MODULO 2. IL PROTOCOLLO BITCOIN

Il network, la blockchain e il mining

Villaggio**Bitcoin**

Corso base su Bitcoin

Villaggio**Bitcoin**

Modulo 1

Modulo 2

Modulo 3

Modulo 4

IL PROTOCOLLO BITCOIN

- Come avviene una transazione
- Cenni funzionamento Blockchain
- Mining ed emissione nuovi btc
- Politica monetaria e valore
- Incentivi e teoria dei giochi
- Transazioni btc nella pratica
- Monitorare un transazione onchain

Villaggio Bitcoin

BITCOIN: RECAP

- Protocollo, network e moneta
- *Bitcoin* e *bitcoin*
- Due principali innovazioni:

1. NESSUN ENTE CENTRALE
2. SCARSITÀ IN AMBITO DIGITALE

→ ORO DIGITALE

Villaggio Bitcoin

ECOSISTEMA BITCOIN

DEFINIZIONI

PROTOCOLLO
SOFTWARE
NETWORK
MONETA

TEORIA DEI GIOCHI

TECNOLOGIE

FILOSOFIA OPEN SOURCE
FIRME DIGITALI
CRITTOGRAFIA
STATISTICA E PROBABILITÀ
BLOCKCHAIN
PROOF-OF-WORK
MINING
...

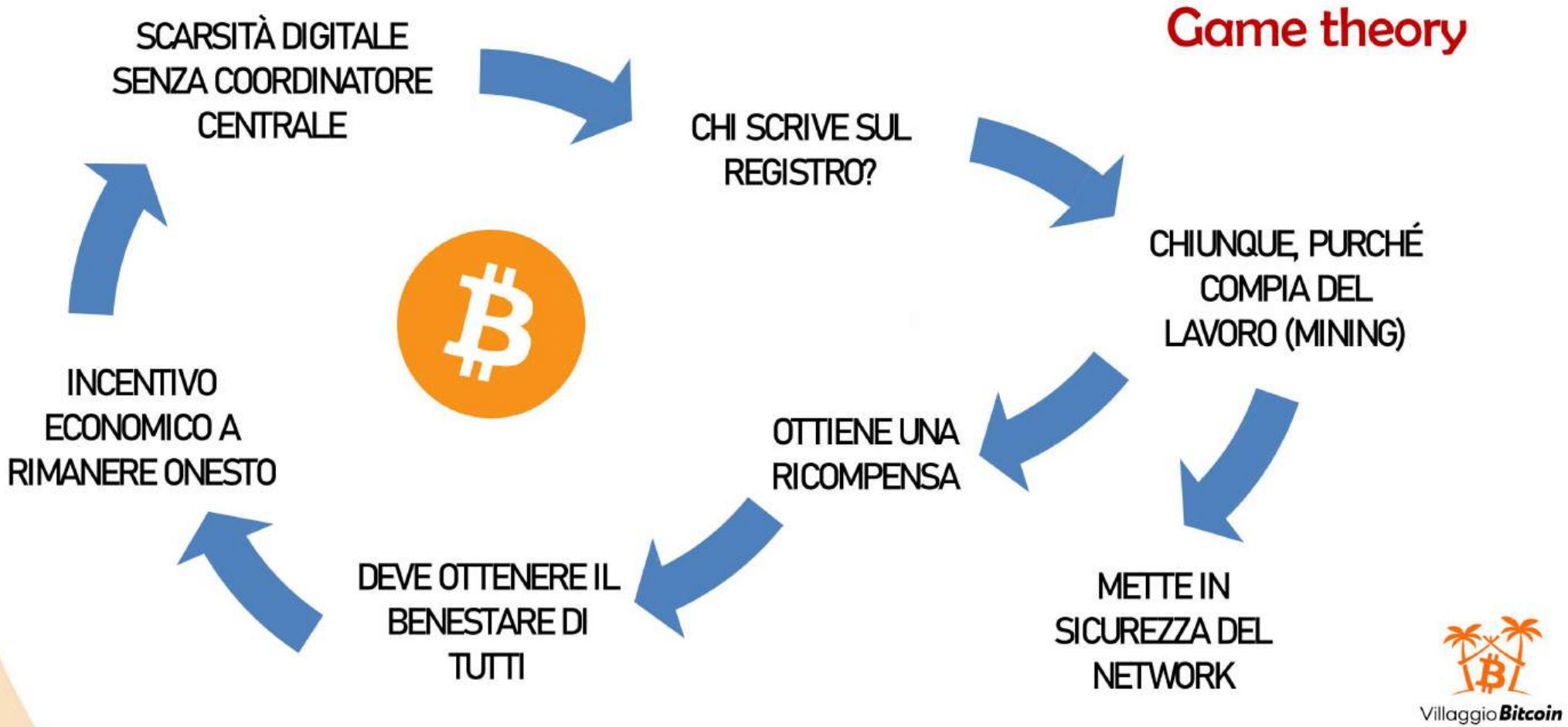
CARATTERISTICHE

Decentralizzazione
Resistenza al cambiamento
Resilienza
Scarsità
Non censurabilità
Non confiscabilità

Gratuito
Permissionless
Aperto e trasparente
Privacy
Borderless
...

Villaggio Bitcoin

PRINCIPI DI FUNZIONAMENTO



Villaggio Bitcoin

LA MONETA: BTC o SATS

Divisibile fino a 8 ordini grandezza (0,00000001 btc) chiamata **Satoshi** o **sat**

UTXO «bloccati» in una chiave pubblica (indirizzo pubblico):

Esempi di indirizzi pubblici (*bitcoin address*):

- bc1q7cyrfmck2ffu2ud3rn5l5a8yv6f0chkp0zpemf
- bc1qqkjdahh55hzrxa79637jkz3ujsq09s2t6eg4f6
- 3CsPq8YUymGyezXhvcyUXrvpAyawSWfmEr
- 3Q4o9hGfN4qYaE97CSRdqFBpUznoQMtXWF
- 17JC56XYjVf47iHsZHhZgTzhG62HGvbs3a
- 1AuN3JZtVbYHi5War7qoS75z6VMfvnE1F6

Villaggio **Bitcoin**

CRITTOGRAFIA ASIMMETRICA

- Coppia di chiavi Privata e Pubblica
- Chiave Privata —DERIVA→ Chiave Pubblica —DERIVA→ Indirizzo bitcoin

Villaggio Bitcoin

LE TRANSAZIONI STEP BY STEP

1. Da una chiave pubblica (indirizzo) ad un'altra chiave pubblica.
   Il mittente, con la chiave privata, firma la transazione (Firma Digitale)
2. La transazione viene trasmessa nel Network
3. Ogni nodo verifica la sintassi della transazione
4. La transazione verificata va nella mempool
5. I ***Miners*** la inseriscono nel successivo blocco (Blockchain)
6. Il primo ***Miner*** trova la «soluzione», confermando il blocco
7. Tutti verificano la soluzione e concordano sul trasferimento avvenuto da indirizzo a indirizzo (consensus)
8. La transazione rimane «scolpita» nel blocco sulla Blockchain

