MODULO 3. IL WALLET BITCOIN

L'utilizzo pratico dell'oro digitale

Villaggio**Bitcoin**

Corso base su Bitcoin

Villaggio**Bitcoin**

Modulo 1

Modulo 2

Modulo 3

Modulo 4

TODAY

Il Wallet

Bitcoin

- RECAP: Il protocollo e le transazioni
- Chiavi e indirizzi
- Il wallet e tipologie
- Seed e password del wallet
- Cenni di sicurezza informatica
- In action!
- Q&A

Villaggio **Bitcoin**

ECOSISTEMA BITCOIN

- Competizione tra miners
- Blocchi da 10 minuti
- Ogni 4 anni si dimezzano ricompense (**Halving**)

TEORIA DEI GIOCHI

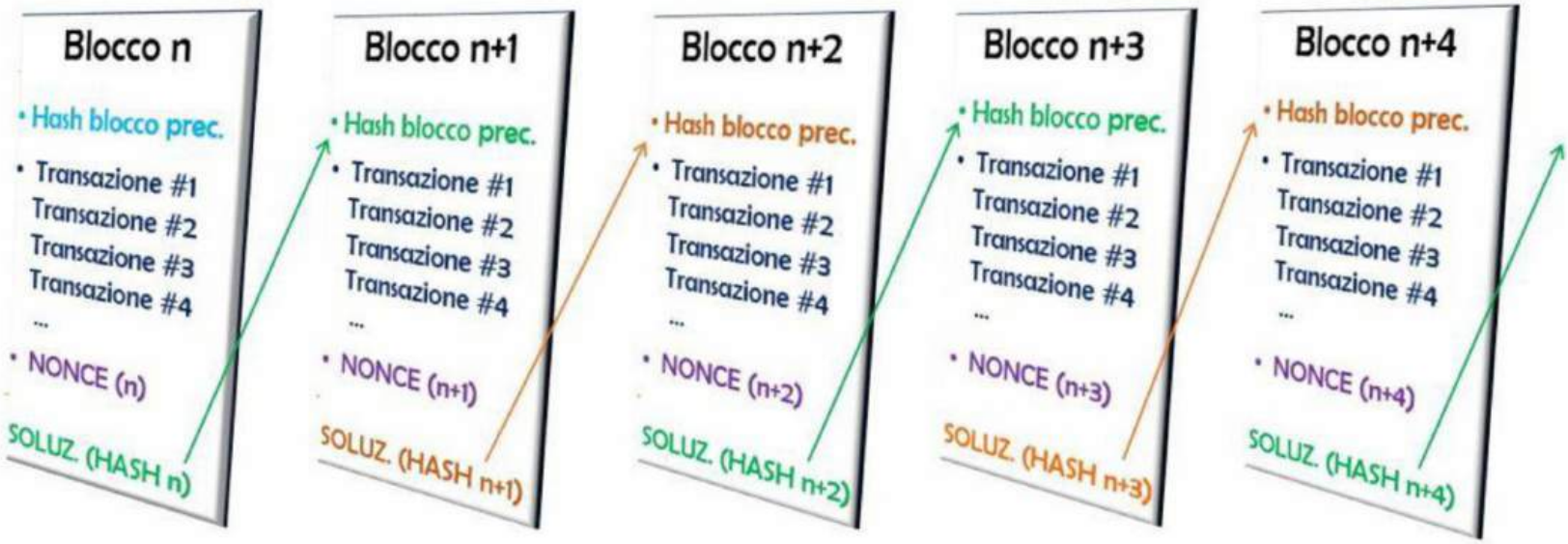
Villaggio Bitcoin

BITCOIN: LA BLOCKCHAIN

Risoluzione problema double-spending

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

CONSENSO DISTRIBUITO



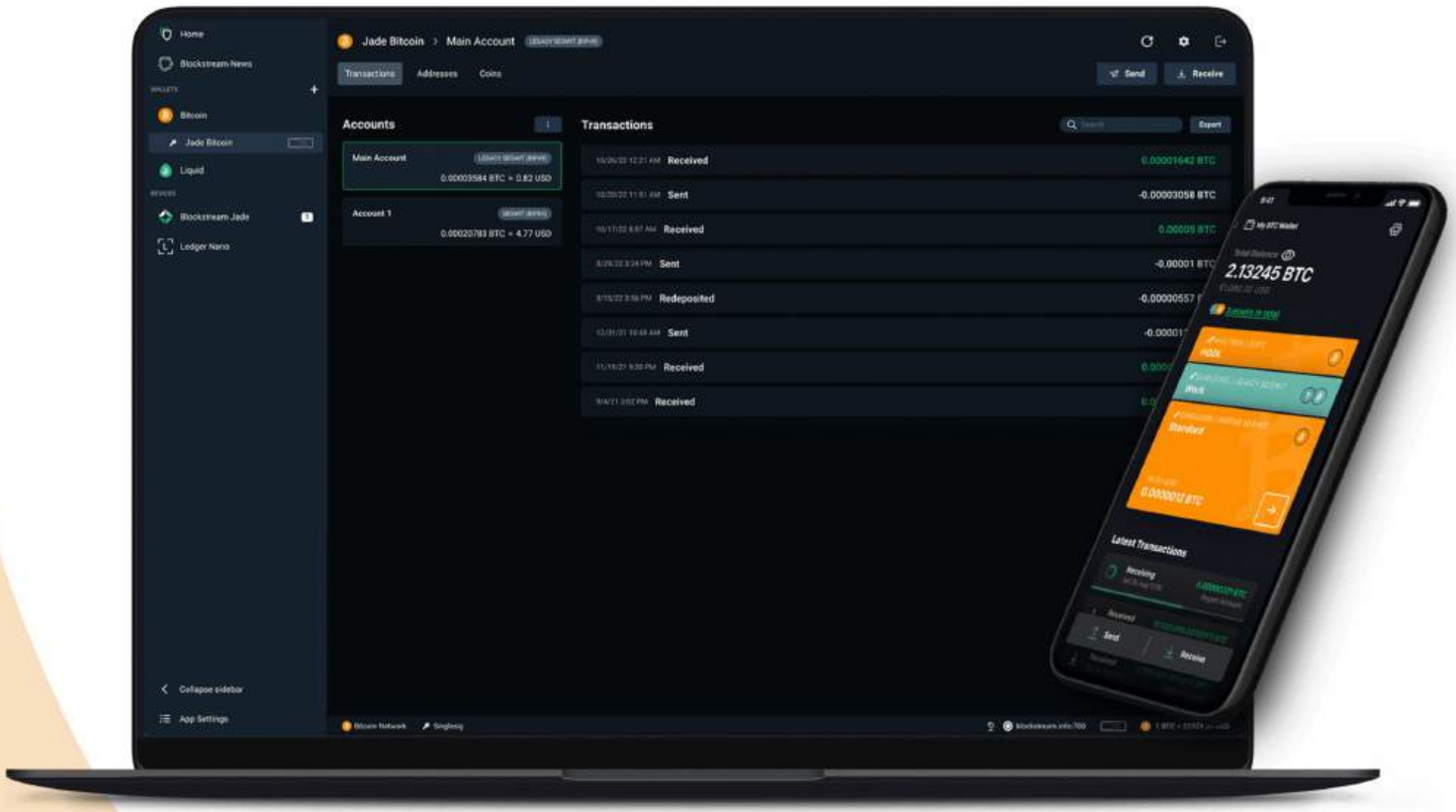
Villaggio Bitcoin

LE TRANSAZIONI STEP BY STEP

1. **Da una chiave pubblica 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**

WALLET BITCOIN



Villaggio Bitcoin

CRITTOGRAFIA ASIMMETRICA

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

https://www.bitaddress.org

Villaggio Bitcoin

INDIRIZZI BITCOIN

Chi li assegna?

Noi stessi... a caso!

- Generazione entropia

