Blockchain e *Criptovalute*: nasce l'*Internet* del valore

Francesco Fabris
Dipartimento di Matematica e Geoscienze

Circolo Matematico 2018/19

25 gennaio 2019

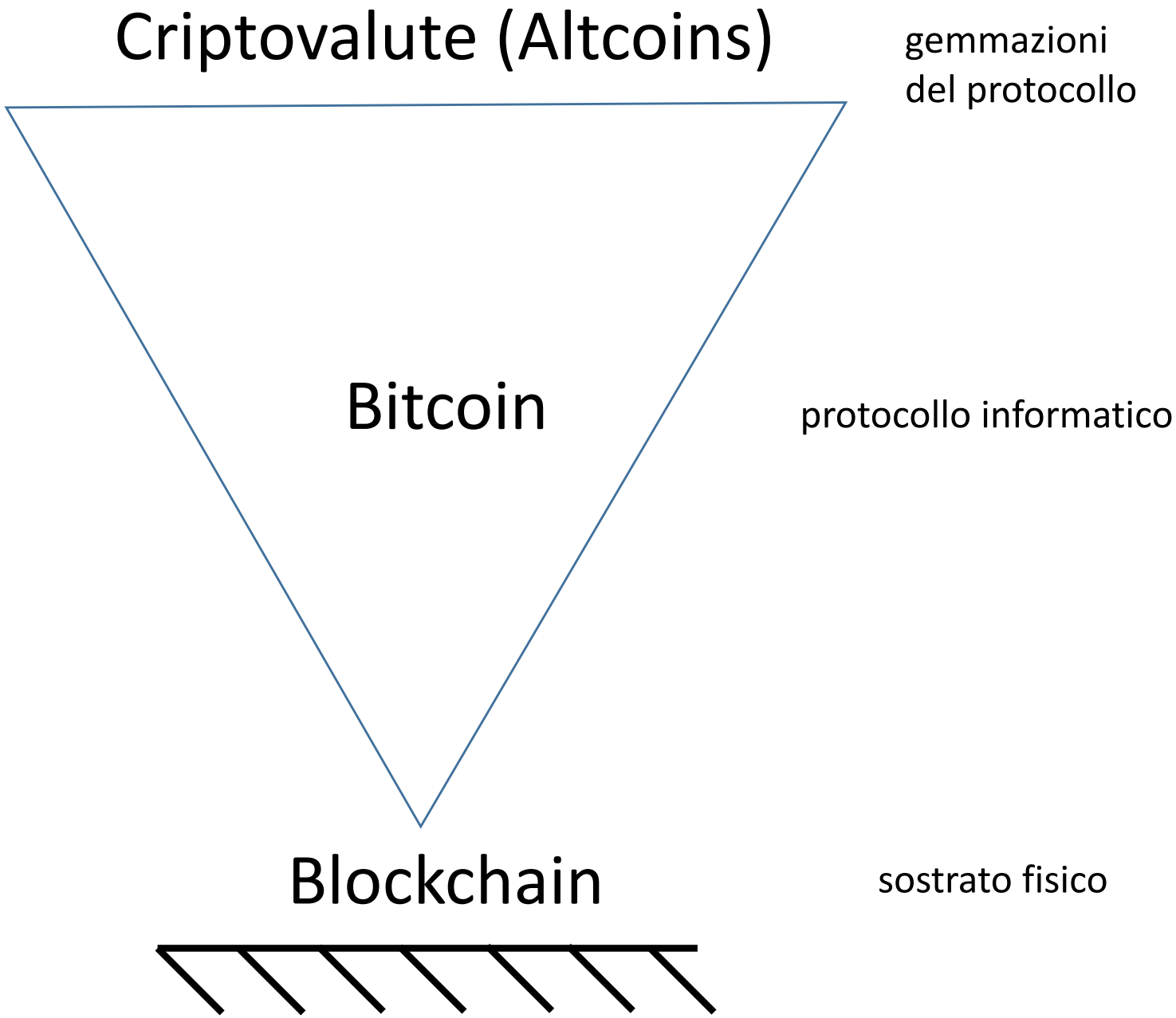
15:15 - 17:00 Aula Morin

Oggi parleremo di un’applicazione della *crittografia* e delle *firme numeriche*

la Blockchain

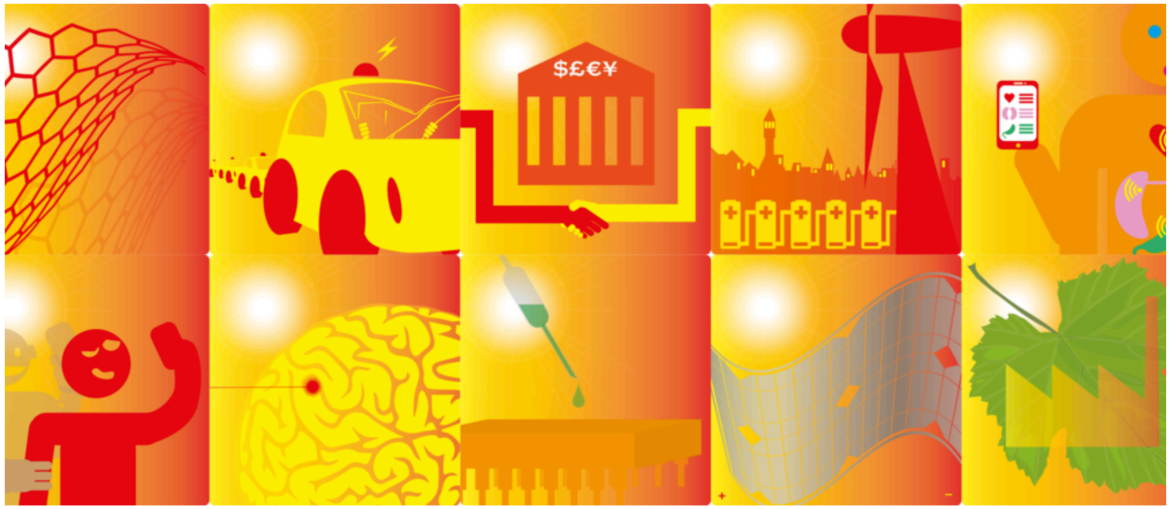
il Bitcoin

le criptovalute


Criptovalute (Altcoins)
gemmazioni
del protocollo
Bitcoin
protocollo informatico
Blockchain
sostrato fisico

WORLD ECONOMIC FORUM

These are the top 10 emerging technologies of 2016



3. The Blockchain

Much already has been made of the distributed electronic ledger behind the online currency Bitcoin. With related venture investment exceeding $1 billion in 2015 alone, the economic and social impact of blockchain's potential to fundamentally change the way markets and governments work is only now emerging.

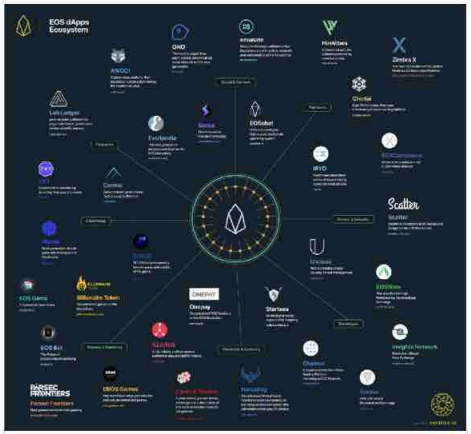
L’evoluzione del Web

Web 1.0	➔	biblioteca globale (file di testo, siti web poveri e intesi come deposito di dati)
Web 2.0	➔	uso di immagini, video e di social media (file complessi e interattività)
Web 3.0	➔	banca digitale globale (trasmissione del valore, con dati monetizzabili grazie all’introduzione delle criptovalute)

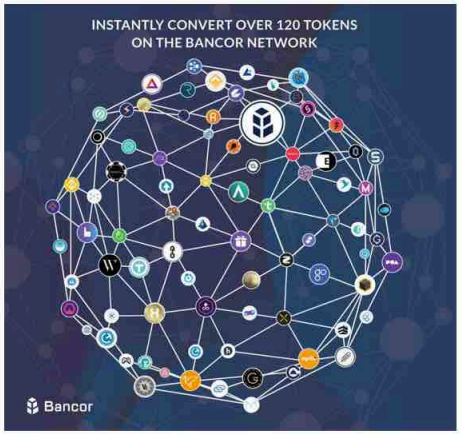
I LIVELLO DI ANALISI: L’ECOSISTEMA COMPLESSIVO

II LIVELLO DI ANALISI: LA STRUTTURA DEL BITCOIN

I LIVELLO DI ANALISI: L’ECOSISTEMA COMPLESSIVO



Rete EOS



Rete Bancor

Bancor X protocol

Rete Ethereum

Saturday, September 30, 2017

IMF Head Foresees the End of Banking and the Triumph of Cryptocurrency

Bitcoin "puts a question mark on the fractional banking model we know today."

Christine Lagarde

Jim Reid

Deutsche Bank Strategist Says End of Fiat-based Currency Systems Near, Recommends Bitcoin