Villaggio**Bitcoin**

LE TRANSAZIONI STEP BY STEP

1. Da una chiave pubblica (indirizzo) ad un'altra chiave pubblica.
   Il mittente, con la chiave privata, firma la transazione (Firma Digitale)
2. La transazione viene trasmessa nel Network
3. Ogni nodo verifica la sintassi della transazione
4. La transazione verificata è inserita nella mempool
5. I Miners la inseriscono nel blocco (Blockchain)
6. Il primo ***Miner*** trova la «soluzione», confermando il blocco
7. Tutti verificano la soluzione e concordano sul trasferimento avvenuto da indirizzo a indirizzo (consensus)
8. La transazione rimane «scolpita» nel blocco sulla Blockchain

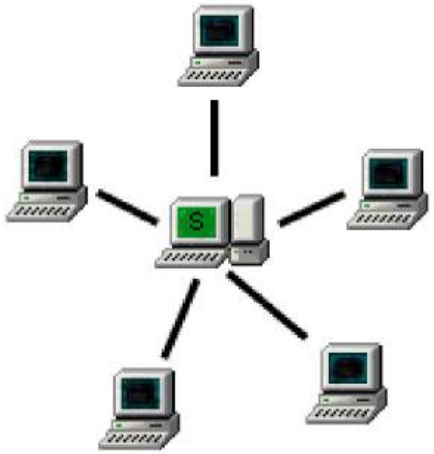
Villaggio **Bitcoin**

BITCOIN: L'ARCHITETTURA

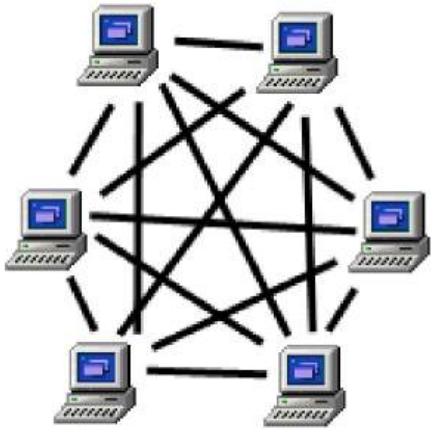
- Server based network
- Software proprietario
- Profilazione utenti

napster

PayPal



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



BitTorrent

eMule

Villaggio Bitcoin

BITCOIN: L'ARCHITETTURA

- Ecosistema P2P:
  - Nodi
  - Miner
  - Wallet

Villaggio Bitcoin

LE TRANSAZIONI STEP BY STEP

1. Da una chiave pubblica (indirizzo) ad un'altra chiave pubblica.
   Il mittente, con la chiave privata, firma la transazione (Firma Digitale)
2. La transazione viene trasmessa nel Network
3. Ogni nodo verifica la sintassi della transazione
4. La transazione verificata è inserita nella mempool
5. I Miners la inseriscono nel blocco (Blockchain)
6. Il primo ***Miner*** trova la «soluzione», confermando il blocco
7. Tutti verificano la soluzione e concordano sul trasferimento avvenuto da indirizzo a indirizzo (consensus)
8. La transazione rimane «scolpita» nel blocco sulla Blockchain

Villaggio **Bitcoin**

LE TRANSAZIONI STEP BY STEP

1. Da una chiave pubblica (indirizzo) ad un'altra chiave pubblica.
   Il mittente, con la chiave privata, firma la transazione (Firma Digitale)
2. La transazione viene trasmessa nel Network
3. Ogni nodo verifica la sintassi della transazione
4. **La transazione verificata è inserita nella mempool**
5. **I *Miners* la inseriscono nel blocco (Blockchain)**
6. **Il primo Miner trova la «soluzione», confermando il blocco**
7. Tutti verificano la soluzione e concordano sul trasferimento avvenuto da indirizzo a indirizzo (consensus)
8. La transazione rimane «scolpita» nel blocco sulla Blockchain

Villaggio Bitcoin

LE TRANSAZIONI STEP BY STEP

1. Da una chiave pubblica (indirizzo) ad un'altra chiave pubblica.
   Il mittente, con la chiave privata firma la transazione (Firma Digitale)
2. La transazione viene trasmessa nel Network
3. Ogni nodo verifica la sintassi della transazione
4. La transazione verificata è inserita nella mempool
5. I Miners la inseriscono nel successivo blocco (Blockchain)
6. Il primo ***Miner*** trova la «soluzione», confermando il blocco
7. **Tutti verificano la soluzione e concordano sul trasferimento avvenuto da indirizzo a indirizzo (consensus)**
8. **La transazione rimane «scolpita» nel blocco sulla Blockchain**

Villaggio **Bitcoin**

IL MINING

Oro

Estrazione nuovo oro dalle miniere

bitcoin

- Forniscono *Hash Power*
- Risoluzione problema doppia spesa
- Esibiscono la Proof-of-Work (Prova di lavoro)
- Confermano i blocchi di transazione

MINING

Emissione nuovi satoshi

Villaggio Bitcoin

LA VALIDAZIONE DEI BLOCCHI

MINER E PROOF-OF-WORK

- Continui tentativi dei miners
- Questione probabilistica
- Potenza di calcolo
- Solo 1 vincitore per ogni blocco
- Blocchi in media da 10 minuti

Villaggio Bitcoin

BITCOIN: MINING

PROVA DI LAVORO
(Proof-of-work)

- Il miner che trova per primo la soluzione del blocco candidato trasmette a tutti la soluzione trovata.
- Se corretta, si aggiudica nuovi btc (oggi 3,125 btc + le commissioni) e il blocco viene aggiunto sulla blockchain da tutti i nodi.

