MODULO 1. CAPIRE BITCOIN

La storia, le origini e la filosofia

Villaggio Bitcoin

Corso base su Bitcoin

Villaggio**Bitcoin**

Modulo 1

Modulo 2

Modulo 3

Modulo 4

CAPIRE BITCOIN

" Ma spiegami in due parole...

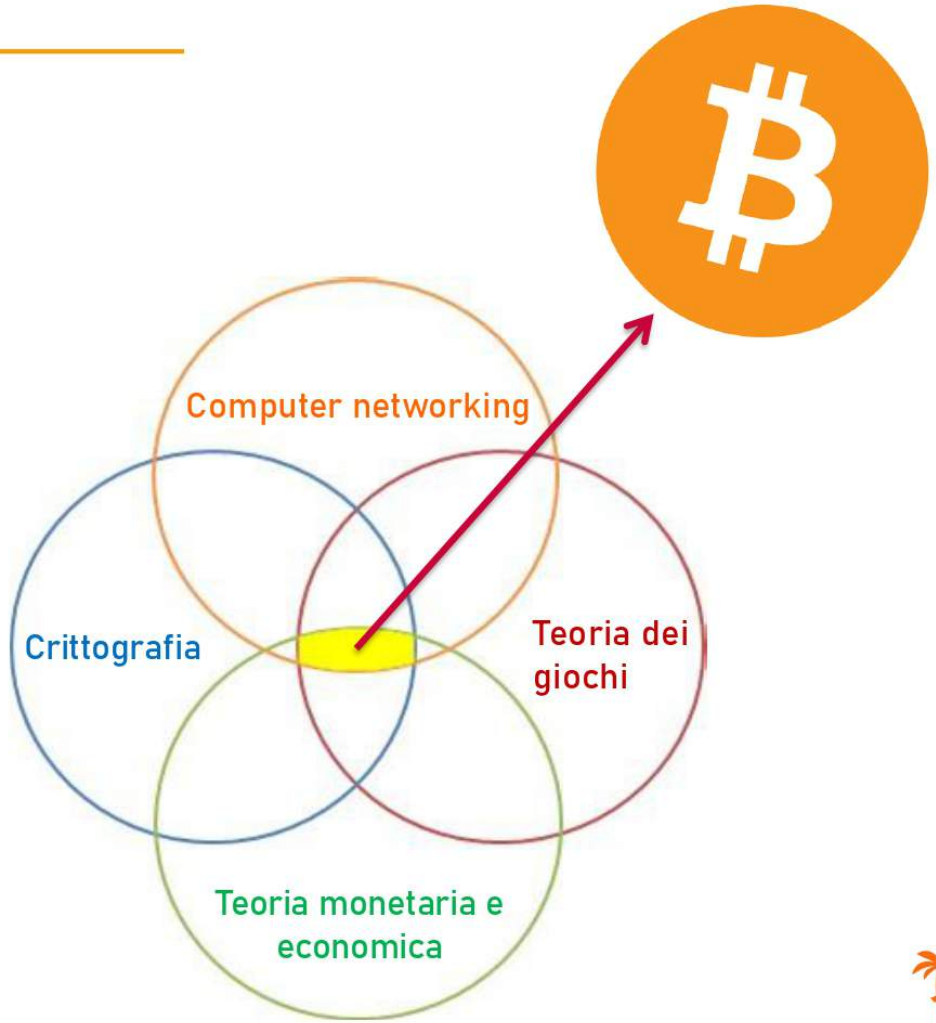
cosa sono questi *bitcoin* ?? "

Villaggio**Bitcoin**

CAPIRE BITCOIN

4 ambiti principali:

- *Crittografia*
- *Computer networking*
- *Teoria dei giochi*
- *Teoria monetaria e economica*



Villaggio Bitcoin

CAPIRE BITCOIN

Moneta

3 funzioni:

1. *Riserva di valore*
2. *Mezzo di scambio*
3. *Unità di conto*

Villaggio**Bitcoin**

LA MONETA: LE ORIGINI

- Baratto → Pietre, perline, sale, conchiglie, falci, pecore, …
- Oro, Argento, rame, metalli… ←

Villaggio Bitcoin

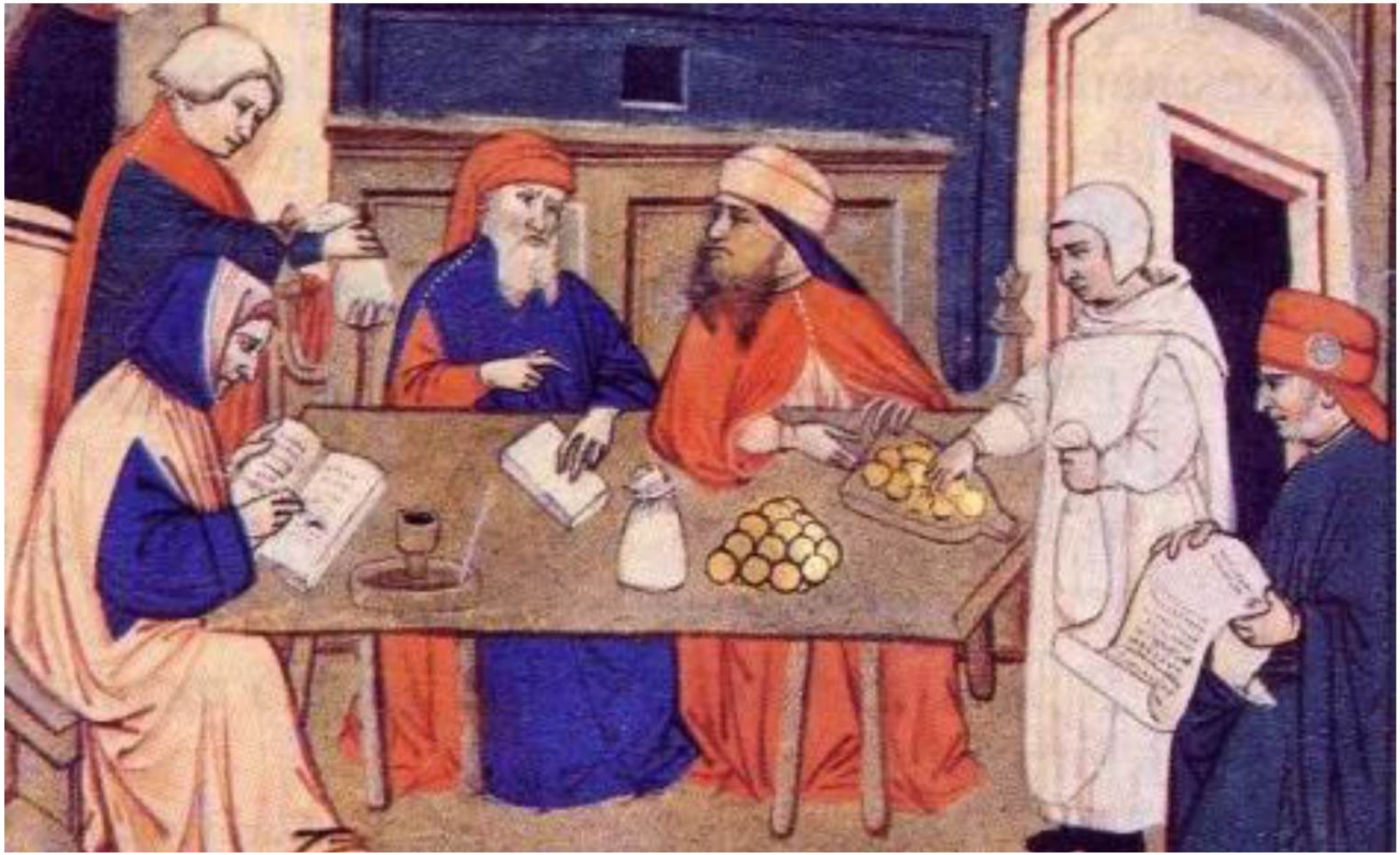
LE ORIGINI: L'ORO

- ✓ Resistenza a deterioramento
- ✓ Facile da verificare
- ✓ Scarsità
- ✓ Difficile da riprodurre

- ❖ Verifica non immediata
- ❖ Difficile da dividere
- ❖ Trasporto e sicurezza

Villaggio**Bitcoin**

Moneta rappresentativa



Villaggio Bitcoin

LA MONETA: LE ORIGINI

- Baratto
- Pietre, perline, sale, conchiglie, falci, pecore, …

- Oro, Argento, rame, metalli…

- Moneta rappresentativa

Villaggio Bitcoin

Riserva frazionaria

Emissioni di più banconote rispetto alle scorte esistenti

Villaggio**Bitcoin**

LA MONETA: LE ORIGINI

- Baratto
- Pietre, perline, sale, conchiglie, falci, pecore, …

- Oro, Argento, rame, metalli…

- Moneta rappresentativa

- Riserva frazionaria
- Denaro di Stato (Fiat Money), a corso legale

Villaggio Bitcoin

Moneta fiat

Gold Standard

1971: «*Nixon Shock*»

Creazione moneta dal nulla

«*Moneta fiat*»

Signoraggio bancario

Riserva frazionaria

Villaggio**Bitcoin**

Moneta fiat

Chi siamo

Alla Banca centrale europea (BCE) lavoriamo per mantenere stabili i prezzi nell'area dell'euro. Così anche in futuro potrai acquistare con lo stesso denaro gli stessi beni e servizi che ti puoi permettere oggi.

