libero accesso (permission-less)
- riserva di valore (store of value)
- rispettoso della privacy

Recap

- transazioni p2p
- resistente alla censura
- libero accesso (permission-less)
- riserva di valore (store of value)
- rispettoso della privacy

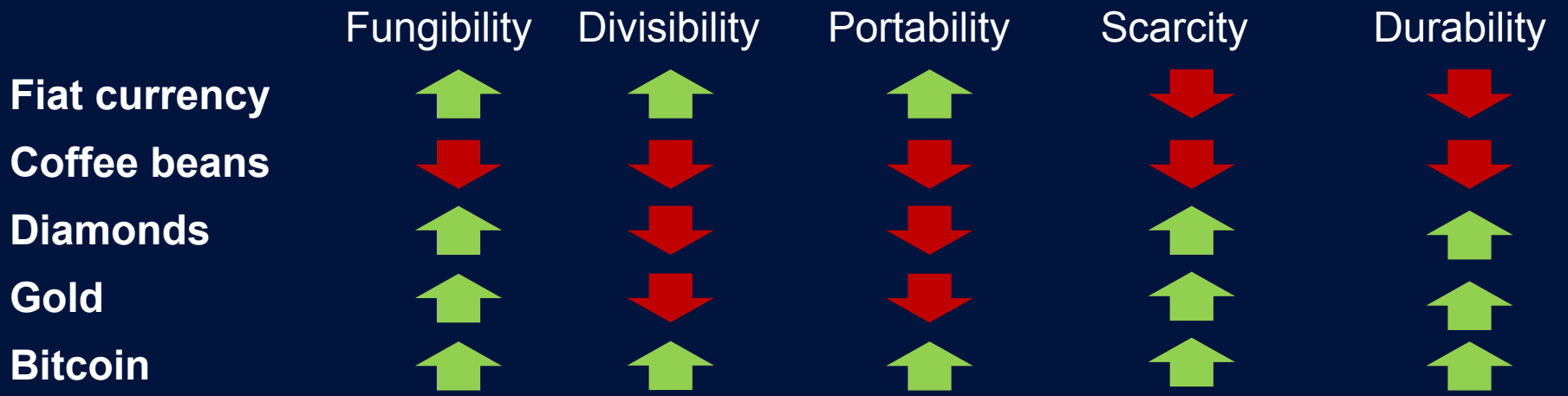
Recap

- transazioni p2p
- resistente alla censura
- libero accesso (permission-less)
- riserva di valore (store of value)
- rispettoso della privacy

almost

Perché Bitcoin è una buona forma di moneta

L’abilità di un asset di essere un buon trading token può essere valutato basandosi sulla sua fungibilità, divisibilità, trasportabilità, scarsità e resistenza nel tempo.

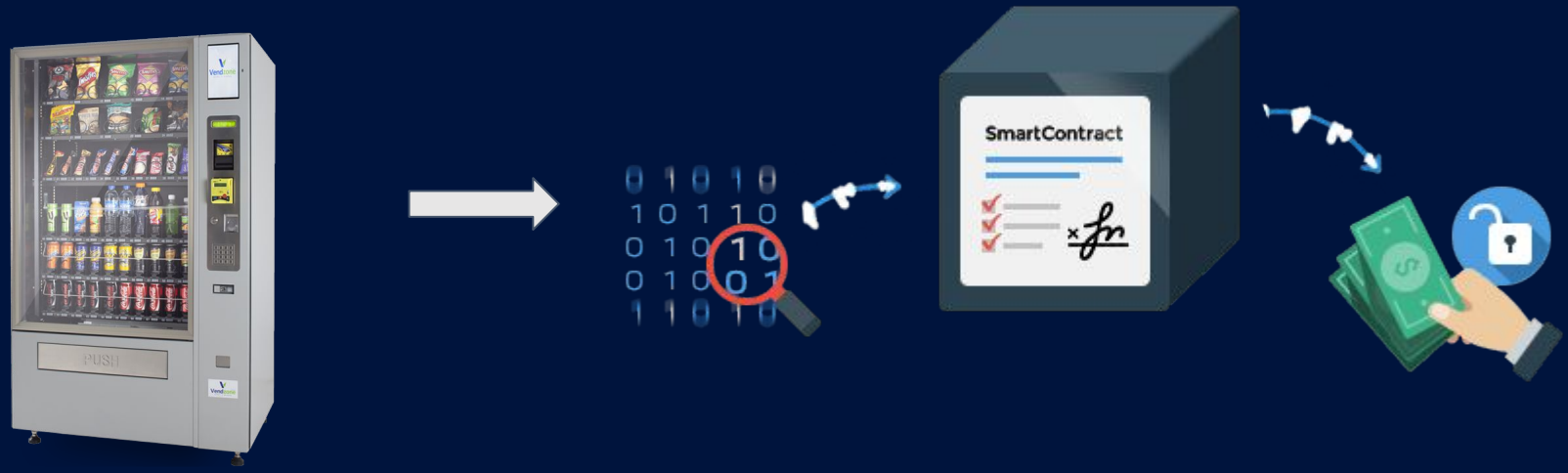


Perchè usare Blockchain solo per i casi d’uso finanziari?