- SHA256, RIPEMD160
- Secp256k1 – ECDSA
- Base58check (bech32)
- Collision-resistant

ENTROPIA

⇩

Kwsmqow4bidFNsETYd1NPxZmxDWCHHq54WEnybfXo5vXoqhU8J4x

Chiave privata (**k**)

⇩

K = G * k

Chiave pubblica (**K**)

⇩

Indirizzo Bitcoin

bc1q5shngj24323nsrmxv99st02na6srekfctt30ch

Villaggio **Bitcoin**

INDIRIZZI BITCOIN

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

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

Esempi di indirizzi pubblici (*bitcoin address*):

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

Villaggio **Bitcoin**

IL WALLET BITCOIN

FUNZIONI

- Generare **chiavi** private
- Custodirle al meglio (**!**)
- Comporre le **transazioni**
- Verificare le **firme digitali**
- Calcolare il «saldo» e conferme su **blockchain**

Private Key

SECRET

L2J6RE57EoGNBeTPqdkpL4yQsgmLTB3ZSboXPRG5YyCeWytfXwUN

« Not your key? Not your bitcoin! »

Villaggio Bitcoin

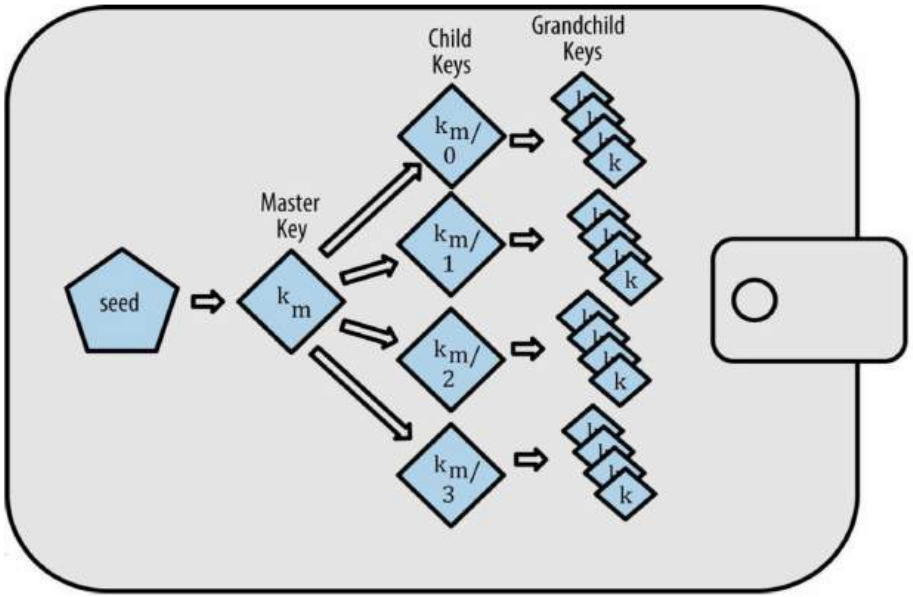
IL SEED

HD wallet

- BIP32 e BIP39
- Codice di 12 o 24 parole (mnemonic)

Esempio di seed:

twice note flip busy stumble flock
wash need forum venture arch modify



Chiavi private (**k**) da non divulgare!