“You should be taking this technology as seriously as you should have been taking the development of the Internet in the early 1990s. ”
Blythe Masters, CEO of Digital Asset Holdings and former CFO of J.P. Morgan's Investment Bank

Problema centrale nel trasferimento di valore: problema della doppia spesa

cioè spedere due volte la stessa quantità di denaro - con i bit è possibile

Tradizionalmente il problema viene risolto in due modi:

1. transazione di un’entità fisica (contante, cioè monete o banconote)

2. intermediario (banca) che garantisce l’impossibilità della doppia spesa

Col contante c’è il problema dell’impossibilità di trasmetterlo a distanza

Con la banca vi possono però essere altri problemi:

a) la banca può rifiuta una transazione
b) la banca chiede una commissione (anche rilevante) per la transazione
c) la transazione impiega uno (o più giorni) per andare a buon fine
d) manca l’anonimato

Tutto inizia da un manipolo di “nerd”...

- Nell’agosto del 2008 viene registrato il dominio "bitcoin.org"
- Il 31 ottobre dello stesso anno, su una mailing list di crittografi, appare un link a un articolo di tale *Satoshi Nakamoto* dal titolo “*Bitcoin: A Peer-to-Peer Electronic Cash System*”.
- Nakamoto realizza il software *open source* per bitcoin e lo rilascia nel gennaio 2009 su *SourceForge*. Nasce *Bitcoin* (BTC)
- Il primo blocco viene generato nel gennaio 2009
- L’identità di *Satoshi Nakamoto* rimane avvolta da mistero

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

31 October 2008

Initial release 0.1.0 / 9 Gennaio 2009 (9 anni fa)
Latest release 0.17.1 / 25 Dicembre 2018 (2 mesi fa)

"I JUST WANT to report that I successfully traded 10.000 bitcoins for pizza" (circa 41$ all'epoca)
scrisse l'utente *laszlo* sul *Bitcoin forums* nel Maggio 2010

ora quella pizza costerebbe 35 mln $!!

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must