Perchè il paradigma nasce esclusivamente per loro

Concetti base - Smart Contract

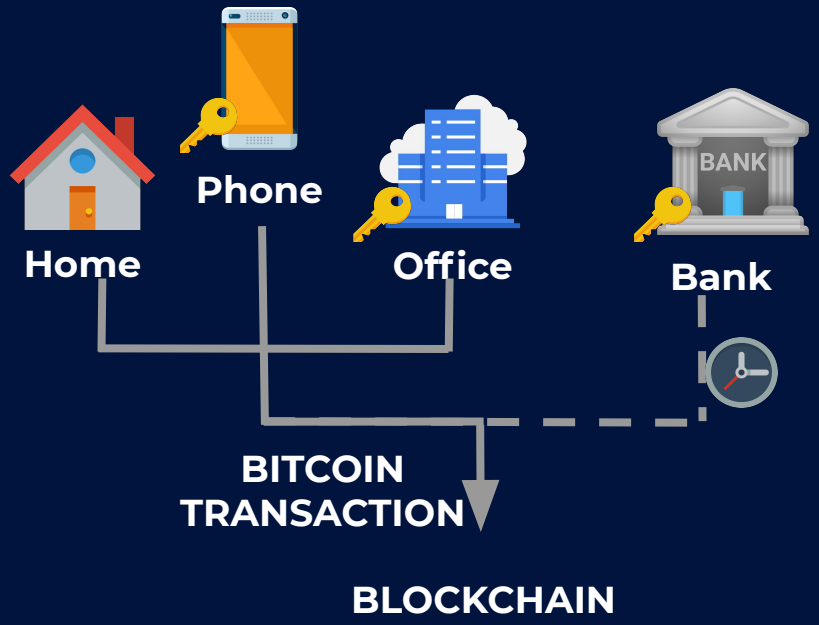
Programma informatico trustless che applica i termini di un contratto in maniera trustless, l'esecuzione del codice è garantito da una rete che verifica le condizione di spesa di una transazione



Concetti base - Smart Contract 2

MultiSig + Timelock

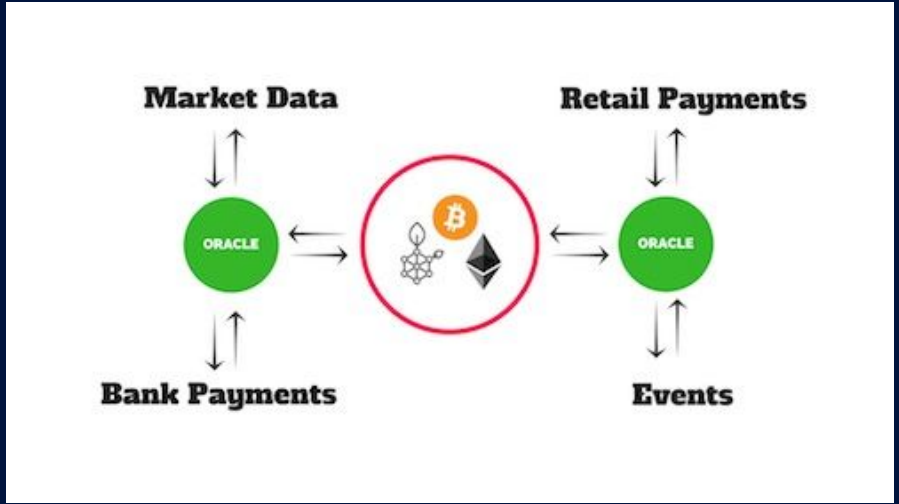
Speciale tipologia di smart contract che permette l'imposizione di vincoli di spesa su più firme e sul tempo trascorso dall'emissione