Villaggio**Bitcoin**

IL WALLET: TIPOLOGIE

- HD wallet vs
Non deterministic (JBOK)

Desktop wallet

- Specter
- Bitcoin Core
- BitPay
- Electrum
- Wasabi
- Sparrow
- Green

Hardware wallet

- BitBox02
- Coldcard
- KeepKey
- Ledger Nano S
- Trezor Model T
- Trezor One
- Jade
- Portal

Mobile wallet

- WoS
- Phoenix
- BitPay
- BLW
- BRD
- Eclair Mobile
- Edge
- Electrum
- Breez wallet
- Blue wallet
- Green
- Blink

paper

brain

web

Villaggio Bitcoin

IL SEED

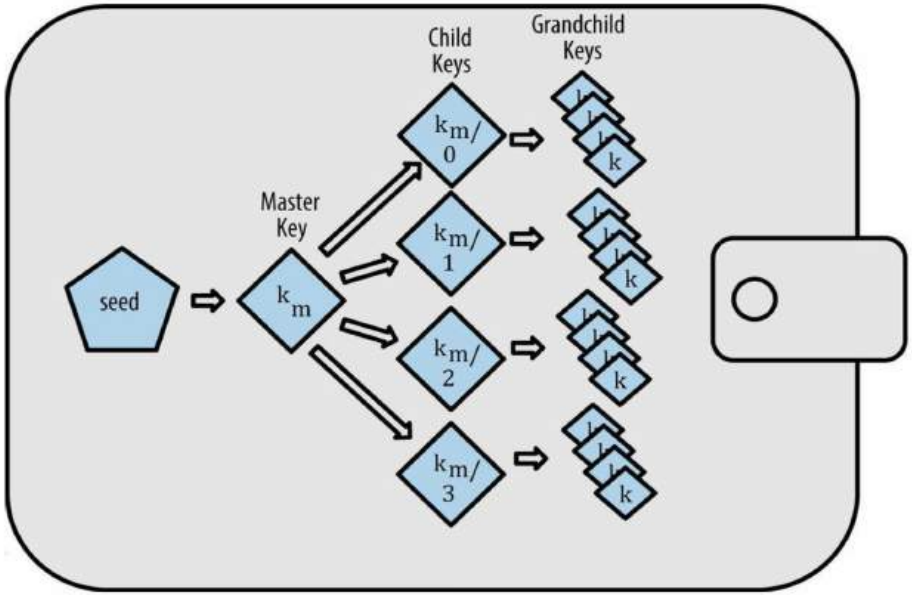
• HD wallet vs
Non deterministic (JBOK)

HD wallet

- BIP32 e BIP39
- Codice di 12 o 24 parole (mnemonic)

Esempio di seed:

twice note flip busy stumble flock
wash need forum venture arch modify



Chiavi private (**k**) da non divulgare!

Villaggio Bitcoin

IL WALLET: TIPOLOGIE

- HD wallet vs Non deterministic (JBOK)
- Lightweight wallet (SPV) vs Full node

Desktop wallet

- Specter
- Bitcoin Core
- BitPay
- Electrum
- Wasabi
- Sparrow
- Green

Hardware wallet

- BitBox02
- Coldcard
- KeepKey
- Ledger Nano S
- Trezor Model T
- Trezor One
- Jade
- Portal

Mobile wallet

- WoS
- Phoenix
- BitPay
- BLW
- BRD
- Eclair Mobile
- Edge
- Electrum
- Breez wallet
- Blue wallet
- Green
- Blink

paper

brain

web

Villaggio Bitcoin

FULL NODE

```
ubuntu@torontola: ~
File  Edit  View  Search  Terminal  Help
ubuntu@torontola:~$ sudo ufw allow 8333/tcp
Rules updated
Rules updated (v6)
ubuntu@torontola:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
ubuntu@torontola:~$ bitcoin-cli --getinfo
{
  "version": 170100,
  "protocolversion": 70015,
  "walletversion": 169900,
  "balance": 0.00000000,
  "blocks": 388343,
  "timeoffset": -8,
  "connections": 16,
  "proxy": "",
  "difficulty": 79102380900.22598,
  "testnet": false,
  "keypoololdest": 1552300978,
  "keypoolsize": 1000,
  "paytxfee": 0.00000000,
  "relayfee": 0.00001000,
  "warnings": ""
}
ubuntu@torontola:~$
```

- Sincronizzazione intera blockchain
- Parte attiva del network
- Max privacy e sicurezza
- Contributo alla decentralizzazione e resilienza Bitcoin

Villaggio **Bitcoin**

IL WALLET: TIPOLOGIE

- HD wallet vs Non deterministic (JBOK)
- Lightweight wallet (SPV) vs Full node
- Custiodial vs Non-Custodial
- Hot wallet vs Cold wallet