Inoltre contribuiamo alla sicurezza e alla solidità del sistema bancario europeo, per fare in modo che i tuoi soldi in banca siano al sicuro.

Manteniamo i prezzi stabili e il tuo denaro al sicuro

Banca Centrale Europea

Inflazione dilagante

Continui fallimenti bancari

Villaggio Bitcoin

FIAT MONEY

€uro

- Sicurezza basata su carta e fiducia
- Moneta inflazionistica (perde valore nel tempo)
- Governance stabilita dal governatore
- Signoraggio a banchiere centrale
- Autorizzazione e tracciamento
- Costi di servizio e burocrazia

Debito pubblico mondiale

Oltre 315 TRILIONI $

3,3 volte il PIL mondiale

+18% rispetto al 2020
258.000.000.000.000 $

+50% rispetto al 2013 (!)
210.000.000.000.000 $

Fonte: Institute of International Finance (IIF)

Villaggio**Bitcoin**

FIAT MONEY

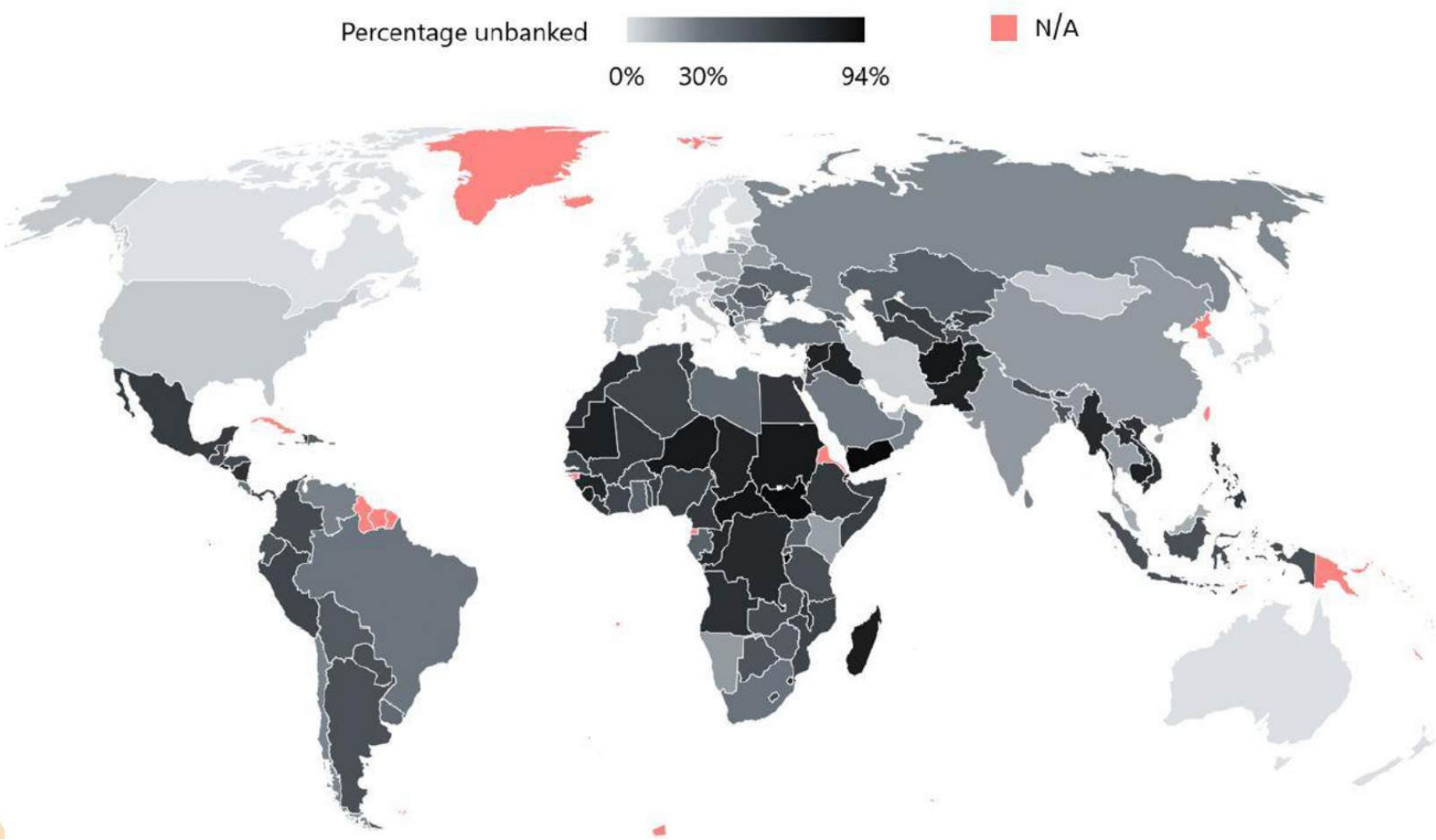
€uro

Almeno 4 criticità:

- Centralizzazione finanza (fiducia)
- Esclusione sociale (*unbanked*)

Villaggio**Bitcoin**

FIAT MONEY



Villaggio Bitcoin

FIAT MONEY

€uro

Almeno 4 criticità:

- Centralizzazione finanza (fiducia)
- Esclusione sociale (*unbanked*)
- Privacy e controllo
- Distribuzione poteri e privilegi

Villaggio Bitcoin

Cosa non va oggi?

Exit Strategy

Scuola Austriaca di Economia

Movimento Chyperpunk

Villaggio Bitcoin

BITCOIN: LE ORIGINI

Teorie Keynesiane

- Ruolo Banca Centrale
- Regolazione tassi interesse
- Inflazione al 2%
- Spesa aggregata e PIL
- Consumismo e indebitamento

≠

Scuola Austriaca di Economia

- Assenza di un pianificatore centrale
- Monete in concorrenza
- Sistema dei prezzi
- Risparmio e scarsità risorse

Villaggio**Bitcoin**

La Scuola Austriaca di Economia

L'economia è una scienza sociale

- Teoria marginale del valore
- L'azione umana il punto di partenza
- Libero mercato e concorrenza tra forme di denaro

Villaggio Bitcoin

Exit strategy?

NON CREDO CHE POTREMO DISPORRE DI UNA MONETA SANA E ONESTA SENZA PRIMA AVERLA TOLTA DALLE MANI DEI GOVERNI.

SE NON POSSIAMO CON LA VIOLENZA, DOBBIAMO INVENTARCI UNO STRATAGEMMA, INTRODUCENDO QUALCOSA CHE LORO NON POSSONO FERMARE.