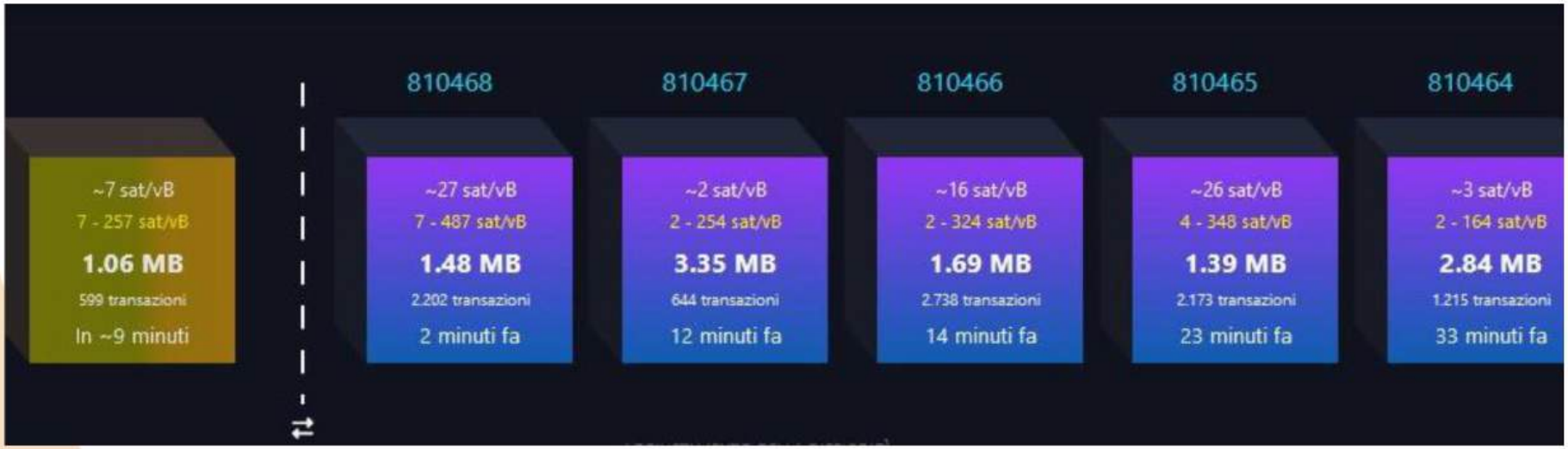
Villaggio Bitcoin

BITCOIN: LA BLOCKCHAIN

Risoluzione problema double-spending

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

CONSENSO DISTRIBUITO



Villaggio Bitcoin

LE TRANSAZIONI STEP BY STEP

1. Da una chiave pubblica (indirizzo) ad un'altra chiave pubblica.
   Il mittente, con la chiave privata firma la transazione (Firma Digitale)
2. La transazione viene trasmessa nel Network
3. Ogni nodo verifica la sintassi della transazione
4. La transazione verificata è inserita nella mempool
5. I Miners la inseriscono nel successivo blocco (Blockchain)
6. Il primo ***Miner*** trova la «soluzione», confermando il blocco
7. **Tutti verificano la soluzione e concordano sul trasferimento avvenuto da indirizzo a indirizzo (consensus)**
8. **La transazione rimane «scolpita» nel blocco sulla Blockchain**

Villaggio **Bitcoin**

NETWORK HASH RATE

630 Esa hash/sec

(dato aprile 2024)

BITCOIN: IL MINING

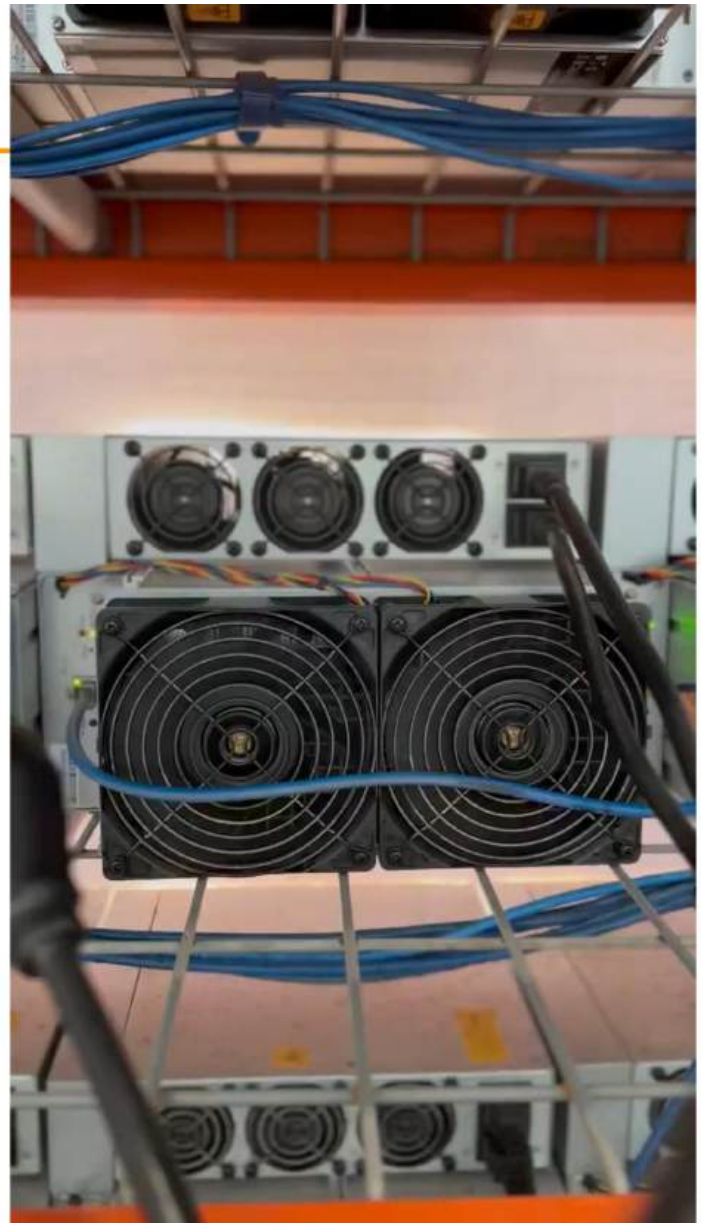
- Industria in continua crescita
- Fornisce Hash rate power
- Emissione nuovi bitcoin
- Sicurezza infrastruttura

ANTMINER HYDRO CONTAINER

Villaggio Bitcoin

BITCOIN MINING

- Nuovo settore imprenditoriale
- Ricerca energia basso costo
- Modulabile
- Aperto e senza barriere