Desktop wallet

- Specter
- Bitcoin Core
- BitPay
- Electrum
- Wasabi
- Sparrow
- Green

Hardware wallet

- BitBox02
- Coldcard
- KeepKey
- Ledger Nano S
- Trezor Model T
- Trezor One
- Jade
- Portal

Mobile wallet

- WoS
- Phoenix
- BitPay
- BLW
- BRD
- Eclair Mobile
- Edge
- Electrum
- Breez wallet
- Blue wallet
- Green
- Blink

paper

brain

web

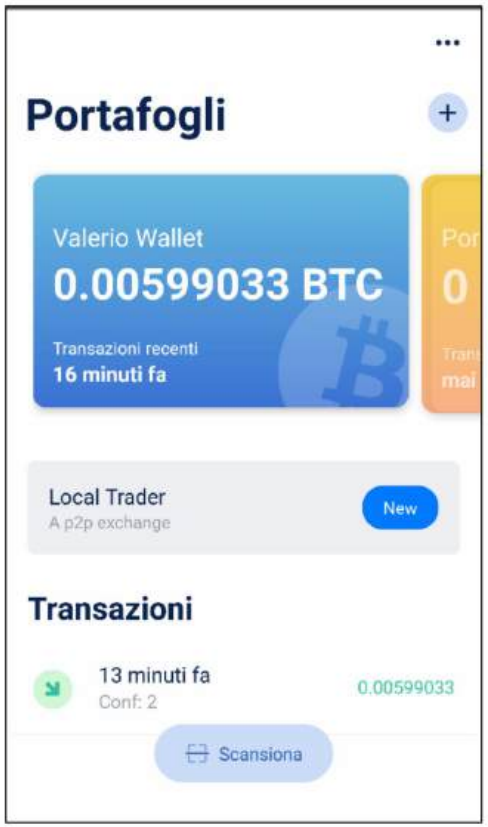
Villaggio Bitcoin

DESKTOP WALLET

- Specter wallet
- Bitcoin Core
- BitPay
- Electrum
- Wasabi
- Sparrow
- Green

Villaggio Bitcoin

MOBILE WALLET



- WoS
- breez wallet
- blue wallet
- Altana
- Green
- Phoenix
- SBW
- Samourai
- Electrum
- Edge

Villaggio Bitcoin

HARDWARE WALLET

- BitBox02
- Coldcard
- KeepKey
- Ledger Nano S
- Trezor Model T
- Trezor One
- Portal

Jade

Villaggio Bitcoin

HARDWARE WALLET

Blockstream JADE

VillaggioBitcoin

HARDWARE WALLET

NOW AVAILABLE

BitBox02

Swiss made open source

Secure dual-chip architecture
Full Open Source
Bitcoin-only edition
Easy backup

Villaggio**Bitcoin**

Rivenditore ufficiale

VILLAGGIO BITCOIN SHOP

WWW.VILLAGGIOBITCOIN.IT

Villaggio**Bitcoin**

HARDWARE WALLET

Portal

hardware wallet

Villaggio **Bitcoin**

WALLET: altre tipologie

Paper wallet

Brain wallet

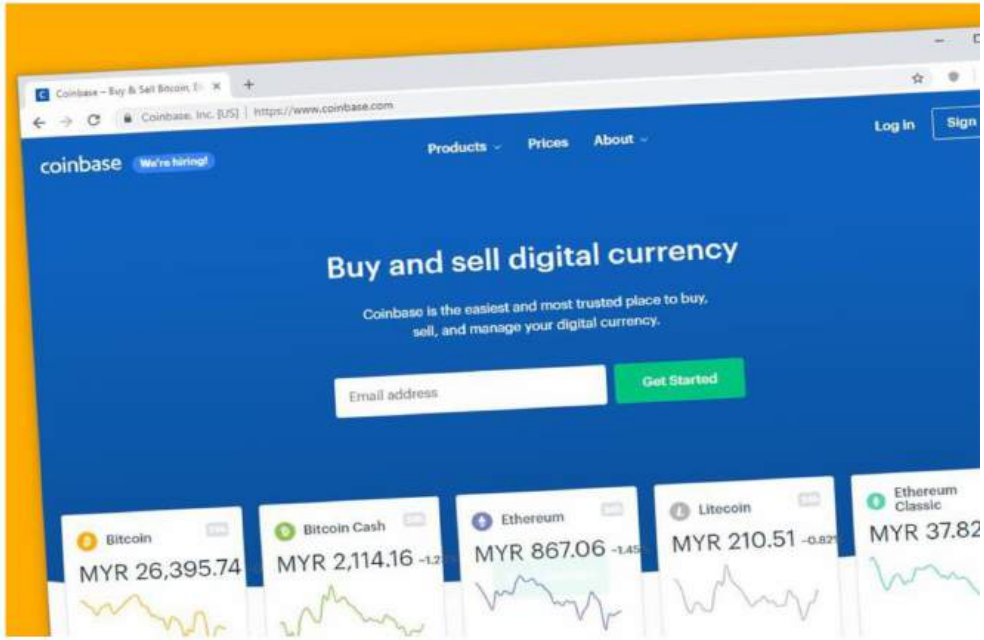
- Memorizzazione chiavi
- Basso livello sicurezza
- Non adatto per trasferimento fondi

Villaggio Bitcoin

WEB WALLET

CUSTODIAL!