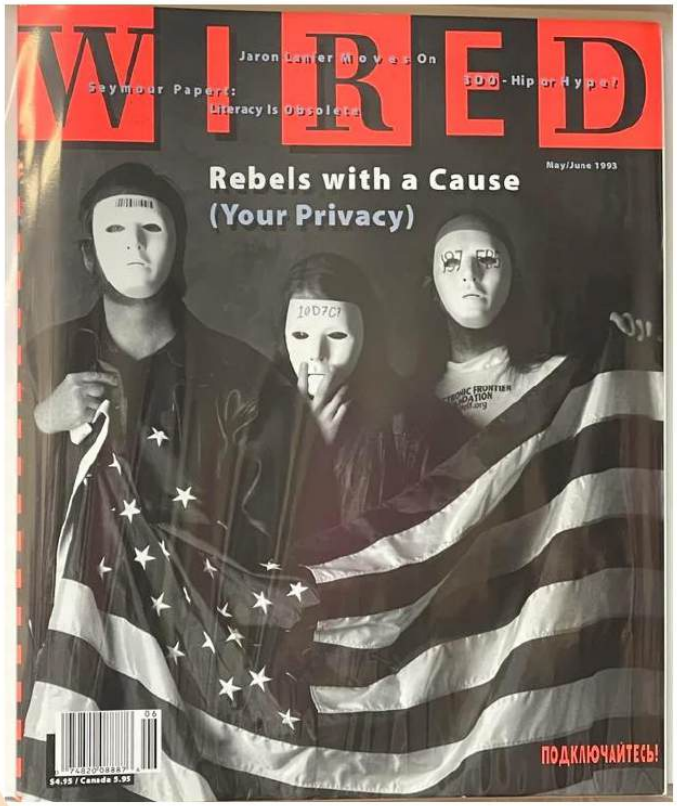
Friedrich Von Hayek - 1984

Nobel per l'Economia nel 1974
Esponente Scuola Austriaca di Economia

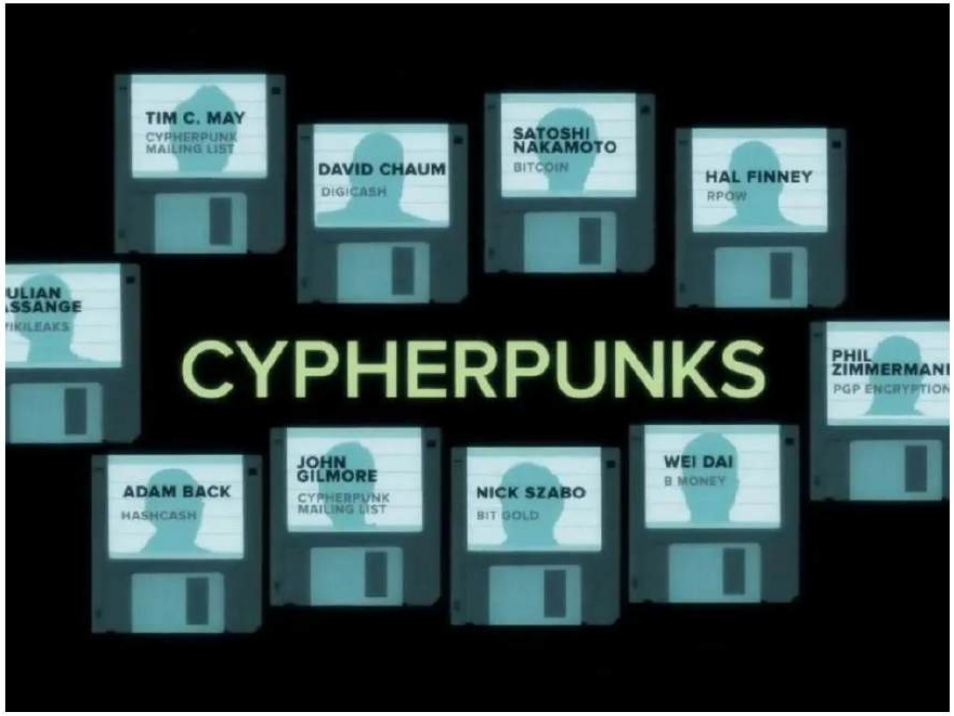
Villaggio**Bitcoin**

BITCOIN: PERCHÉ?

Cripto-anarchia



Movimento Cypherpunk



Villaggio Bitcoin

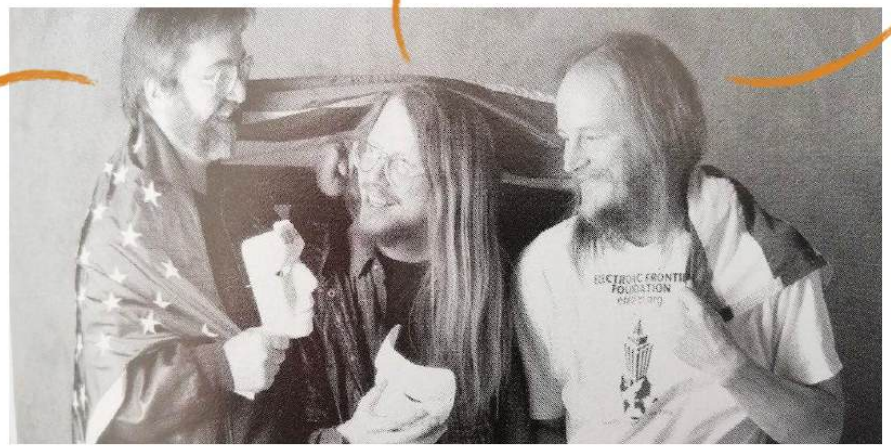
BITCOIN: PERCHÉ?

Movimento Cripto-anarchico

Eric Hughes

John Gilmore

Timothy C. May



”

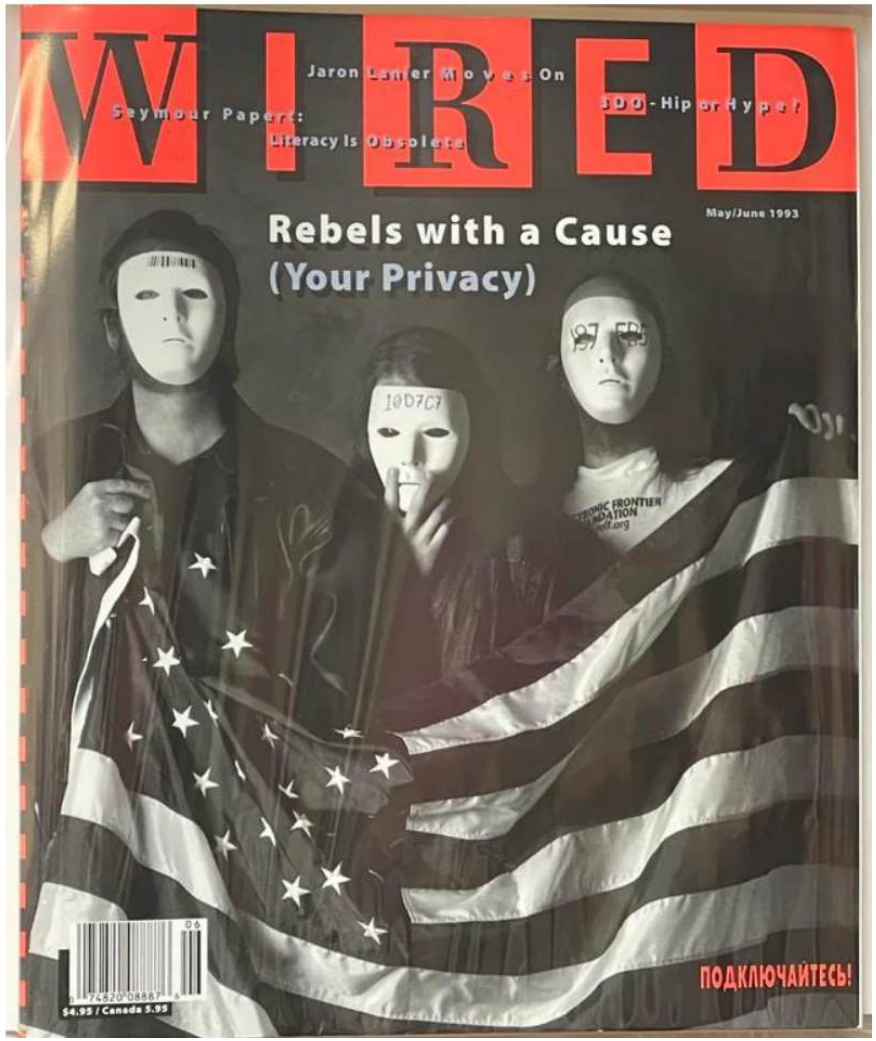
Uno spettro sta emergendo nel mondo moderno, lo spettro dell'anarchia crittografica. L'informatica è sul punto di fornire la possibilità a individui e gruppi di comunicare e interagire tra loro in modo completamente anonimo.

