# La mia esperienza con le blockchains

Vincenzo Vespri - Università di Firenze

Evento De Componendis Cifris
Dipartimento di Matematica
Bologna, 22 Gennaio 2018

# Mia storia

Sono un analista "infiltrato" . Il mio collegamento con la Crittografia è che insegno a Informatica. Circa tre anni fa, sno stato contattato da studenti interessati. Per utilizzare la tecnologia blockchain in modo nuovo. Faccio proposta per una spin-off universitaria. Obiettivo il mondo dei buoni pasto. L'intermediario ha circa il 15% del valore del buono pasto. La tecnologia blockchain permette di evitare l'intermediario. Tecnologicamente tutto funziona. App basato sui bitcoin. Contatto con Tinaba (This is not a bank) di Arpe.

Sorpresa non è possibile perché dalla legge viene richiesto esplicitamente un intermediario.

Questo è un problema per questa tecnologia. Tante potenziali applicazioni, ma non c' è ancora il contesto legale.

Possibii applicazioni:

smart property: un oggetto potrebbe consultare la blockchain per autenticare le credenziali di un utente e riconoscere il suo legittimo proprietario, in questo modo sarebbe possibile trasferire digitalmente la proprietà di qualsiasi bene tangibile, rendendo il passaggio effettivo istantaneamente

smart contracts: più controparti potrebbero stipulare e finalizzare accordi e contratti, con la garanzia che questi verranno garantiti e resi effettivi automaticamente al vericarsi di opportune condizioni

smart agents: i nodi che condividono la blockchain, rappresentano una sorta di semplice ambiente di calcolo distribuito, con alcune modifiche sarebbe possibile implementare agenti autonomi in grado di replicare se stessi, migrare e scambiare o gestire le risorse

Per maggiori dettagli vedasi ad esempio
https://www.hyperledger.org/projects

Combinando le possibilità offerte è possibile estendere ulteriormente il campo applicativo, pensiamo al settore delle financial securities, grazie alla possibilità di introdurre contratti digitali tra le parti sarebbe possibile scambiare prodotti finanziari, ma sarebbe anche possibile gestire l'erogazione di prestiti e perfino di lotterie. Inoltre è possibile pensare a sistemi di crowdfunding o a sistemi di voto digitale completamente trasparenti. La capacità di fornire la garanzia dell'esistenza o meno di un dato in un certo istante di tempo rendono la blockchain un deposito ideale di record pubblici o brevetti , inoltre può costituire la base per veri e propri sistemi di cloud storage decentralizzati . Se ampliamo il concetto di nodo includendo nella sua definizione qualsiasi dispositivo connesso, è possibile utilizzare la blockchain per far interagire autonomamente i nodi della Internet of Things in modo sicuro e scalabile

In una rete distribuita spesso è necessario certificare la data di creazione o di modifica di una informazione in modo tale che nessuno, nemmeno chi ha creato l'informazione, possa alterarla. Per implementare un sistema di questo tipo è necessario rendere disponibile pubblicamente una infrastruttura in grado di raccogliere, processare e rinnovare le marche temporali, o timestamp, dei documenti digitali.

Significa risolvere il problema dei cosiddetto problema del consenso dei generali bizantini. La blockchain rappresenta un servizio di timestamp decentralizzato, infatti un blocco è considerato più recente di un altro se viene aggiunto dopo di esso, per tale ordinamento vale la proprietà transivita ed inoltre, supponendo che la sequenza di blocchi non presenti biforcazioni, tale ordine è totale. Di conseguenza una transazione è considerata più recente di un'altra se contenuta in un blocco più recente. Nel caso in cui le due transazioni fossero contenute nello stesso blocco, esse vengono ordinate in base all'ordine con cui compaiono all'interno del blocco.

Il teorema CAP (Consistency, Availability e Partition tolerance), anche noto come teorema di Brewer, asserisce che un sistema distribuito è impossibilitato a garantire simultaneamente tutte e tre le seguenti proprietà:
consistenza forte: tutti i nodi condividono gli stessi dati allo stesso momento;
disponibilità: una richiesta deve poter ricevere esito positivo o negativo, in qualsiasi momento;
tolleranza al partizionamento: la rete è resistente al fallimento o alla disconnessione di uno o più nodi;

# Ricadute sul sistema bancario

Le Fintech sono startup di tecnologia abbinata ai servizi finanziari che lavorano per renderli accessibili a chiunque, ovunque ci si trovi, che stanno creando un nuovo settore, quello della tecno-finanza, utilizzando pienamente in chiave financial services i nuovi paradigmi tecno-business.
Le criptovalute sono di primaria importanza nel Fintech.

Questa innovazione si sta polarizzando su due principali direttive collegate:
1) la Blockchain emerge al di là dei Bitcoin come un nuova tecnologia che contribuirà ad eliminare alcune importanti barriere tipiche dei metodi tradizionali di trasferimento del valore;
2) nuove criptovalute e forme collegate di implementazioni blockchain-based.

Le possibilità offerte da un diffuso registro pubblico e distribuito (DLT) che raccoglie in un database permanente tutte le transazioni effettuate e che opera attraverso un network di blocchi collegati tra di loro in ordine lineare e cronologico, sono illimitate. La Blockchain può affermarsi nei servizi finanziari come una rete di valore basata sulla notarizzazione digitale per diversi fattori:

a) l'assenza di una clearing house o di una istituzione centrale che verifica ed elabora i dati in quanto ogni blocco della catena crea un sistema auto-validante;

b) la totale digitalizzazione dei processi elimina l'attività di back-office, documentazione cartacea, tempi di vidimazione ed errori umani, le operazioni sempre corrette sono svolte in tempi ristretti;

c) il sistema decentrato non è modificabile o cancellabile da terzi perché incentrato sulla elevata sicurezza della crittografia a cui si aggiunge l'impossibilità di hackerarlo in quanto intaccare la validità di un dato in blocco presente in tutti i nodi di una blockchain, porta gli altri a non riconoscerlo e quindi ad escluderlo dal sistema.

Bank of England ha osservato che oltre ai costi di transazione estremamente ridotti, la rimozione degli intermediari elimina rischi operativi, solvibilità e di liquidità ad essi associati.
L'emissione di nuove divise digitali sviluppa nuove forme di business collegate, come Ethereum che ha aperto una nuova via che unisce uno scambio in criptovaluta ad uno Smart Contract linkato alla moneta

# Problemi

1) La natura disruptive del digitale presenta anche lati oscuri e rischi ancora da esplorare, quali i problemi di cyber-sicurezza e potenziali violazioni della privacy

2) manca una legislazione coerente

3) quando si introduce un App alla blockchain, l'App deve avere la stessa sicurezza della blockchain, se no il sistema, pur essendo basato sulla blockchain, non è sicuro.

# Ritornando a me

Senza spin-off non ho potuto trattenere studenti.Conseguenza (punto di forza) diaspora di studenti in aziende informatiche.

Hesplora (start up innovativa)

Oraclize (Londra)

Vargroup (grande azienda)

Cabel-Invest Bank (aziende che si occupano di FinTech)

Engineering