Villaggio Bitcoin

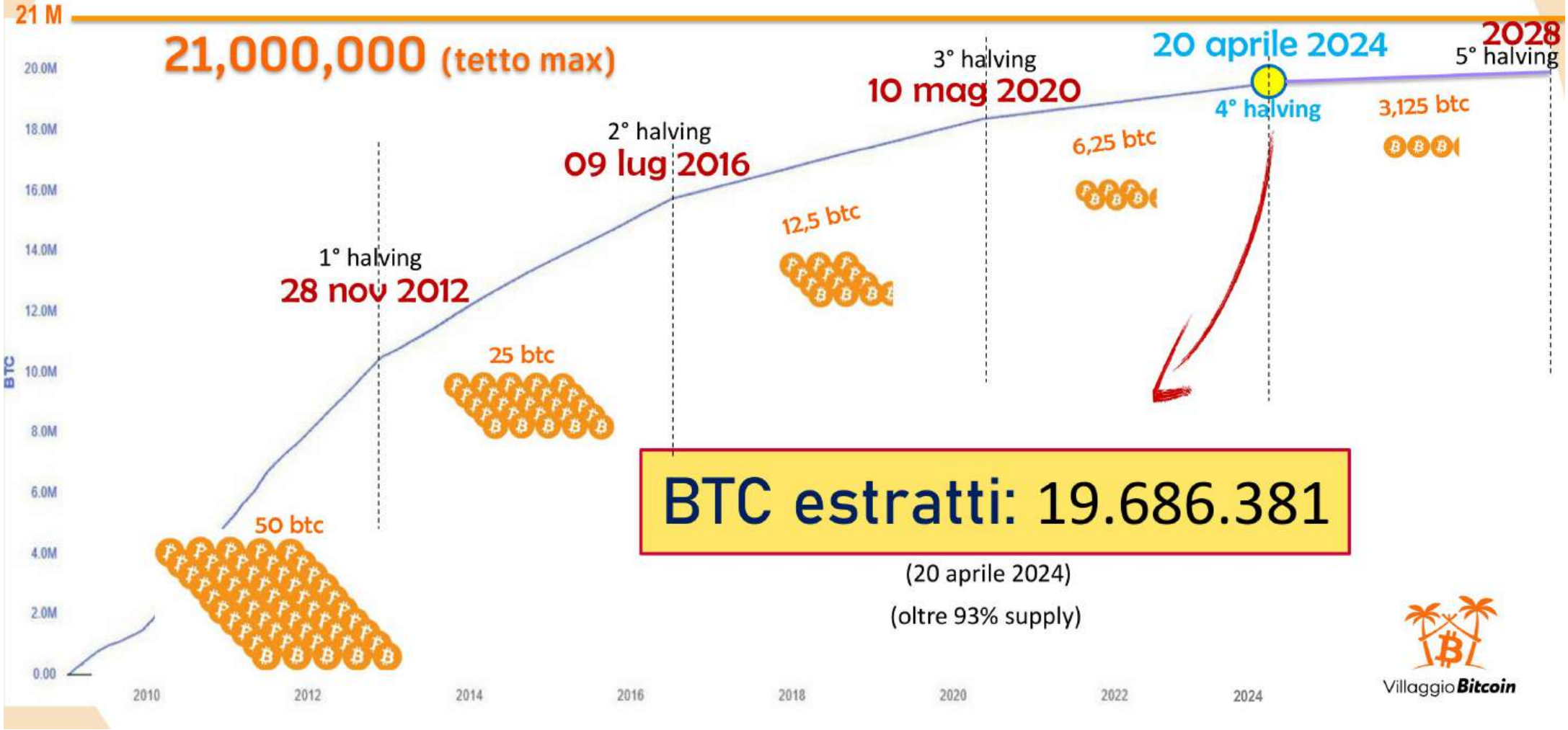
Il MINING E LA POLITICA MONETARIA

- Competizione tra miners
- Blocchi da 10 minuti
- Incentivi economici a mantenersi onesti
- Ogni 4 anni si dimezzano ricompense (**Halving**)

Game theory

Villaggio **Bitcoin**

LA POLITICA MONETARIA



BTC estratti: 19.686.381

(20 aprile 2024)

(oltre 93% supply)

Villaggio Bitcoin

LA POLITICA MONETARIA

Aggiustamento automatico della difficoltà

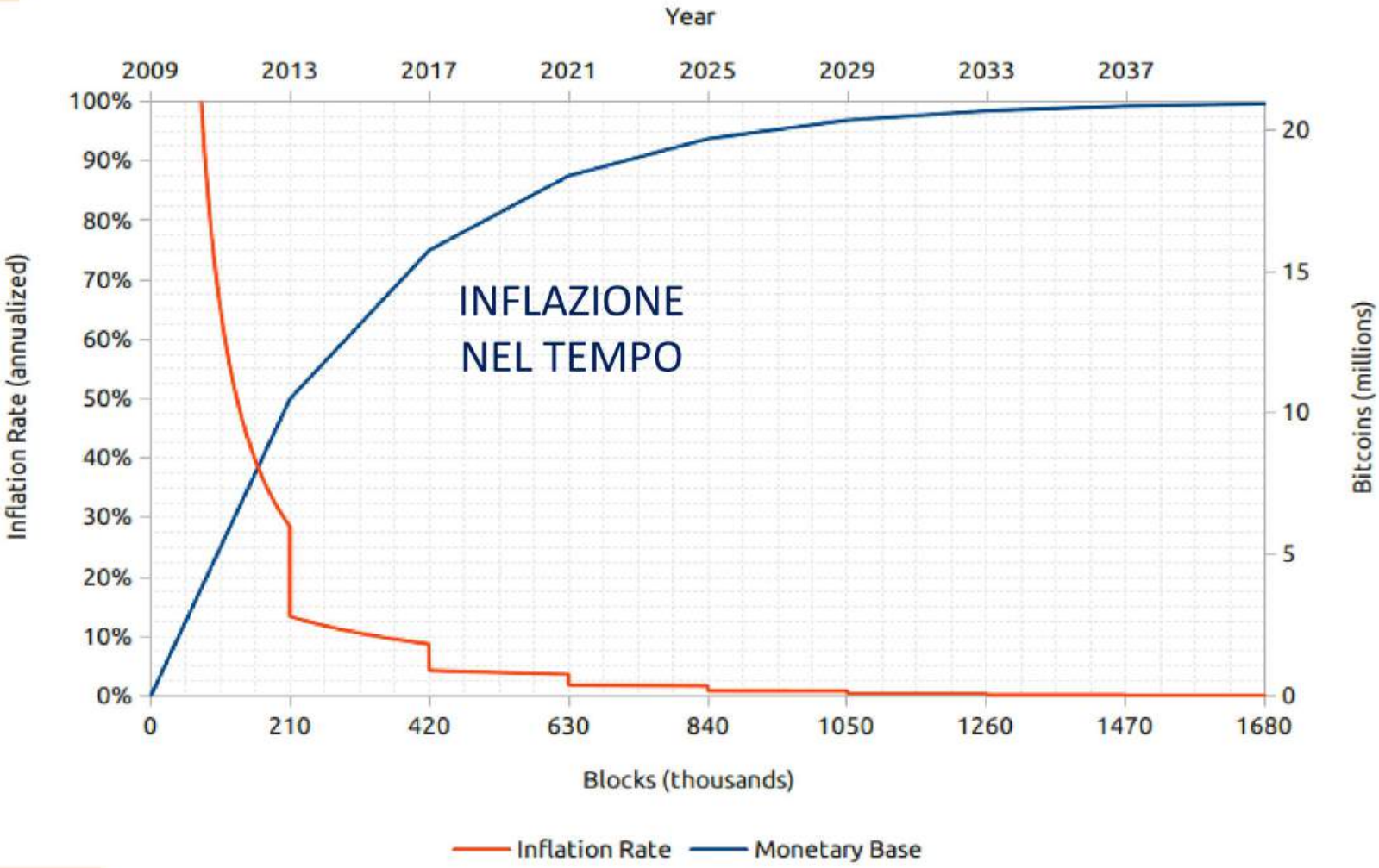
- Innalzamento o abbassamento del target
- Ogni circa 2 settimane
- blocchi ogni 10 minuti di media

Il tempo di emissione di nuovi btc ***NON*** dipende dalla potenza di calcolo della rete

Inflazione controllata e prevedibile

Villaggio**Bitcoin**

LA POLITICA MONETARIA



TETTO MAX:

21 MILIONI BTC

N totale di halving

N di nuovi bitcoin emessi per blocco

$$\sum_{i=0}^{32} 210{,}000 \frac{50}{2^i}$$

N di blocchi tra i vari halving

N di halving fino a oggi

Villaggio**Bitcoin**

COMMISSIONI DI TRANSAZIONE

RICOMPENSA PER I MINERS:

1. **Sussidio** del blocco (fisso **3,125** btc)

+

2. **Commissioni** di tutte le transazioni incluse in quel blocco (**variabile**)

- Non obbligatoria
- Non dipende da importo trasferito
- In funzione della priorità

Villaggio Bitcoin

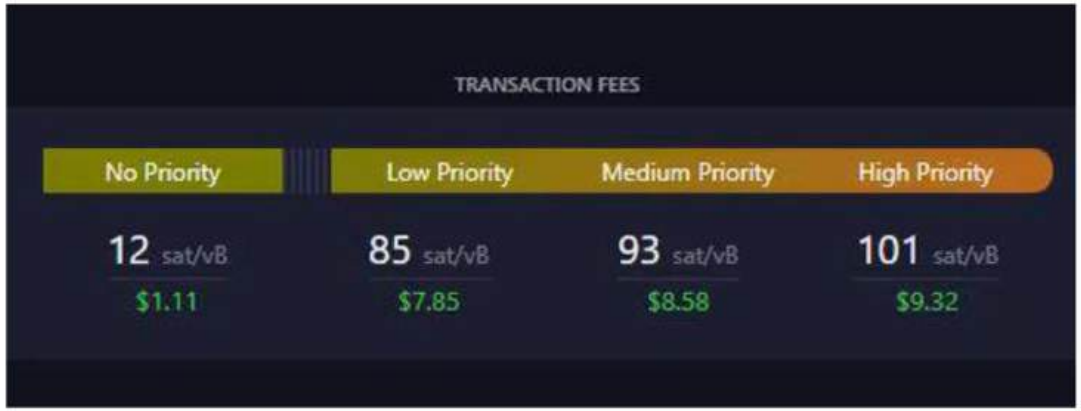
COMMISSIONI DI TRANSAZIONE

RICOMPENSA PER I MINERS:

1. **Sussidio** del blocco (fisso **3,125** btc)

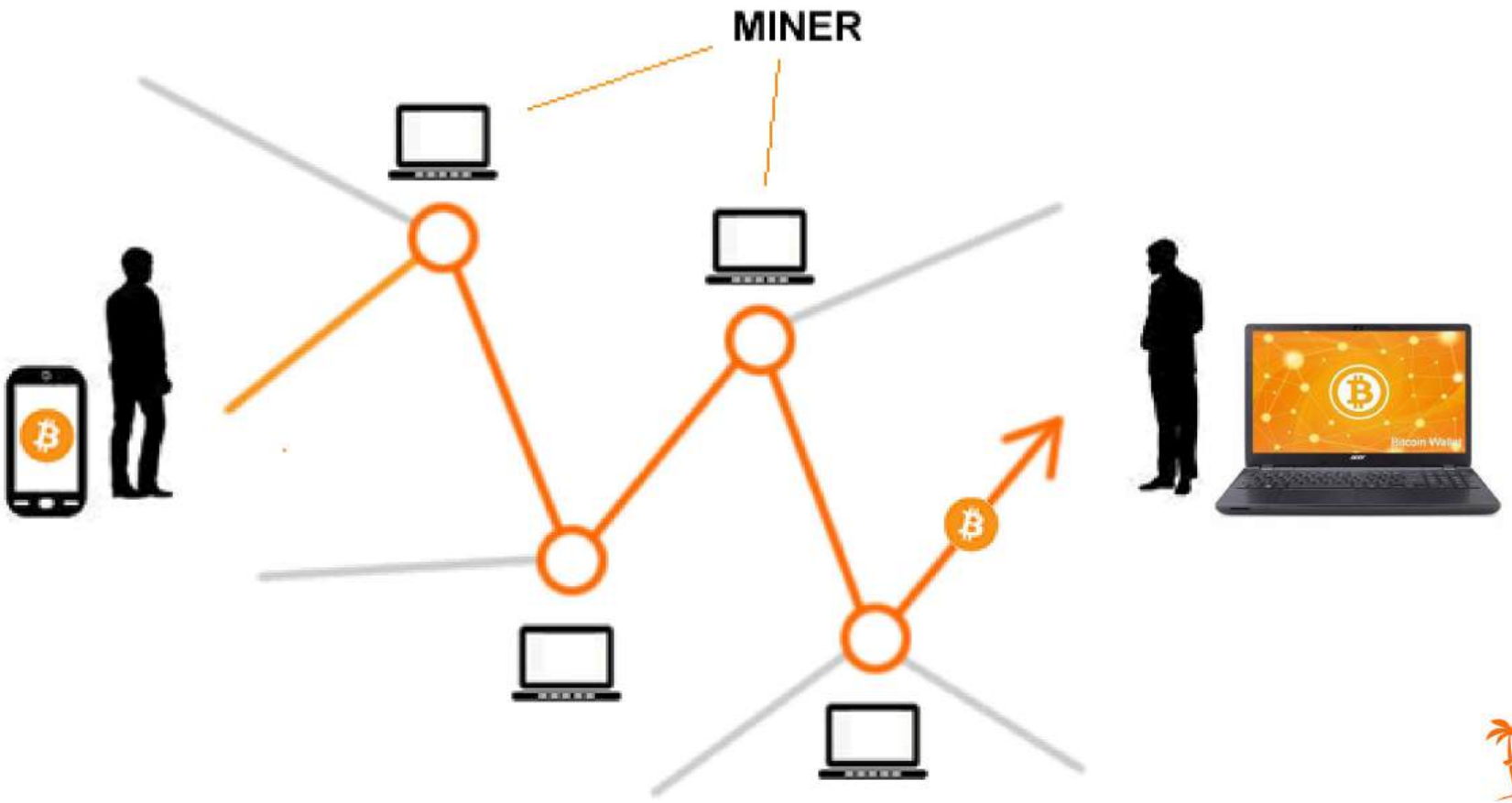
+

2. **Commissioni** di tutte le transazioni incluse in quel blocco (**variabile**)



Villaggio Bitcoin

IN ACTION!



