

# «Blockchain»

**Sebastian Zdrojewski**  
**CEO Rights Chain Ltd.**



**RIGHTS CHAIN**  
Where Digital Artworks are Born

# Il «hype» #blockchain

Nel corso del 2017 la capitalizzazione di mercato totale delle criptovalute è passato da

17,7 mld USD a

612,9 mld USD

# Il «hype» #blockchain

- 86.034 progetti presenti su GitHub
- Una media di 8.603 progetti/anno
- Un picco di 26.885 progetti solo nel 2016
- Solo il 8% dei progetti è attualmente mantenuto
- Vita media: 1,22 anni per progetto
- (fonte: Deloitte)

# Il «hype» #blockchain

*“è la tecnologia che cambierà completamente il settore*

*[settore a piacimento]”*

# La realtà dei fatti

- La tecnologia in sé è complessa (anche per “addetti”)
- Mancanza di framework legali
- Conflitti con normative esistenti
- Il “ledger” pubblico è... pubblico (problemi di privacy)
- Il “ledger” pubblico è anonimo (identity management)
- è immutabile
- è lento
- è collettivamente costoso

# Cosa la rende “nuova”

- è nuova (**2008**)
- è un DB transazionale (**1973**)
- utilizza la tecnologia “peer-to-peer” (**1999**)
- usa lo schema di chiave pubblica e privata o “PKI” (**1976**)
- adotta metodologie di marcatura temporale (**1660**)
- adotta meccanismi di “hashing” (**1992**)
- sfrutta metodologie della Teoria dei Giochi (**1928**)
- introduce il concetto di “Smart Contract” (**1994**)

# Cosa fa “Blockchain”

è un **registro** elettronico che:

- **memorizza** delle informazioni
- le firma digitalmente:
  - attribuisce una data e un autore
- le dispone in modo cronologico
  - rendendo così i dati non alterabili nel tempo
- distribuisce il dato tra tutti i computer che lo compongono

# Un esempio?



Sebastian Konstanty Zdrojewski  
Nato a Lodz, Polonia  
etc. etc. etc.

# Un esempio?

- Attacco informatico
- Guasto irreversibile
- Cancellazione dati
- Distruzione archivi



# Un esempio?



Sebastian Konstanty Zdrojewski  
Nato a Lodz, Polonia  
etc. etc. etc.

# Un esempio?

- Ma se questo dato venisse distribuito?



# Un esempio?

- In caso di perdita totale di un archivio...



# Un esempio?

- In caso di perdita totale di un archivio...



# Tipologie

## **Blockchain pubblico:**

- Ethereum
- Bitcoin
- Principalmente utilizzate per criptovalute
- Prestazioni ridotte e non garantite
- Altissima resilienza (migliaia di nodi)
- Nessun controllo di accesso
- Nessuna validazione di identità

## **Blockchain Privato:**

- Adattabile a diversi ambiti
- Prestazioni elevate
- Resilienza in base alla dimensione
- Controllo di accesso
- Validazione identità possibile

# Qualche «mito»

Ethereum

20.2 TWh

Hungary: 21,55 TWh

(est. 2014 Wikipedia)

Bitcoin

73.2 TWh

Austria: 69.75 TWh

(est. 2015 Wikipedia)

# Cosa non è Blockchain

- non ha interazione con il mondo esterno
- non ha meccanismi di **controllo della qualità** del dato inserito
- **non sostituisce** (né lo farà) un database tradizionale
- non è la soluzione a «**qualsiasi**» problema
- non ha meccanismi di tutela della «**privacy**»

# Qualità

- integrità dei dati controllata da ogni «ledger»
- i dati non possono essere alterati o manomessi
- estremamente resiliente

Il che rende la tecnologia interessante per ambiti come:

- controllo della governance
- conservazione a lungo termine di (meta)dati
- sistemi di «audit»

**#blockchain**

*“è la tecnologia che cambierà completamente il settore  
[settore a piacimento]”*

# Thank You

## SEBASTIAN ZDROJEWSKI

/in/en3py (linkedin)

@En3pY (Twitter)

s.zdrojewsk@rightschain.net