Exchange e piattaforme «crypto»



Villaggio Bitcoin

HOT or COLD WALLET?

WALLET TYPE	HOT	COLD
Mobile wallet		
Desktop wallet		
Hardware wallet		
Paper wallet		
Brain wallet		
Web wallet	 **TOTALMENTE CUSTODIAL** **I bitcoin non sono vostri!**	

Villaggio Bitcoin

LE FEE DI TRANSAZIONE

RICOMPENSA PER I MINERS
2 contributi:

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

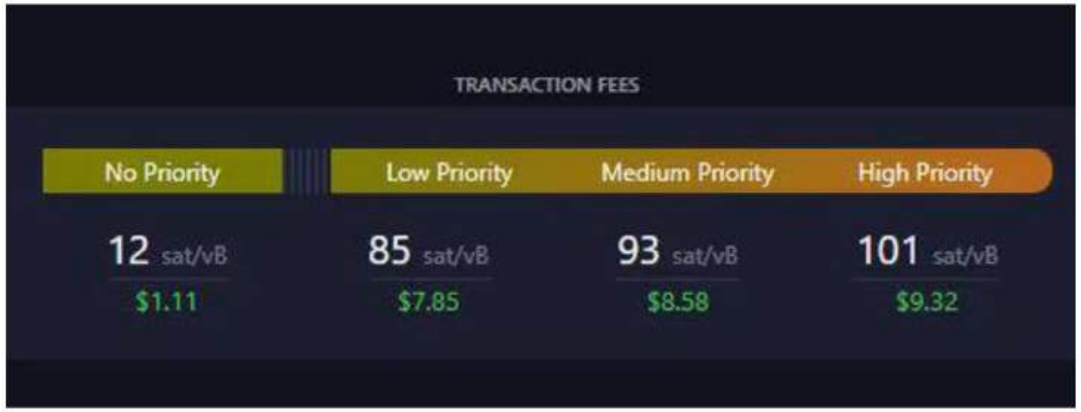
IMPOSTARE LE FEE DI TRANSAZIONE

RICOMPENSA PER I MINERS:

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

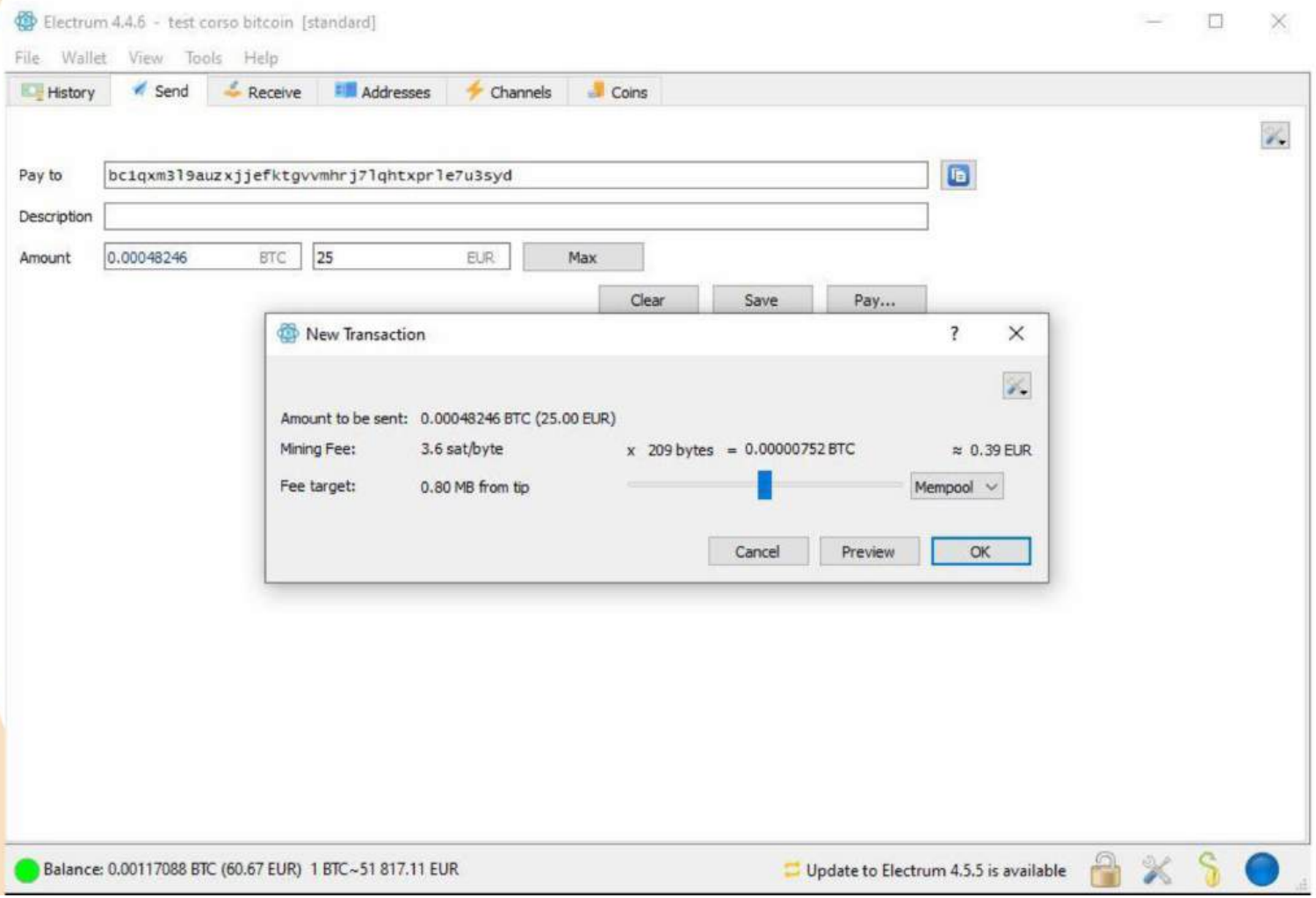
+

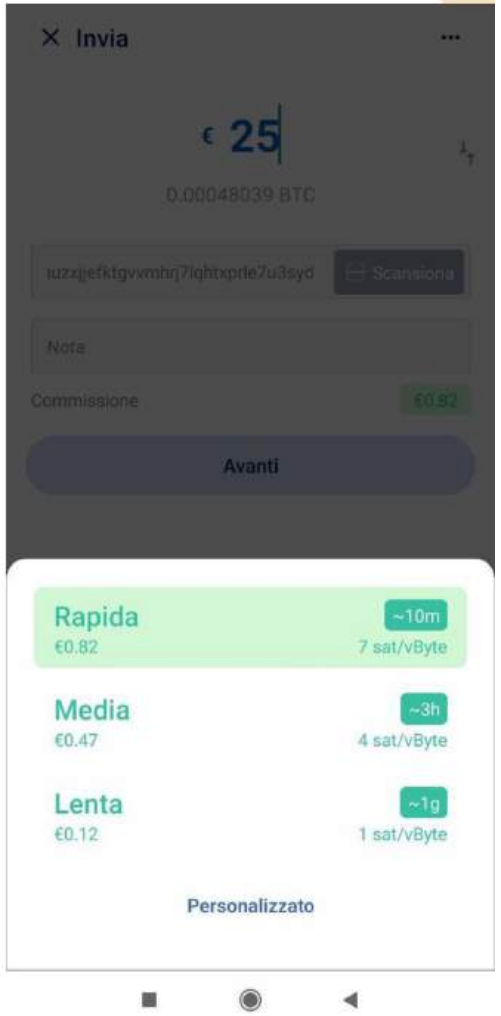
2. **Commissioni** di tutte le transazioni incluse in quel blocco (**variabile**)



