INTESA SANPAOLO

# Blockchain e cryptocurrencies: tecnologie disruptive da reinterpretare per abilitare uno scale-up industriale

Torino, 17 aprile 2018

# PREMESSA



Visti i *constraints* in termini temporali, la presentazione **mira** a **illustrare** alcune **nozioni** relativamente a:

- le **tecnologie Blockchain, bitcoin** e **Distributed Ledger** (con gli attuali benefici e limiti);
- le **cryptocurrencies e** delle **Initial Coin Offering** (ICO);
- le **posizioni espresse** da alcuni **Regulators** sui temi precedentemente menzionati;
- alcune sperimentazioni e **iniziative di rilievo**

al fine di avere una visione d'insieme sui temi menzionati e interpretare alcuni trend atto.

# AGENDA

1. Blockchain pubblica, bitcoin e blockchain privata/DLT
2. Altre cryptocurrencies e Initial Coin Offering (ICO)
3. Cenni sulle posizioni espresse da alcuni Regulators
4. Conclusioni: verso l'industrializzazione
5. Use case: La blockchain rivoluziona anche l'agricoltura con Pavo

# La blockchain: un registro pubblico distribuito che può eliminare la necessità di intermediari

- La **blockchain** (**pubblica** o **permissionless**) è **un'architettura tecnologica** che ha visto la luce nel **2009**, con la **nascita** del **bitcoin**, per **consentire** lo **scambio diretto** tra **utenti** (peer-to-peer) di **asset digitali** **(bitcoin)**

- La **blockchain** è un **registro** pubblico **condiviso** e **distribuito** dove vengono **registrate tutte** le **transazioni**, in modo **sicuro** perché **protette da crittografia.**

- Grazie agli **smart contracts** è possibile **programmare** e **automatizzare le transazioni**, sulla base di una serie di parametri.

- Tale tecnologia, in linea teorica, potrebbe essere **applicata cross-industry** (anche in ambito pubblico) in tutti i casi in cui sia necessario **certificare il passaggio di informazioni e/o di asset rappresentativi di valore (anche di proprietà)**, **eliminando** la **necessità** di avere un **intermediario** che ne garantisca la validità

Sicura | Trasparente | Non ripudiabile | Programmabile | Tamper Proof

# Cryptovalute: la disruption determinata dal bitcoin (1/2)



**Il bitcoin** è una **valuta virtuale**, regolata da un protocollo informatico in possesso di alcune **caratteristiche fondamentali**:

- la sua **emissione non** è **gestita** da un **ente centrale**, ma avviene secondo regole definite dal **protocollo Bitcoin**
- il suo scambio avviene direttamente tra gli utenti **(peer to peer) senza necessità di banche** o altri **intermediari** a garantire l'ownership degli asset scambiati **(decentralizzazione)**
- utilizza un libro mastro condiviso e pubblicamente visibile nel quale vengono registrate tutte le transazioni eseguite nel sistema, la **blockchain**
- le regole di funzionamento sono basate su un software **open source**
- è **crittograficamente protetta** rendendola sicura e a prova di frode
- è possibile **condizionare** l'**esecuzione** delle **transazioni a determinati eventi (programmabilità)**

# Cryptovalute: la disruption determinata dal bitcoin (2/2)



- le **transazioni** eseguite **non** sono **cancellabili** - «stornabili» -, ma vengono registrate «per sempre» nel libro mastro condiviso **(immutabile)**

- gli utenti che operano sulla rete sono pseudo-anonimi **(chiavi crittografiche)**