”

La tecnologia per questa rivoluzione esiste nella teoria dall'ultimo decennio. E sicuramente sarà una rivoluzione sociale ed economica.

Villaggio Bitcoin

BITCOIN: PERCHÉ?



«The Crypto Anarchist Manifesto»

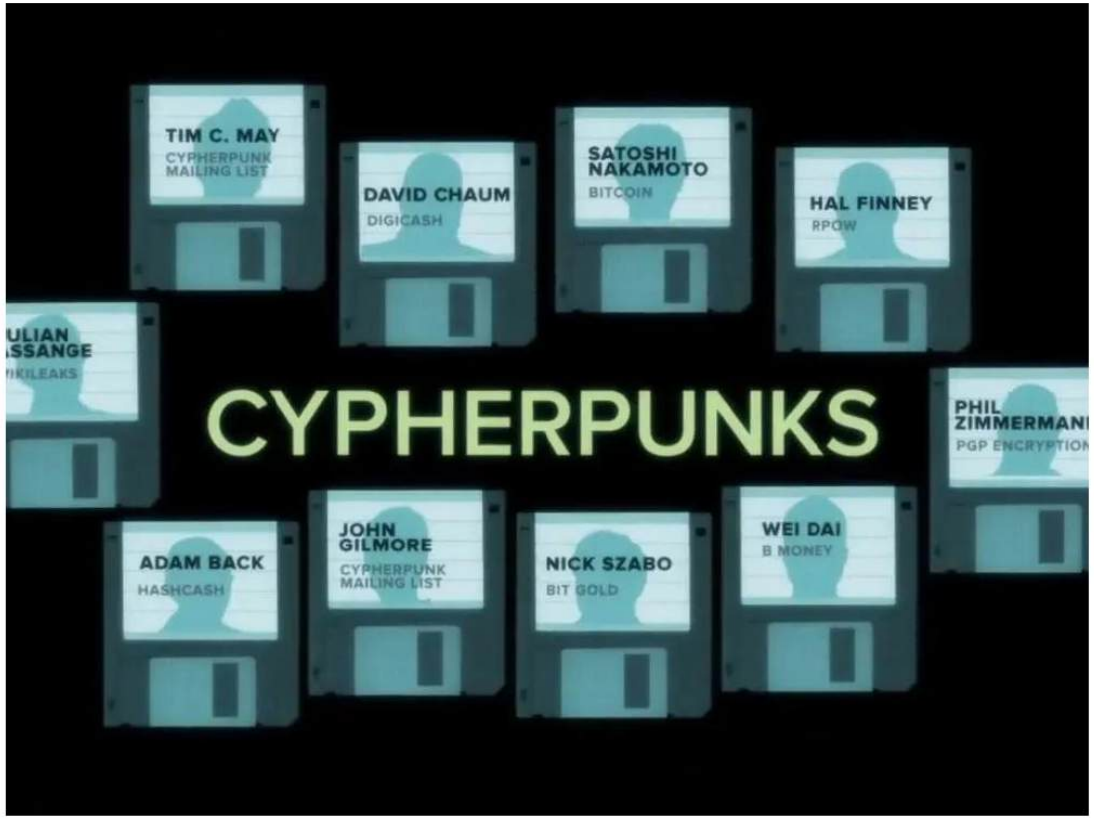
Timothy C. May (1988 e pubblicato nel 1992)

- Focus sulla Privacy
- Anonimato tramite crittografia
- Libertà economica e politica
- Libero mercato

Villaggio Bitcoin

BITCOIN: LE ORIGINI

MOVIMENTO CYPHERPUNK



Villaggio**Bitcoin**

MOVIMENTO CYPHERPUNK

PRIVACY MONEY

- E-cash (1983, **David Chaum**) e Digicash (1989)
- HashCash (**Adam Back**, 1997)
- B-Money (**Wei Dai**, 1998)
- Bit Gold (**Nick Szabo**, 1998)
- *E-gold* (**Douglas Jackson**, 1996-2007)
- RPOW (**Hal Finney**, 2004)

e-gold

Villaggio Bitcoin

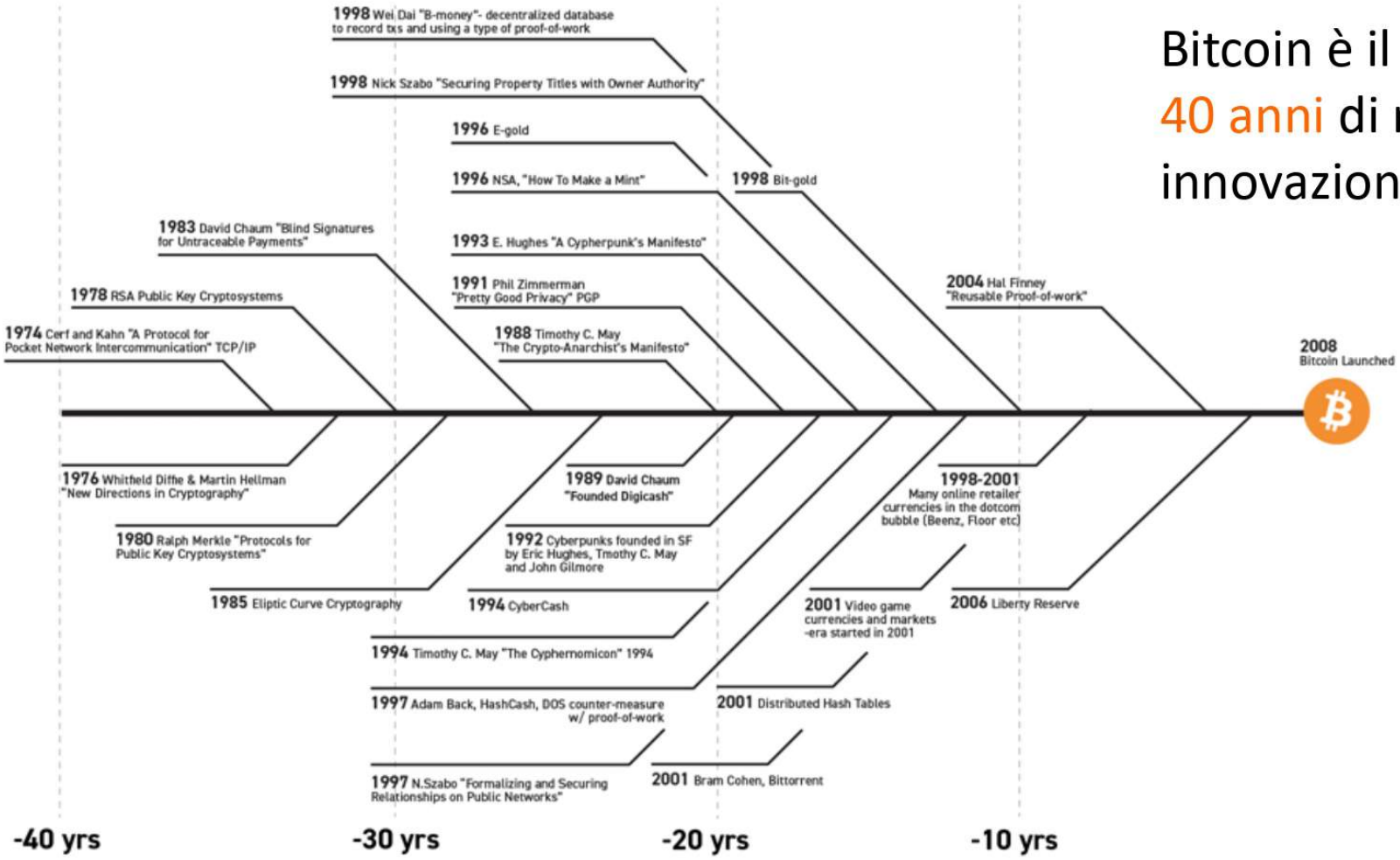
BITCOIN: PERCHÉ?

*«La **Privacy** è necessaria per una società aperta nell'era digitale. Non possiamo aspettarci che i governi, le aziende o altre grandi organizzazioni senza volto ci concedano la privacy.*
***Dobbiamo difendere** la nostra privacy»*

[...]