Villaggio Bitcoin

IL VALORE DI BITCOIN

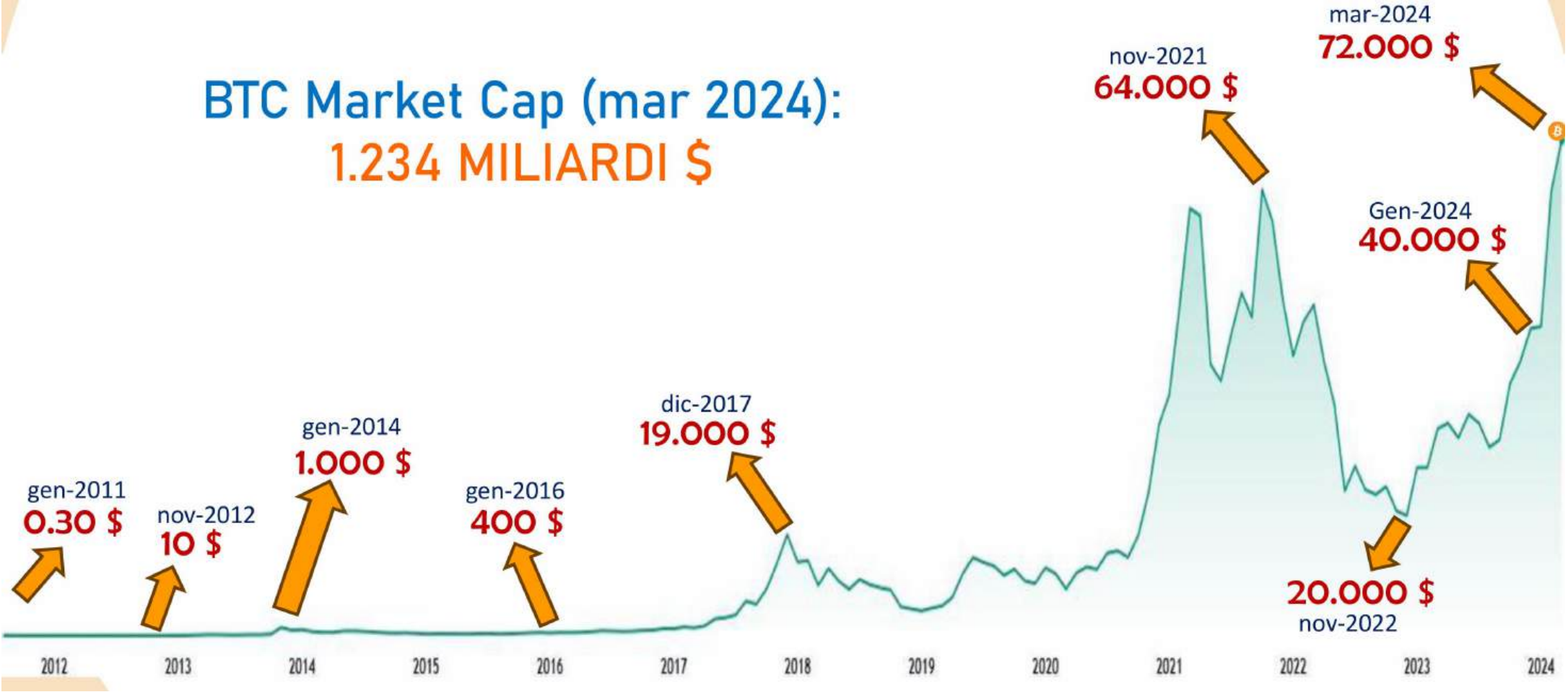
Chi stabilisce il
prezzo di bitcoin?

Domanda e offerta

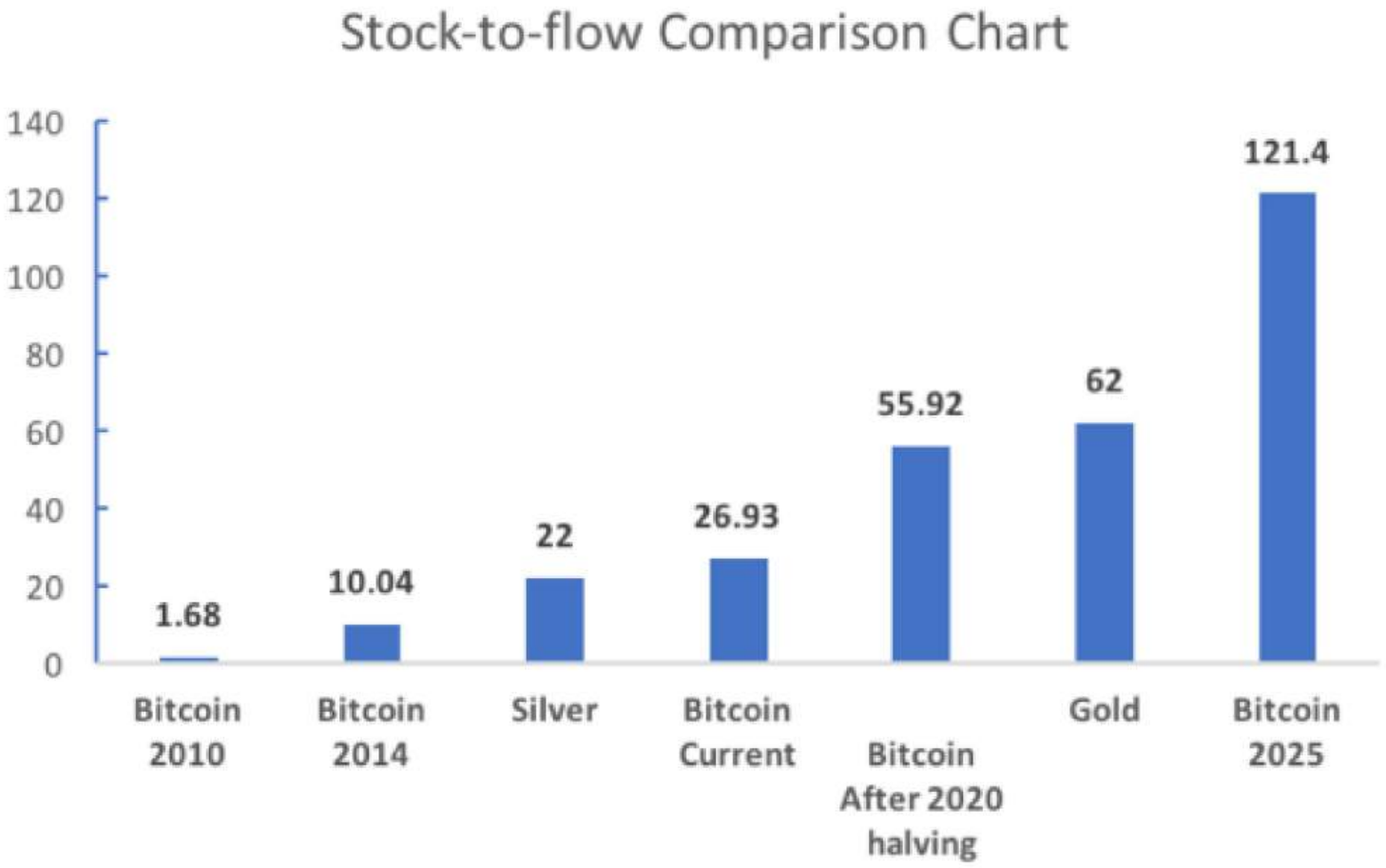
Villaggio Bitcoin

IL VALORE DI BITCOIN

BTC Market Cap (mar 2024):
1.234 MILIARDI $



DIGITAL GOLD



Villaggio Bitcoin

LE TRANSAZIONI STEP BY STEP

1. Da una chiave pubblica (indirizzo) ad un'altra chiave pubblica.
   Il mittente, con la chiave privata firma la transazione (Firma Digitale)
2. La transazione viene trasmessa nel Network
3. Ogni nodo verifica la sintassi della transazione
4. La transazione verificata è inserita nella mempool
5. I Miners la inseriscono nel successivo blocco (Blockchain)
6. Il primo ***Miner*** trova la «soluzione», confermando il blocco
7. Tutti verificano la soluzione e concordano sul trasferimento avvenuto
   da indirizzo a indirizzo (consensus)
8. La transazione rimane «scolpita» nel blocco sulla Blockchain