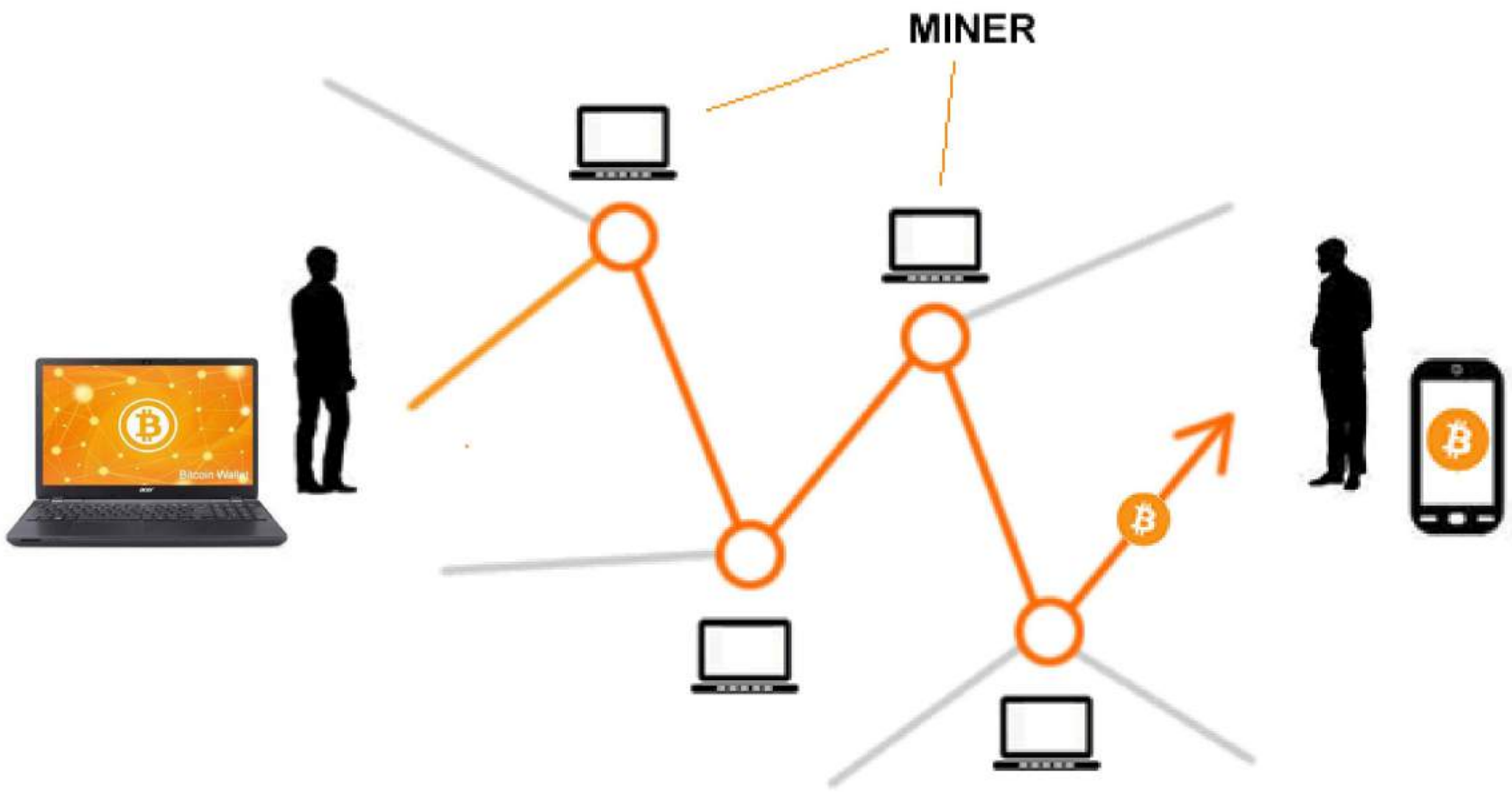
Villaggio Bitcoin

IMPOSTARE LE FEE DI TRANSAZIONE





IN ACTION!