*«Noi Cypherpunks scriviamo codici. Difendiamo la nostra privacy con la **crittografia**, con sistemi di email anonimi, **firme digitali** e **monete elettroniche.***
Siamo attivamente impegnati a rendere le Reti informatiche (come Internet) più sicure per la Privacy.
*Il nostro codice è **gratuito per tutti**, in tutto il mondo.»*

BITCOIN: LE ORIGINI



Bitcoin è il risultato di 40 anni di ricerche, innovazioni e contributi

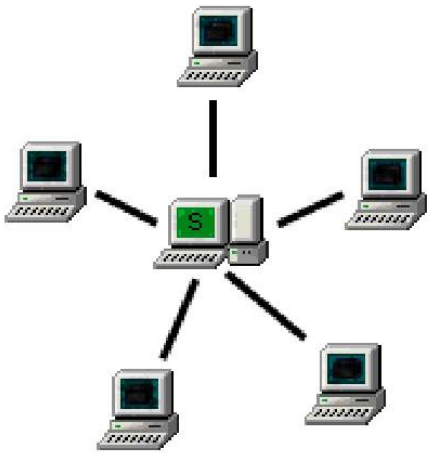
Villaggio Bitcoin

BITCOIN: LE SFIDE TECNOLOGICHE

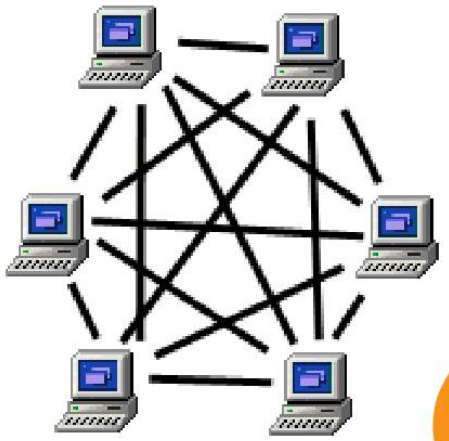
- **Server-based network**
- Software proprietario
- Profilazione utenti

napster

PayPal



- **Peer to peer** (p2p)
- Software Open Source
- Nessuna registrazione



BitTorrent™

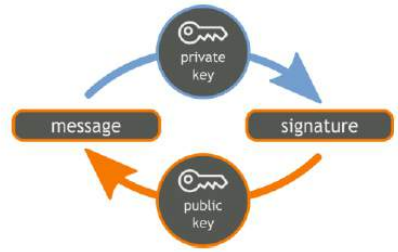
Villaggio Bitcoin

BITCOIN: LE SFIDE TECNOLOGICHE

- Chi firma a autorizza le transazioni?

FIRMA DIGITALE

Crittografia asimmetrica



- Quale moneta di scambio?

PROVA DI LAVORO

Scarsità in ambito digitale

- Come ordinare nel tempo le transazioni?

BLOCKCHAIN

Risoluzione double-spending

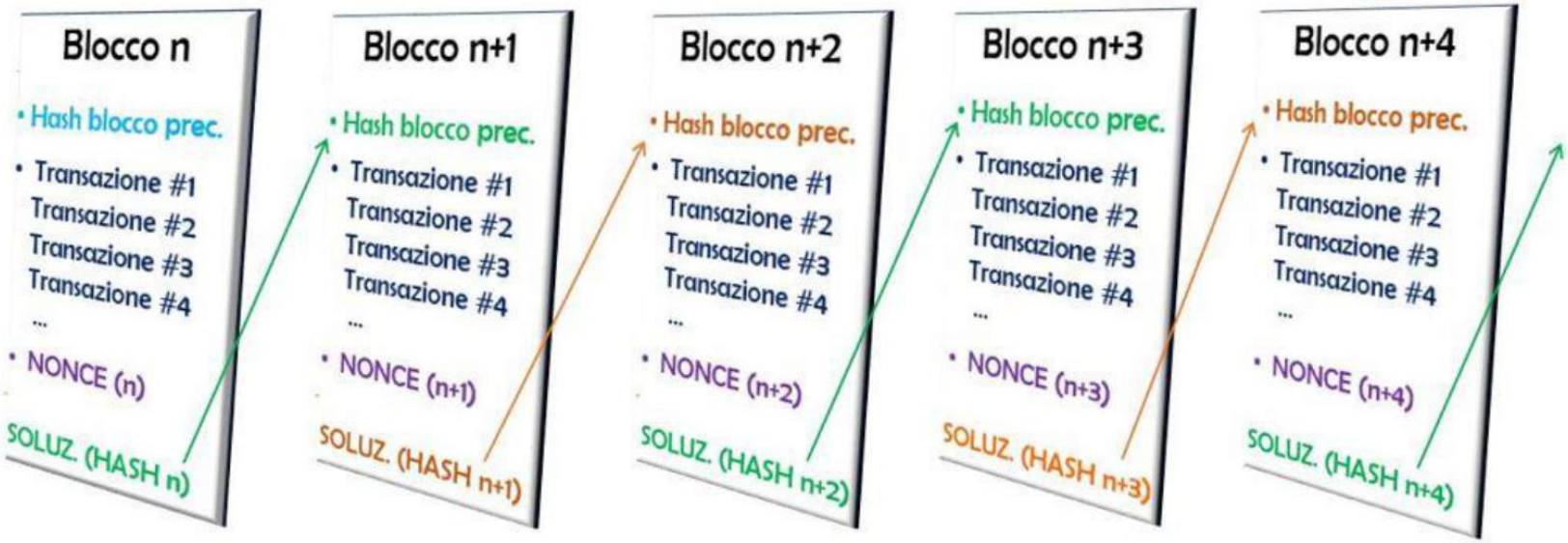
Villaggio Bitcoin

BITCOIN: LA BLOCKCHAIN

Risoluzione problema double-spending

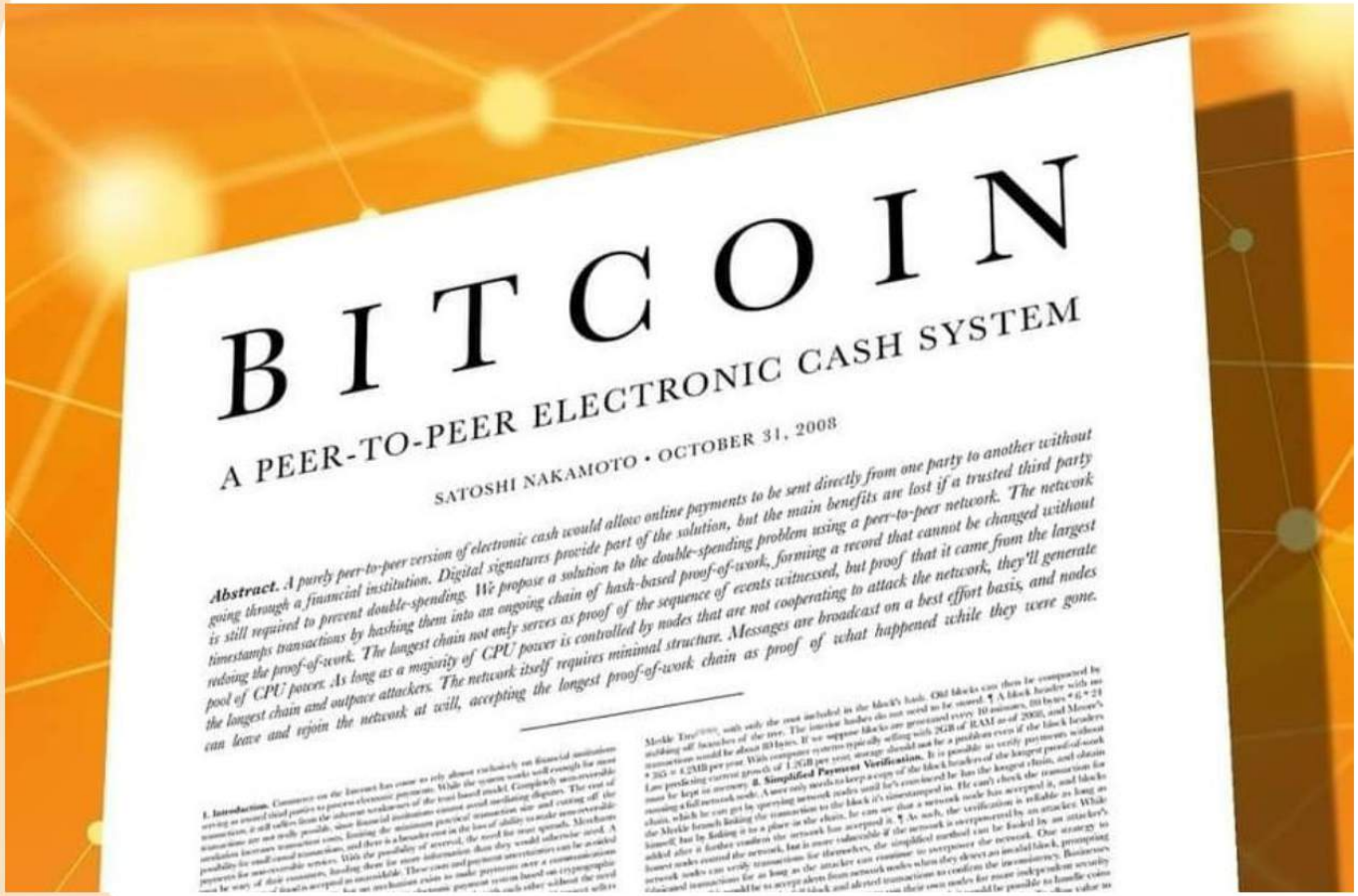
- Libro mastro delle transazioni
- Catena di blocchi legati crittograficamente
- Ordine cronologico condiviso