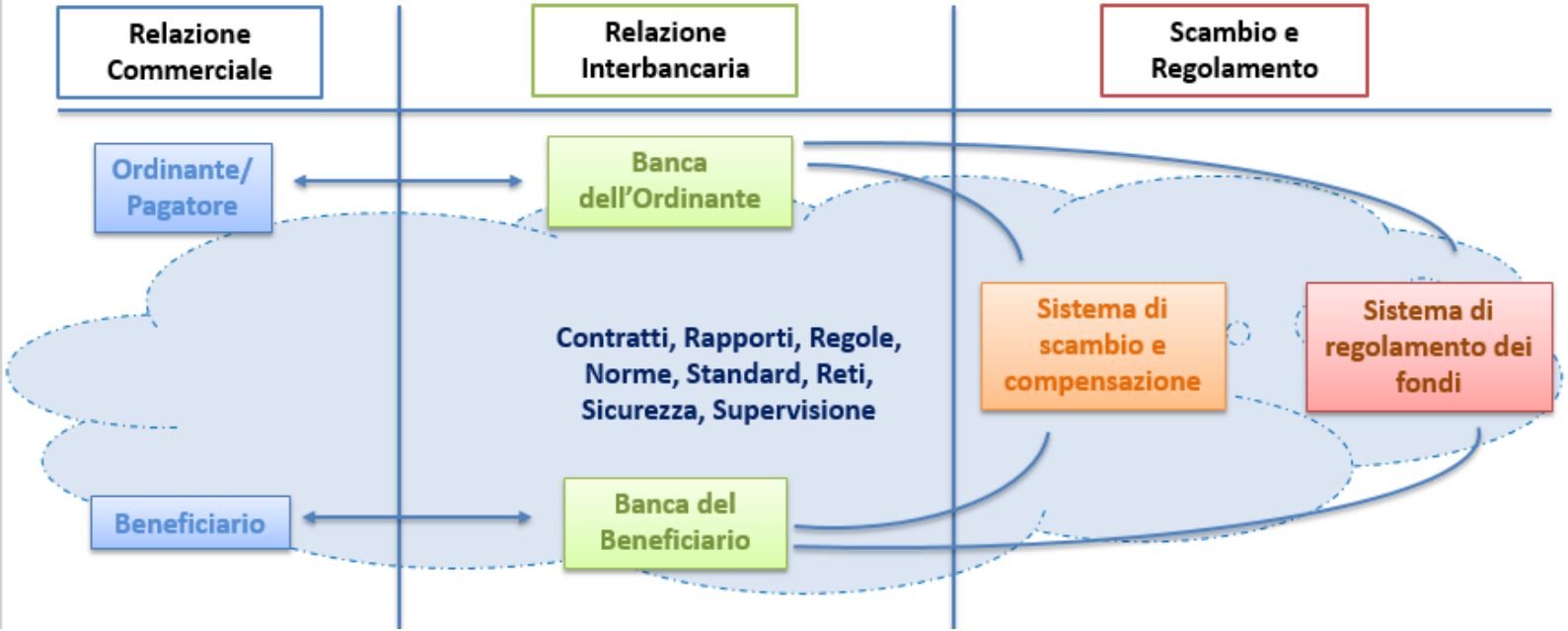
*… **in conclusione:***

*La **blockchain (pubblica) e il bitcoin** sono **legati intrinsecamente**.*

*Il **bitcoin** è una valuta virtuale (o **cryptovaluta**) che può essere **scambiata tra privati e/o aziende sulla blockchain pubblica, senza l'intervento di alcun intermediario finanziario**, sostituendo il trust sulla regolarità e finalità del passaggio di valore - garantito nei sistemi centralizzati da intermediari abilitati e sistemi di clearing e settlement - con l'immutabilità delle transazioni registrate sulla blockchain, che funge da **registro pubblico distribuito** (si dice "distribuito" perché le stesse informazioni sono disponibili su tutti i computer – nodi – che partecipano alla rete blockchain). Proprio per tale motivo la **blockchain pubblica** è anche denominata **trustless**, ossia i **bitcoin possono essere scambiati tra persone/entità giuridiche che non si conoscono** (non c'è bisogno di «trust»), **perché la finalità della transazione è garantita dalle caratteristiche tecnologiche della blockchain**.*

# Pagamenti tradizionali vs pagamenti bitcoin: sintesi delle principali caratteristiche di un sistema di pagamento tradizionale






Intesa Sanpaolo 2018- All rights reserved.