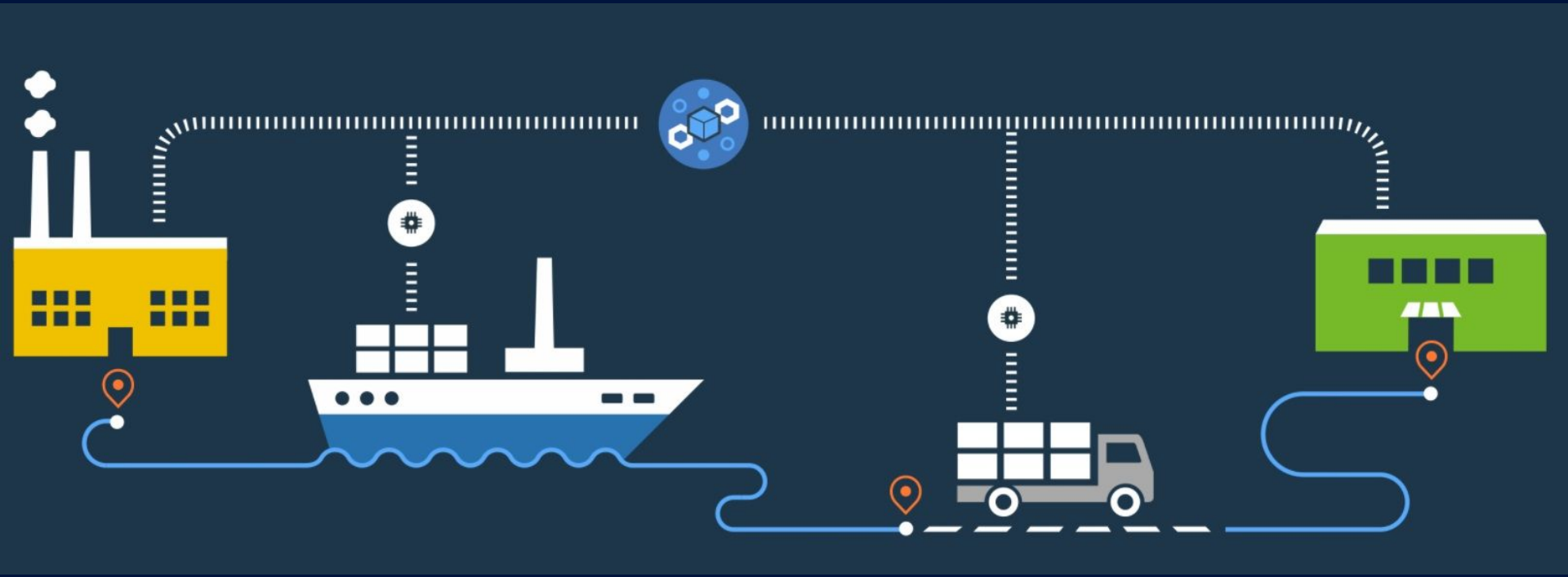
Concetti base - Oracoli

Ponte di collegamento tra il mondo tradizionale e quello blockchain

Event Stream che porta a sbloccare transazioni in base a eventi nel mondo esterno.



Use Case 1
Tracking navale e pagamenti automatici



Tracking navale e pagamenti automatici

Goal:

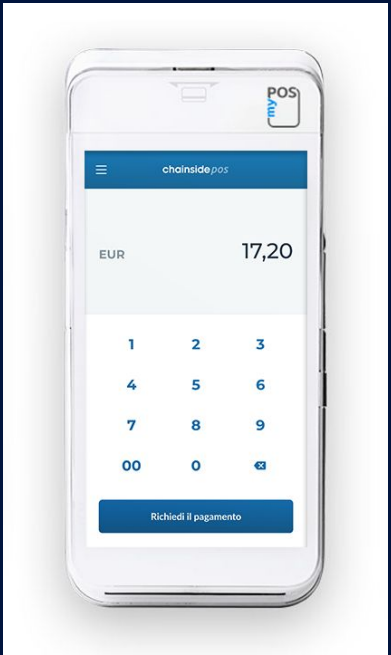
- minimizzare rischio di controparte
- rilascio di pagamenti parziali by step
- dati affidabili di terze parti su cui fare leva

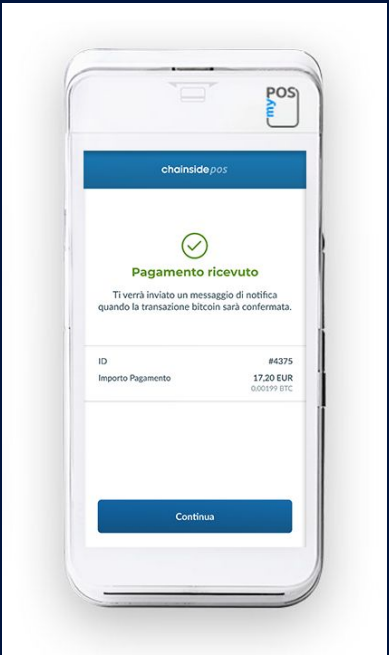
Abilitatori:

- escrows: Chainside, BitGo, etc.
- oracoli: fornitori dati satellitari
- bitcoin smart contracts:
  - multisig: (3-di-4) escrow + oracolo + venditore + acquirente
  - timelock: restituzione fondi automatico con timeout

Use Case 2 - itTaxi

Use Case 2 - itTaxi





Use Case 2 - itTaxi

Extra:

- pay-per-use BTC/LN via tassametro

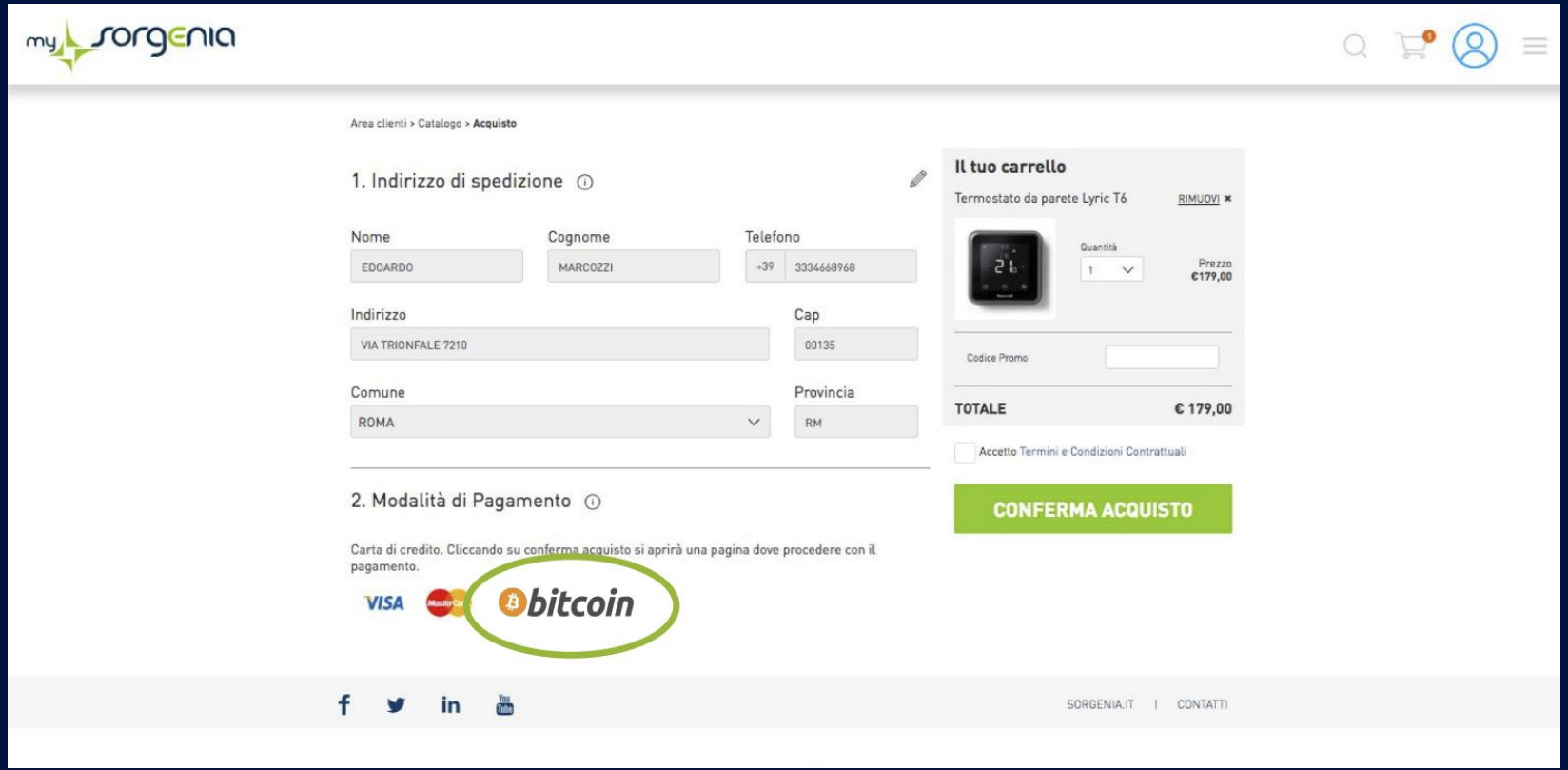
Use Case 2 - itTaxi

Extra:

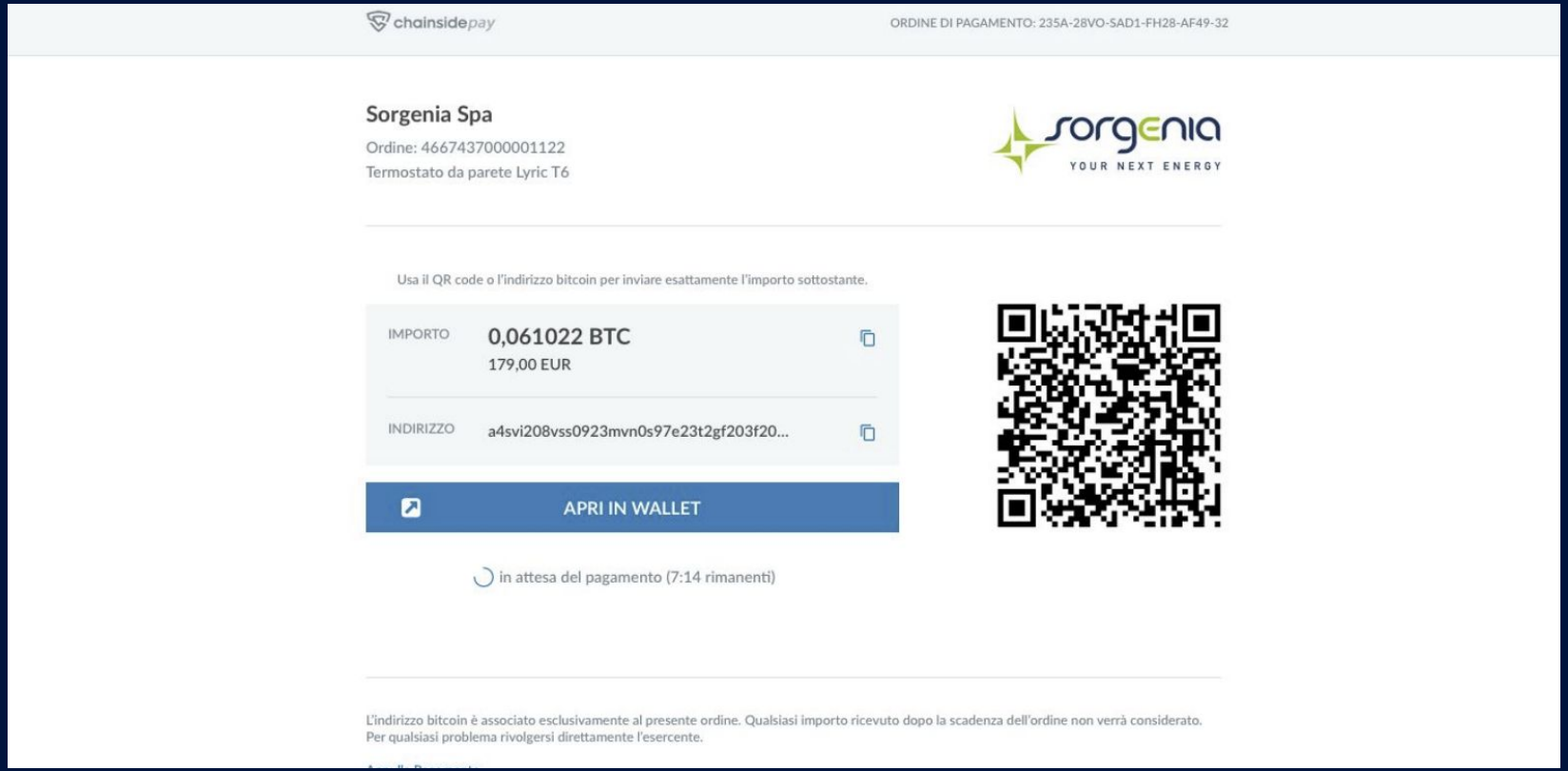
- pay-per-use BTC/LN via tassametro

Use Case 3 - Sorgenia

Use Case 3 - Sorgenia



Use Case 3 - Sorgenia



Use Case 3 - Sorgenia

Extra:

- pay-per-use BTC/LN via smart-meter

Conclusioni

- Gli use-case che prevedono transazioni monetarie sono quelli più sensati nelle applicazioni blockchain
- Il pay-per-use può essere molto rivoluzionario in diversi settori con un rischio di credito più o meno diffuso
- Per collegare il mondo tradizionale a quello blockchain il ruolo degli oracoli è fondamentale

Thanks