CONSENSO DISTRIBUITO



Villaggio Bitcoin

BITCOIN WHITE PAPER



BITCOIN

A PEER-TO-PEER ELECTRONIC CASH SYSTEM

SATOSHI NAKAMOTO • OCTOBER 31, 2008

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.*

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

31 ottobre 2008

https://bitcoin.org/files/bitcoin-paper/bitcoin_it.pdf

- Proposta di risoluzione problema double-spending
- Importanza privacy
- Focalizza il problema sulla fiducia in un intermediario

Villaggio **Bitcoin**

BITCOIN GENESIS BLOCK


THE TIMES

£1.50

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Israel prepares to send tanks and troops into Gaza

Michael Sheen Frost, Nixon and me

Working mums So that's how she does it

Detox in style The best spas on the planet

Giant killing? Guide to the FA Cup third round

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

99p

03 gennaio 2009

- Bitcoin lanciato in produzione
- Autenticità data
- Messaggio politico

Villaggio Bitcoin

BIT QUOTE

”

Il problema alla base delle valute convenzionali è dovuto alla quantità di fiducia necessaria per far funzionare il sistema.

Dobbiamo fidarci del fatto che le banche non svalutino la moneta, ma purtroppo la storia è piena di momenti in cui questa fiducia non è stata rispettata.

Dobbiamo fidarci del fatto che le banche conservino i nostri soldi, ma spesso sono scoppiate bolle legate al credito bancario, e solo una frazione dei soldi era effettivamente in possesso della banca.

Satoshi Nakamoto – 11 febbraio 2010

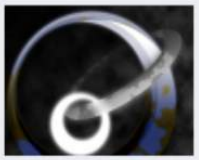
Anonimo inventore di Bitcoin

Villaggio**Bitcoin**

SATOSHI NAKAMOTO

HostFat
Staff
Legendary

Activity: 2492



I support freedom of choice

Ignore

Re: Website translations
May 27, 2010, 11:03:36 AM

Here there is the italian translation of the software.
There can be some mistakes, but it's just ok for the first version
I hope that someone will come to do something better.

Eternity Wall: Messages lasting forever - **The Rock Trading** (ref): A good exchange / gateway Ripple, with support for multisig, since 2007.
https://bitcointa.lk: Bitcointalk backup if offline - **Bitcoin Foundation Italia** - **Blog:** http://theupwind.blogspot.it

satoshi
Founder
Sr. Member

Activity: 364

Re: Website translations
May 27, 2010, 02:18:22 PM

Hurray! We have our first language. I uploaded it to SVN to go in with the 0.3 release.

Villaggio**Bitcoin**

BITCOIN: la community

Bitcoin Pizza Day

- Prima transazione commerciale
- 10,000 bitcoin

Villaggio Bitcoin

BITCOIN: gli exchange

MT.GOX

- Hacking e fallimento
- Not your key, not your coins!

Villaggio Bitcoin

BITCOIN OGGI

Il percorso verso l'adozione di massa

- «Brand mondiale»
- Adozione in crescita
- Conferenze internazionali
- Stati e città
- Ucraina e Russia
- Investitori e imprese

Villaggio Bitcoin

BITCOIN OGGI

Hedge fund: esempi

Michael Saylor (2018):
«Se intendi investire in Bitcoin, un orizzonte temporale breve è 4 anni, un orizzonte temporale medio è 10 anni e l'orizzonte temporale corretto è *per sempre*»

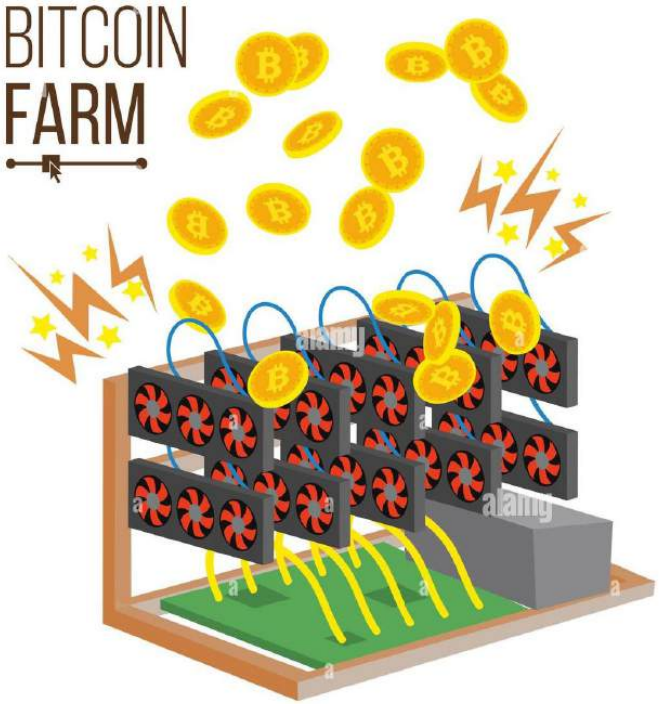
Larry Fink (2024):
«Bitcoin potrebbe rivoluzionare il sistema finanziario, è oro digitale»
«Un asset internazionale che non è ancorato a nessuna valuta tradizionale»
«Bitcoin è un'alternativa all'oro come riserva di valore»

Villaggio Bitcoin

BITCOIN OGGI

Mining

- Industria in continua crescita.
- Hash rate ATH
- Emissione nuovi bitcoin
- Sicurezza infrastruttura



Villaggio Bitcoin

BITCOIN OGGI

El Salvador

- Moneta a corso legale
- Primo caso studio

Villaggio Bitcoin

IL PERCORSO DI ADOZIONE

BITCOIN OGGI

Lugano

CORSO LEGALE «DE FACTO»

- Hub di ricerca e sviluppo
- Finanziamenti per educazione
- Investitori, start-up e capitali