# Il bitcoin: gli attuali limiti per un uso industriale in ambito finanziario



## SCALABILITÀ

- Basso numero di transazioni/secondo
- Le transazioni non sono immediatamente «finali» (elevata latenza)
- L'importo delle spese può crescere in modo considerevole

## PRIVACY E TRACCIABILITÀ

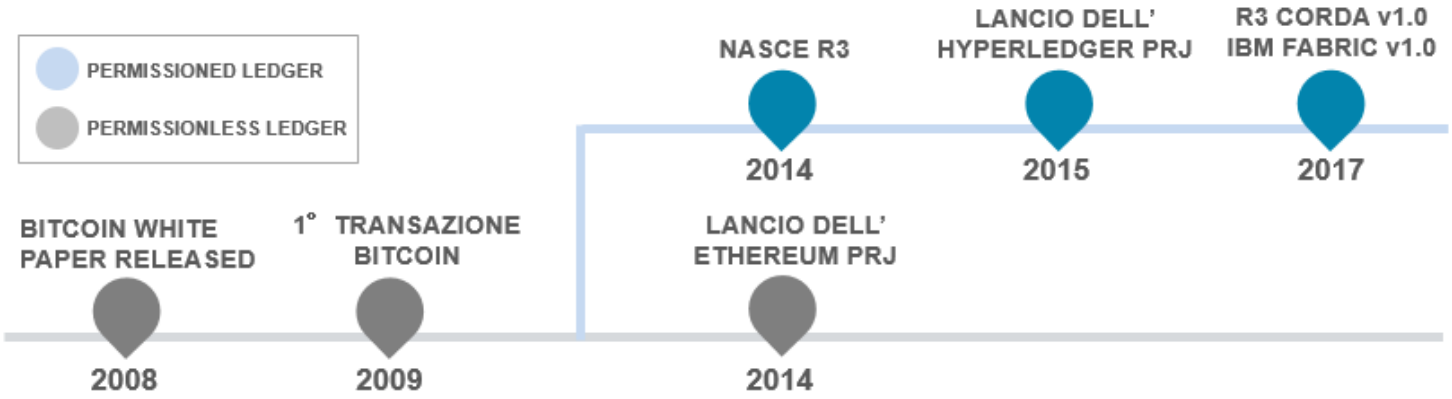
- Le transazioni sono pubbliche
- Gli indirizzi che si scambiano transazioni e gli importi sono pubblici, ma non è presente un matching tra indirizzo e persona
- Sotto certe condizioni gli indirizzi possono essere anonimizzati e rendere impossibile la tracciatura delle transazioni

## STABILITÀ

- Il Prezzo è estremamente volatile a causa di:
  - un mercato limitato
  - emissione predefinita di bitcoin (anelasticità)

# I limiti della Blockchain spostano l'attenzione sui Distributed Ledger






- **Un Distributed Ledger è un database condiviso, sincronizzato e geograficamente distribuito**
- Alla tradizionale natura pubblica, o **"Permissionless"**, della blockchain utilizzata da molte delle cryptovalute presenti sul mercato (a cominciare dal bitcoin), si sono progressivamente affiancati utilizzi della tecnologia in ottica "**Permissioned**", ossia reti dove **solo partecipanti riconosciuti e autorizzati** possono entrare a far **parte** del **network, rendendo «inutile» in tale ambito lo sforzo computazionale richiesto per la Proof-of-Work nella blockchain pubblica.**
- **Alcuni vantaggi:** più efficiente e scalabile, maggiore controllo dei Regulators, più semplice la standardizzazione e l'interoperabilità, privacy e tracciabilità garantite.