Villaggio **Bitcoin**

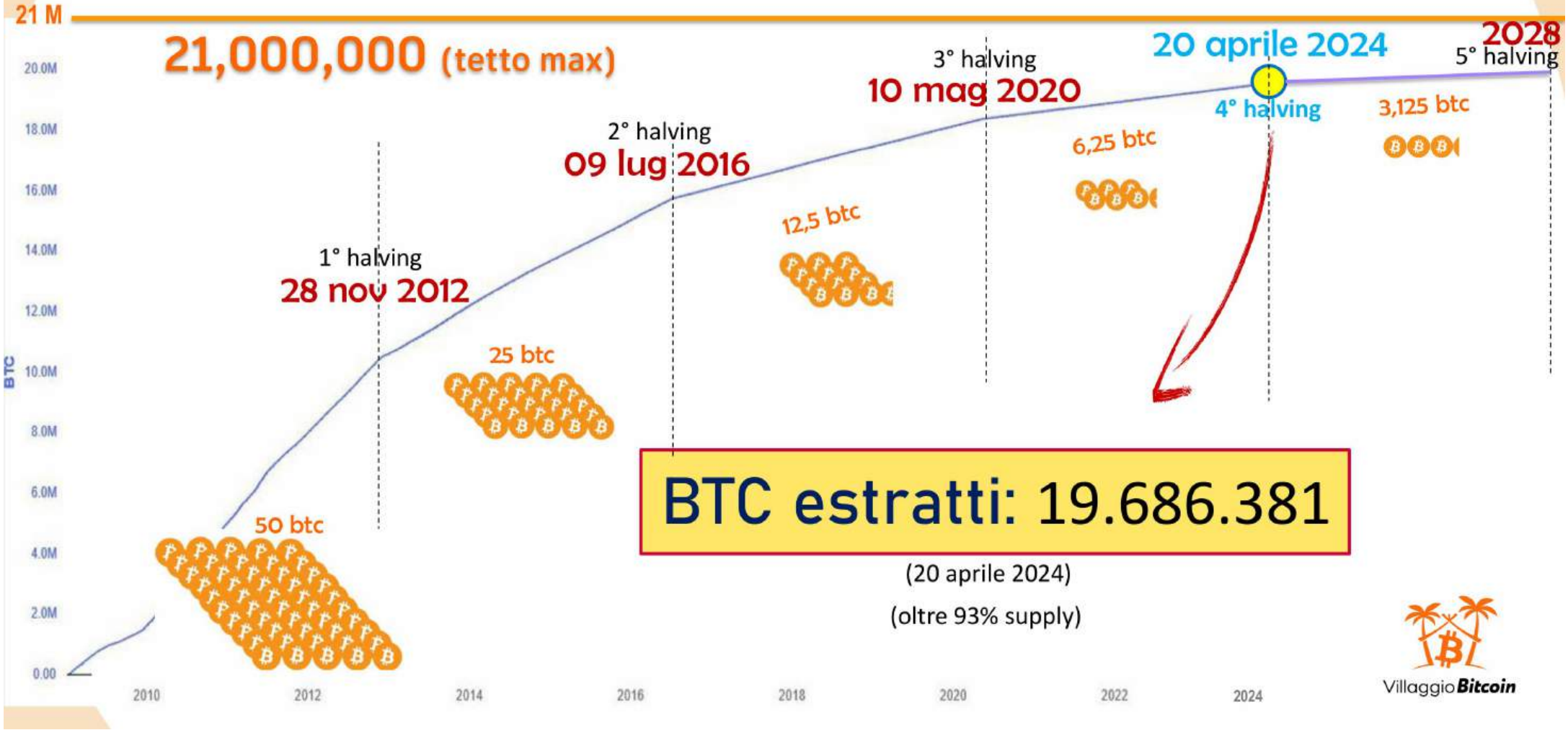
Il MINING E LA POLITICA MONETARIA

- Competizione tra miners
- Blocchi da 10 minuti
- Incentivi economici a mantenersi onesti
- Ogni 4 anni si dimezzano ricompense (**Halving**)

Game theory

Villaggio **Bitcoin**

LA POLITICA MONETARIA



BTC estratti: 19.686.381

(20 aprile 2024)

(oltre 93% supply)

Villaggio Bitcoin

ECOSISTEMA BITCOIN

DEFINIZIONI

PROTOCOLLO
SOFTWARE
NETWORK
MONETA

TEORIA DEI GIOCHI

TECNOLOGIE

FILOSOFIA OPEN SOURCE
FIRME DIGITALI
CRITTOGRAFIA
STATISTICA E PROBABILITÀ
BLOCKCHAIN
PROOF-OF-WORK
MINING
...

CARATTERISTICHE

Decentralizzazione
Resistenza al cambiamento
Resilienza
Scarsità
Non censurabilità
Non confiscabilità

Gratuito
Permissionless
Aperto e trasparente
Privacy
Borderless
...

Villaggio Bitcoin

BIT QUOTE

”

SE NON CI CREDI O NON CAPISCI, NON HO TEMPO PER CERCARE DI CONVINCERTI, MI DISPIACE.