Villaggio Bitcoin

BITCOIN OGGI

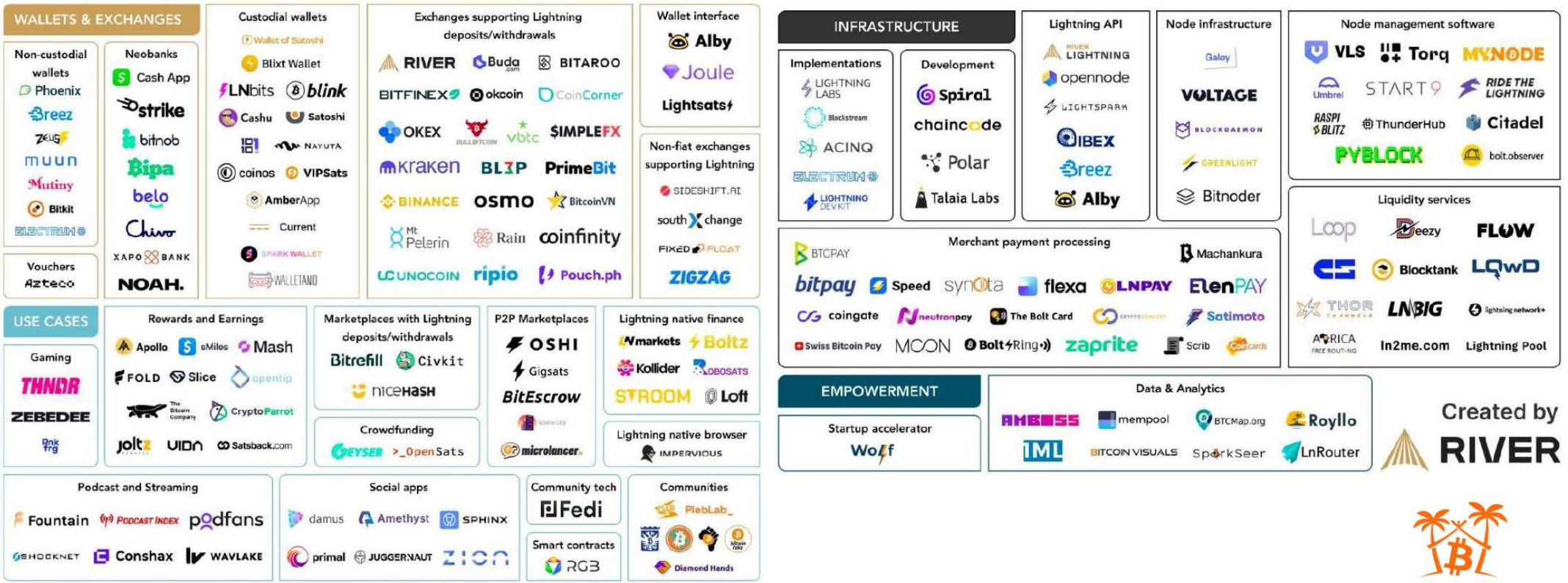
Bitcoin e Lightning Network

- Layer 2 di Bitcoin
- Pagamenti istantanei, confidenziali, sicuri e gratuiti.
- Soluzione al problema della scalabilità.

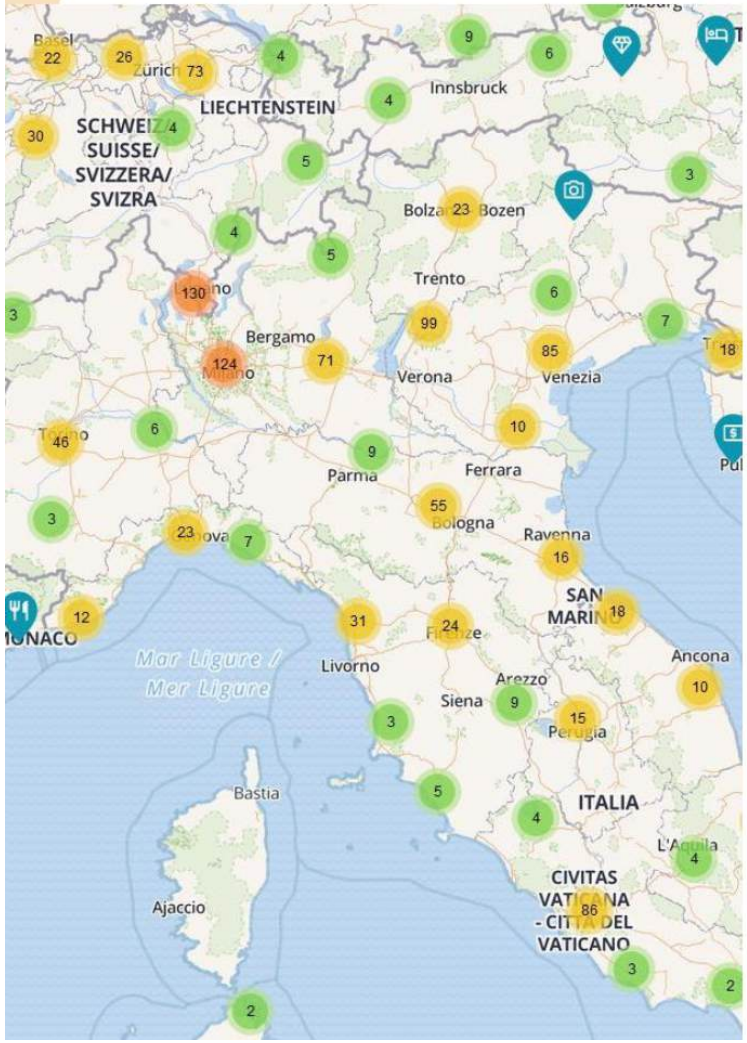
Villaggio**Bitcoin**

BITCOIN OGGI

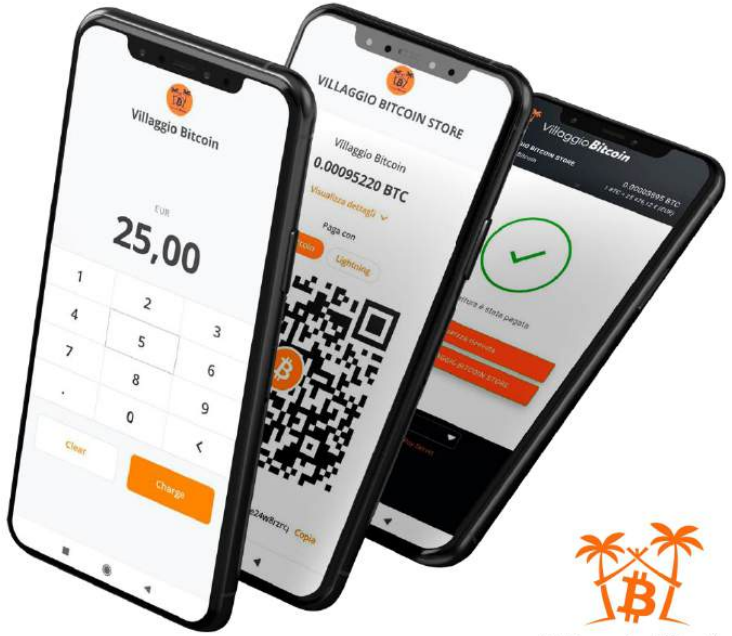
Un nuovo ecosistema



BITCOIN OGGI



- Attività che accettano pagamenti in btc
- Community in continua crescita
- BTCMap



Villaggio**Bitcoin**

Tecnologie a confronto

€uro

- Sicurezza basata su carta e fiducia
- Moneta inflazionistica (progettata per perdere valore nel tempo)
- Politica stabilita arbitrariamente dal governatore (fiducia)
- Signoraggio a banchiere centrale
- Autorizzazione e Tracciamento
- Costi di servizio e burocrazia
- Imposta a corso legale (o «forzoso»)

₿itcoin

- Basata su **matematica** e **crittografia**
- Moneta **deflazionistica** (progettata per *non* perdere valore nel tempo)
- Governance stabilita da **algoritmo** pubblico e trasparente (no fiducia)
- Signoraggio **distribuito nel network**
- Permissionless e **Privacy**
- Nessun costo e **zero** burocrazia
- Adozione **volontaria**