# Blockchain e Distributed Ledger: principali differenze



| Blockchain | | DLT |
|---|---|---|
| ▪ Tutti possono partecipare alla rete, i partecipanti non sono identificati – **rete Permissionless** | **Accesso** | ▪ Solo partecipanti identificati e autorizzati possono accede al network – **rete Permissioned** |
| ▪ Il consenso per l'aggiornamento del registro avviene a livello di network attraverso un meccanismo (tipicamente la Proof-of-Work) potenzialmente eseguibile da tutti gli utenti | **Consenso** | ▪ Il consenso per l'aggiornamento del registro avviene spesso a livello di singolo deal attraverso un meccanismo scelto ad-hoc |
| ▪ Una volta raggiunto il consenso, l'informazione inserita non può più essere cancellata | **Immutabilità** | ▪ Una volta raggiunto il consenso, l'informazione inserita non può più essere cancellata |
| ▪ Possiedono un asset nativo (crypto-valuta) | **Asset nativo** | ▪ Non possiedono un asset nativo |
| ▪ **Tutti gli utenti** posseggono la **stessa versione del registro con tutte le informazioni di tutte le transazioni** eseguite fino a quel momento | **Privacy** | ▪ **Ogni partecipante vede solo le informazioni di propria competenza** |

# Cryptovalute: il mercato complessivo

- Partendo dai principi del bitcoin e del suo protocollo le altcoins hanno cercato di **differenziarsi** focalizzandosi su **specifiche funzionalità** (es. livello di privacy, velocità delle transazioni, applicazione di smart contracts, etc.)

- Il mercato attorno alle cryptovalute ha avuto nell'ultimo periodo un **rapido incremento**, raggiungendo **a gennaio 2018**:
  - **market cap** superiore a $580 miliardi;
  - un volume di transazioni giornaliere complessive superiore a $44 miliardi
  - Dove il bitcoin rappresenta:
    - Il 34% del market cap
    - un volume di transazioni giornaliere superiore a 300k #TXS/DAY
    - un numero di wallet superiore ai 22 milioni

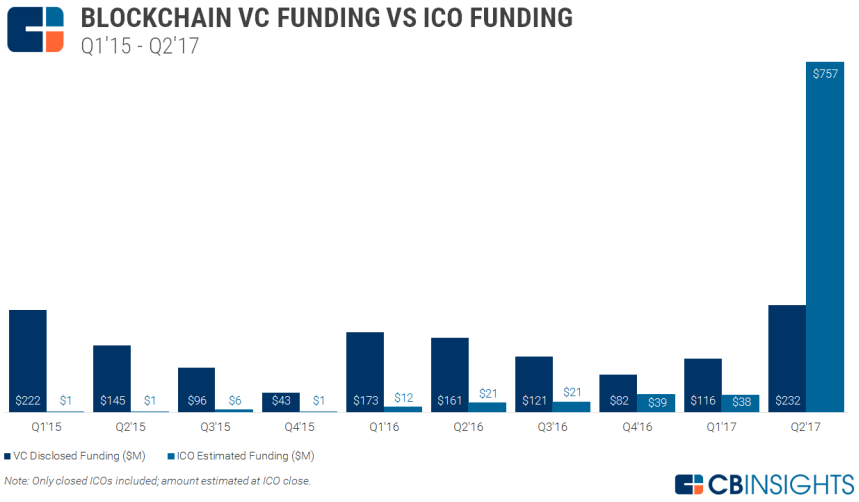
# Initial Coin Offering (ICO): nuova frontiera per raccogliere capitali o bolla speculativa?

- Una delle principali novità degli ultimi anni è costituita da una nuova modalità di emissione delle valute virtuali definita "**Initial Coin Offering**" (ICO)

- La formula delle ICO, se dai creatori è stata classificata come "creazione di valuta virtuale" ha dall'altro suscitato perplessità e preoccupazioni perché **paragonabile** a un **fundraising privo di riferimenti regolamentari** e con **consistenti rischi** per i **consumatori** che vi accedono

- **Dal 2014** sono state **lanciate più di 200 ICO** (di cui 165 nel solo 2017)

- Nei **primi due trimestri del 2017** la **raccolta** tramite ICO ha superato gli **800 Mln di dollari**, contro i circa **350 Mln dei fondi di Venture Capital**; il secondo trimestre in particolare ha visto il sorpasso delle ICO con un raccolta superiore di 3 volte rispetto ai fondi di Venture Capital.