Satoshi Nakamoto – 29 giugno 2010

Inventore anonimo di Bitcoin, spazientito dalle domande di un interlocutore

Villaggio**Bitcoin**

MODULO 2. IL PROTOCOLLO BITCOIN

Il network, la blockchain e il mining

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

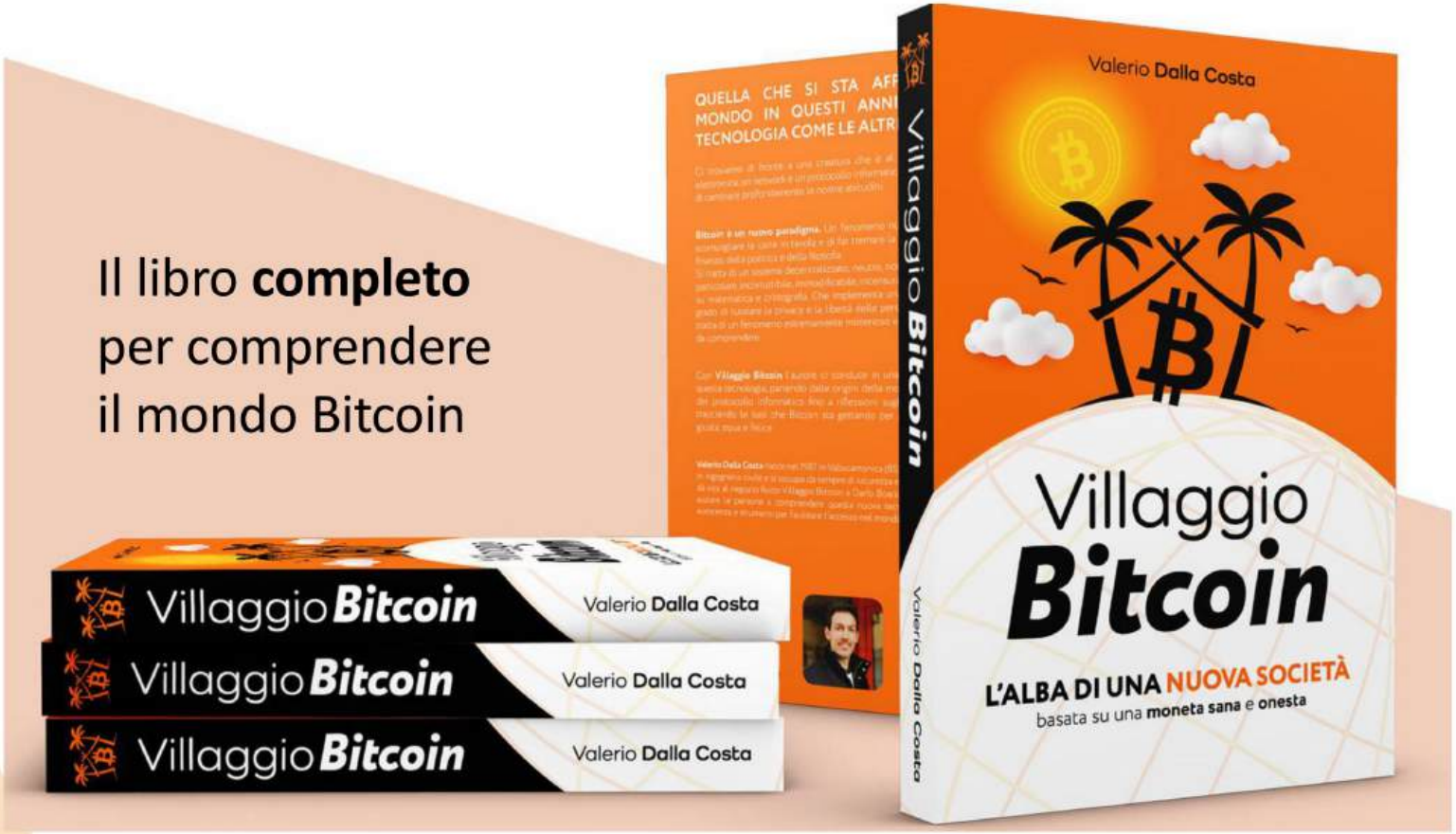
Modulo 3

Modulo 4

Bitcoin book

Villaggio Bitcoin

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



AVAILABLE ON:

amazon

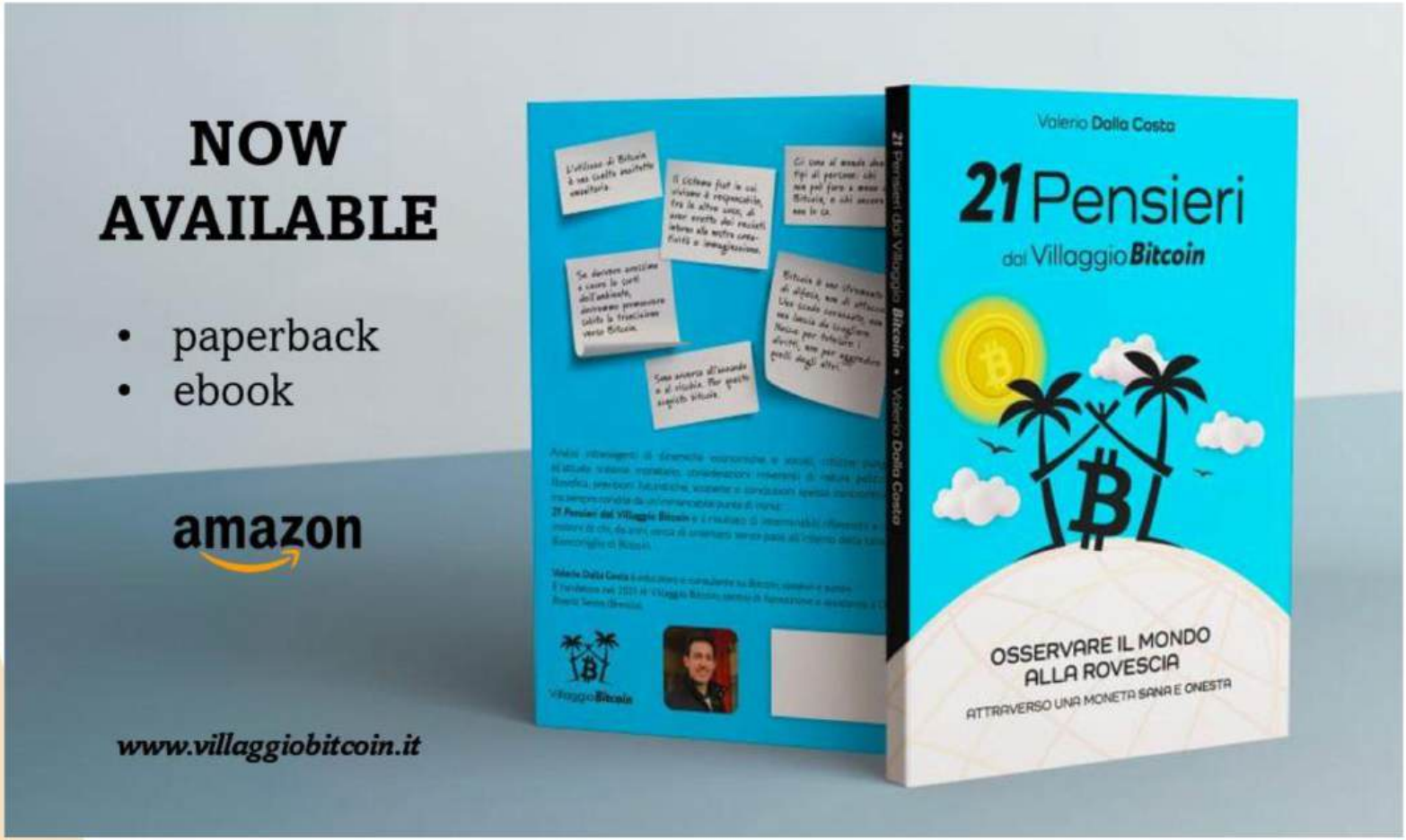
USEMLAB
ECONOMIA E MERCATI

VillaggioShop
villaggiobitcoin.it

Villaggio Bitcoin

Bitcoin book

21 Pensieri



Un testo per interpretare il fenomeno **Bitcoin**

amazon

VillaggioShop
villaggiobitcoin.it

Villaggio Bitcoin