Villaggio**Bitcoin**

LA MONETA BITCOIN

~~**Trading, speculazioni finanziarie e tentativo di arricchirsi**~~

≠

Strumento di cooperazione sociale, gratuito, libero e inclusivo

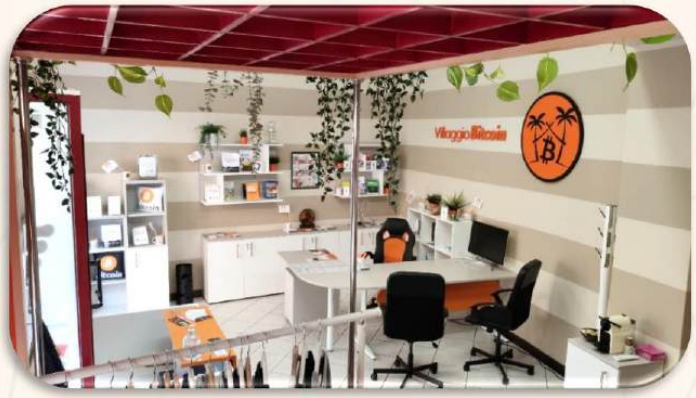
Villaggio**Bitcoin**

MODULO 1. CAPIRE BITCOIN

La storia, le origini e la filosofia

Villaggio**Bitcoin**

Villaggio Bitcoin



www.villaggiobitcoin.it

351 6755119

info@villaggiobitcoin.it

t.me/villaggiobitcoin

Corso base su Bitcoin

Villaggio**Bitcoin**

Modulo 1

Modulo 2

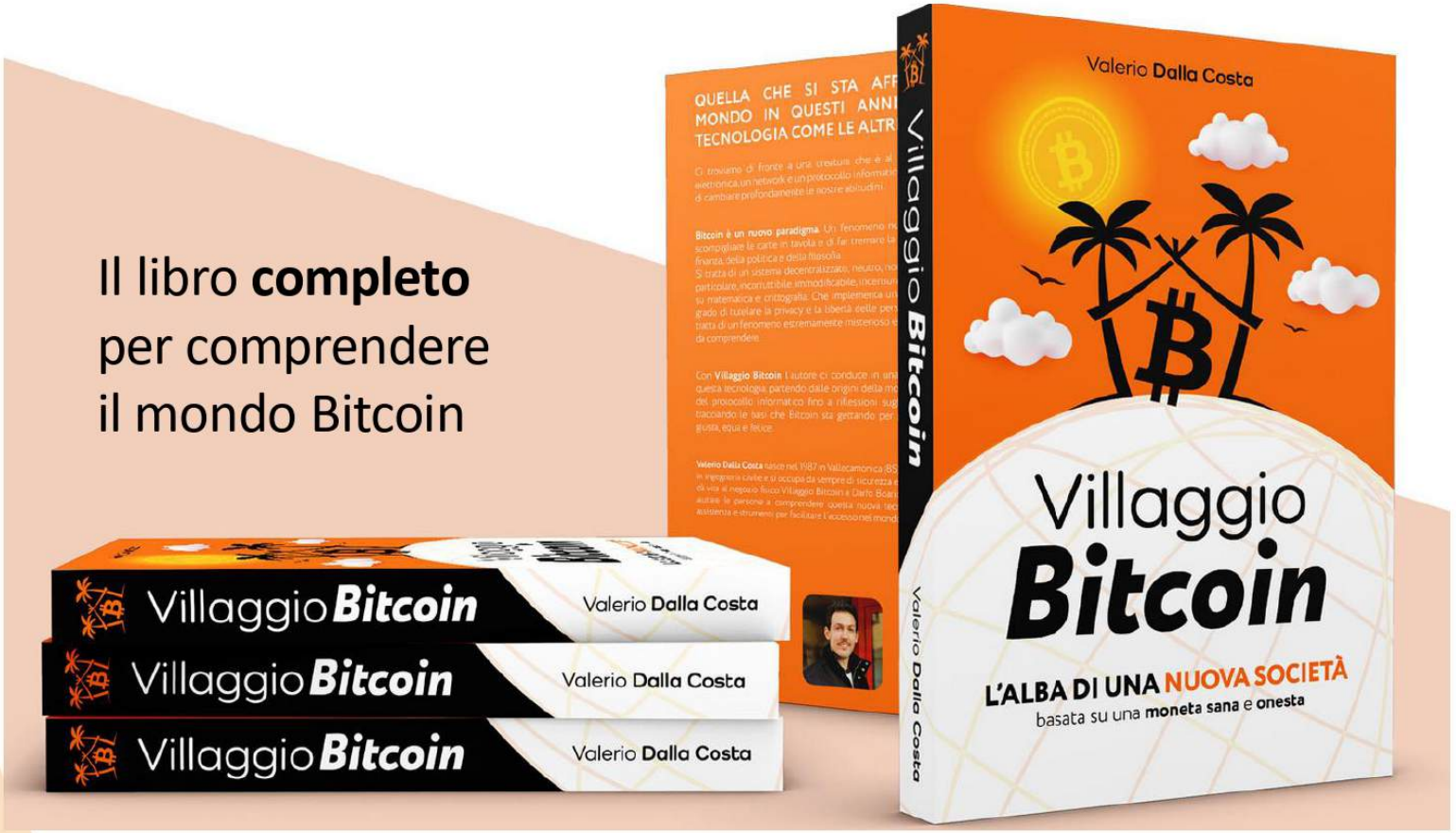
Modulo 3

Modulo 4

Bitcoin book

Villaggio Bitcoin

Il libro **completo**
per comprendere
il mondo Bitcoin



AVAILABLE ON:

amazon

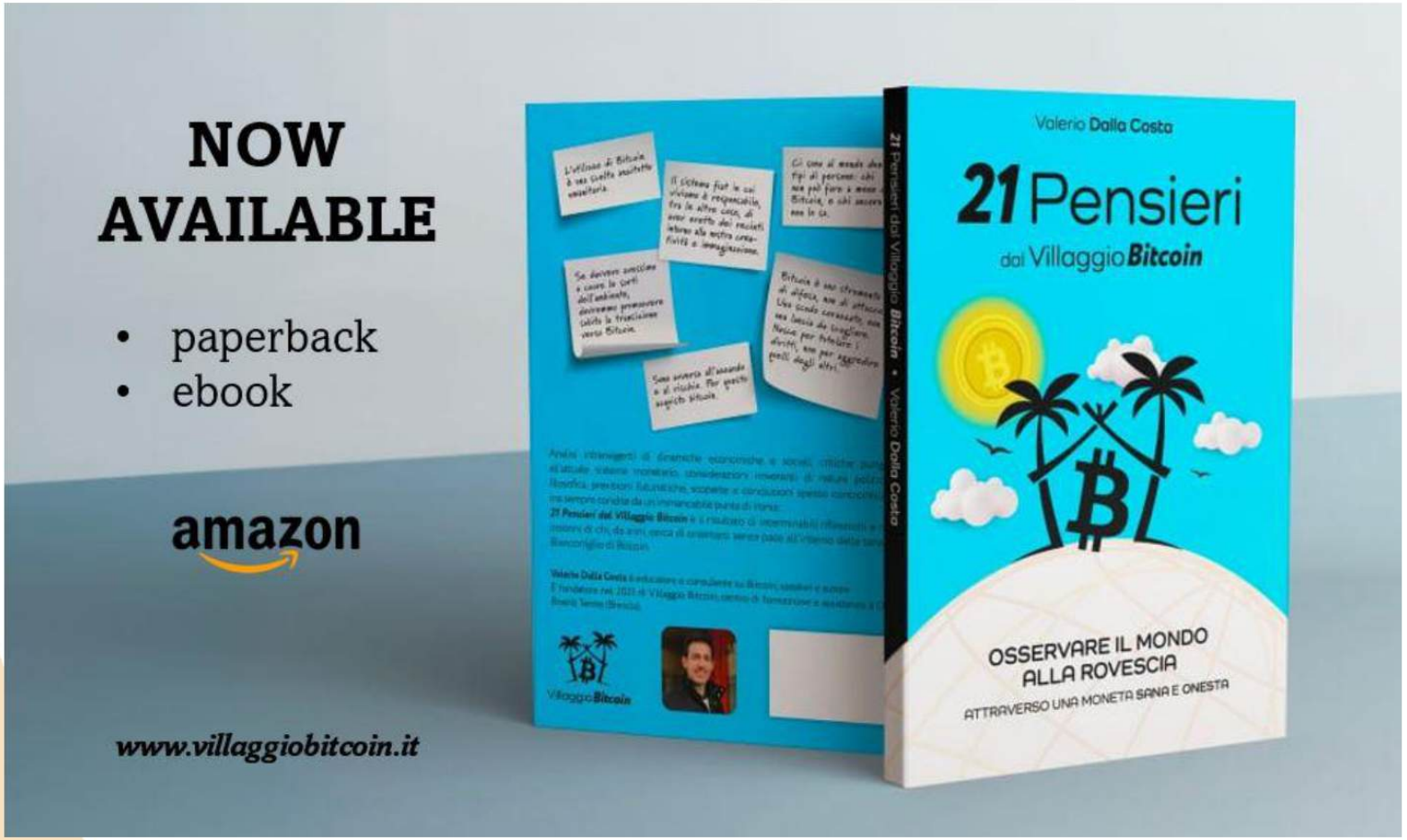
USEMLAB
ECONOMIA E MERCATI

VillaggioShop
villaggiobitcoin.it

Villaggio Bitcoin

Bitcoin book

21 Pensieri



Un testo per interpretare il fenomeno **Bitcoin**

amazon

VillaggioShop
villaggiobitcoin.it

Villaggio Bitcoin