Fonte: https://www.cbinsights.com/research/blockchain-startup-deals-ico-trend/

# Blockchain e cryptocurrencies: il percorso dei Regulators



- In linea generale è stato necessario operare un distinguo tra blockchain e bitcoin/cryptocurrencies perché i **Regulators** potessero **apprezzare le potenzialità della nuova tecnologia**

- Nei giorni scorsi è stato siglato un **accordo di partnerariato tra 22 Paesi UE** per approfondire l'applicazione della blockchain e fare in modo che l'**UE giochi un ruolo chiave in tale ambito**.

- Nel corso degli ultimi anni le banche centrali, le Istituzioni preposte e le autorità monetarie dei diversi Stati o Comunità hanno pubblicato **note e/o avvertenze** con le quali hanno fornito **indicazioni** circa le valute virtuali, i **rischi** e in alcuni casi sono intervenute su **specifici aspetti** per fornire **indicazioni** e/o **pareri.**

- Si segnalano in particolare **la definizione fornita di «valuta virtuale**»** e il **warning** emanato nelle scorse settimane dalle European Supervision Authorities sulle cryptocurrencies

EBA EUROPEAN BANKING AUTHORITY

**** La definizione di Valuta virtuale definita dall'EBA**
"*Rappresentazioni digitali di valore che non sono emesse da una banca centrale o autorità pubblica, né sono necessariamente collegate a una valuta avente corso legale, ma che vengono utilizzate da una persona fisica o giuridica come mezzo di scambio e che possono essere trasferite, archiviate e negoziate elettronicamente.*"

# Conclusioni: verso l'industrializzazione (1/2)

- La **blockchain pubblica** nasce con **l'obiettivo** «**disruptive**» di **disintermediare alcuni players, modificando radicalmente i modelli di business**, ma le diverse industry stanno provando **reinterpretarla**, spesso in una versione DLT/blokchain permissioned, per **cogliere i vantaggi della tecnologia (maggiore efficienza, automazione, interoperabilità)** senza necessariamente modificare radicalmente i modelli di business (anche se il potenziale in questo senso rimane intatto)

- Le iniziative che si basano sulla tecnologia blockchain/DLT riguardano **moltissime industry oltre quella bancaria.** A titolo esemplificativo si citano: insurance, utility e agritech

- I diversi Regulator, ciascuno nel proprio ambito, hanno analizzato e talora provato le nuove tecnologie per comprenderne a fondo le potenzialità

- Cominciano a nascere Progetti cross-settoriali a livello Paese (es. Spagna con Alastria) e partnerariati (i citati 22 Paesi UE)

# Conclusioni: verso l'industrializzazione (2/2)

- Negli ultimi anni si è assistito a una **maturazione** sia della **tecnologia sia della tipologia di iniziative** adottate dai diversi players (si è passati da «studi» a «proof-of-concept» a «piloti»). A titolo meramente esemplificativo solo per l'area di business «Trade Finance» in **ambito R3 ci sono 2 iniziative** che **andranno in produzione tra la fine del 2018 e l'inizio del 2019**.

- L'**adozione progressiva della tecnologia** dipenderà, oltre che dalle diverse industry, da **un'azione auspicabilmente coordinata dei governi**, cosa che pare cominciarsi a palesare. Alcune **precondizioni necessarie all'adozione**:
  - La definizione di un **ampio framework legale**, il più possibile cross-industry e cross-country, coerentemente con il fatto che molte delle aree su cui può essere applicata la tecnologia varcano i confini nazionali (Trade Finance, cross-border payments, capital markets sono solo alcuni ambiti di sperimentazione);
  - Sarebbe molto importante **l'adozione** da parte delle **Pubbliche Amministrazioni** per facilitare il raggiungimento di una massa critica rilevante;
  - **Incentivi economici** all'adozione della blockchain a livello UE e nazionale;
  - **Co-opetition** (in parte già in essere) per la **definizione** di **governance, standards di comunicazione, regole e processi**;
  - La definizione di **prodotti innovativi**, grazie alla maggiore quantità di informazioni disponibili, renderebbe più forti i business plan di tali iniziative.

# THANKS FOR YOUR ATTENTION

**Savino Damico**
**Head of Digital Payments and Biometrics Innovation Department**

✉ savino.damico@intesasanpaolo.com

INTESA SANPAOLO