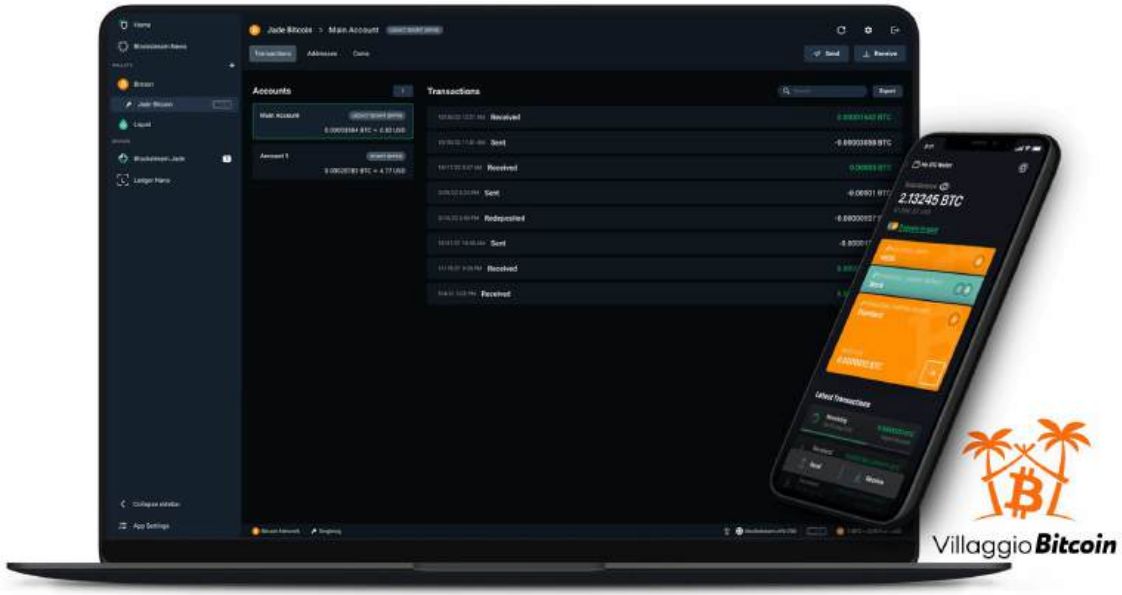
Villaggio Bitcoin

SICUREZZA E PRIVACY

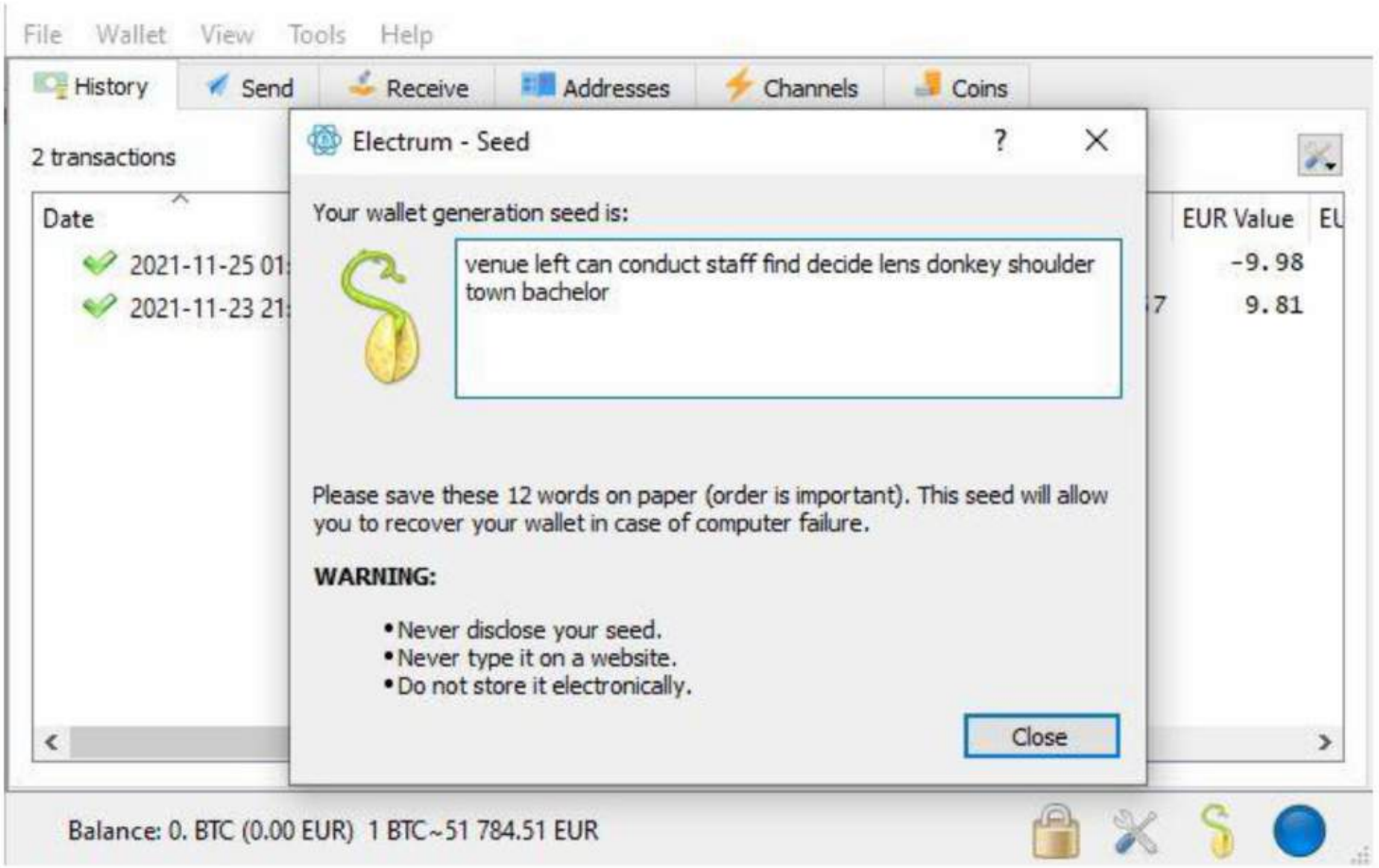
KEEP IN MIND:

«*Not your Key? Not your Coin*!»

- Decidi la tua strategia
- Impara le prassi di sicurezza
- Custodisci BENE il seed



IL SEED



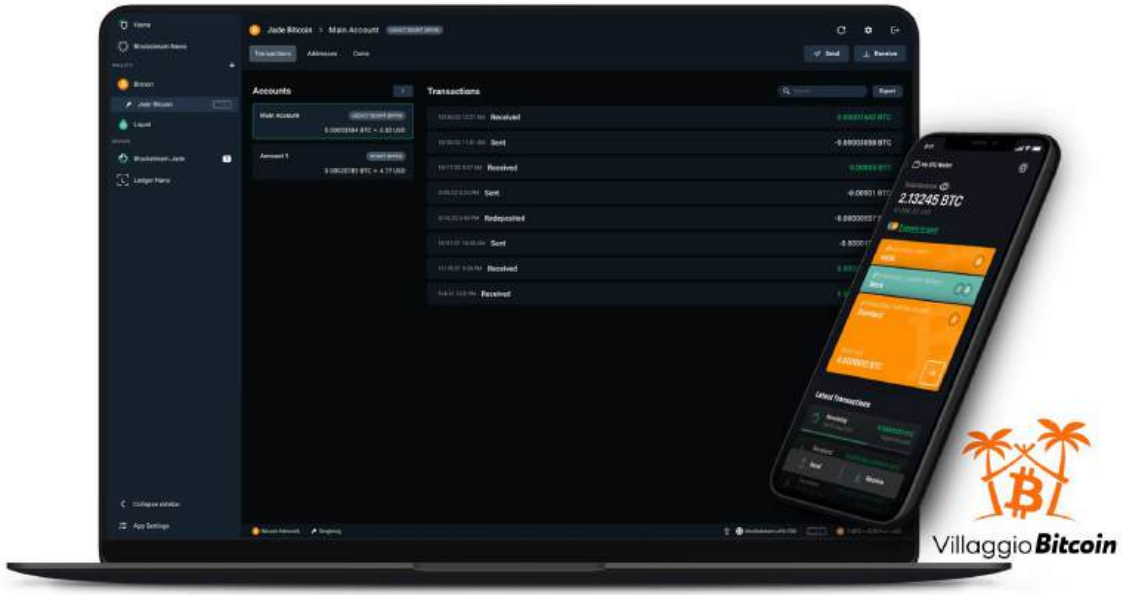
Villaggio Bitcoin

SICUREZZA E PRIVACY

KEEP IN MIND:

«*Not your Key? Not your Coin*!»

- Decidi la tua strategia
- Impara le prassi di sicurezza
- Custodisci BENE il seed
- Tutela la tua privacy
- Ricordati che devi morire :)



MODULO 3. IL WALLET BITCOIN

L'utilizzo pratico dell'oro digitale

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

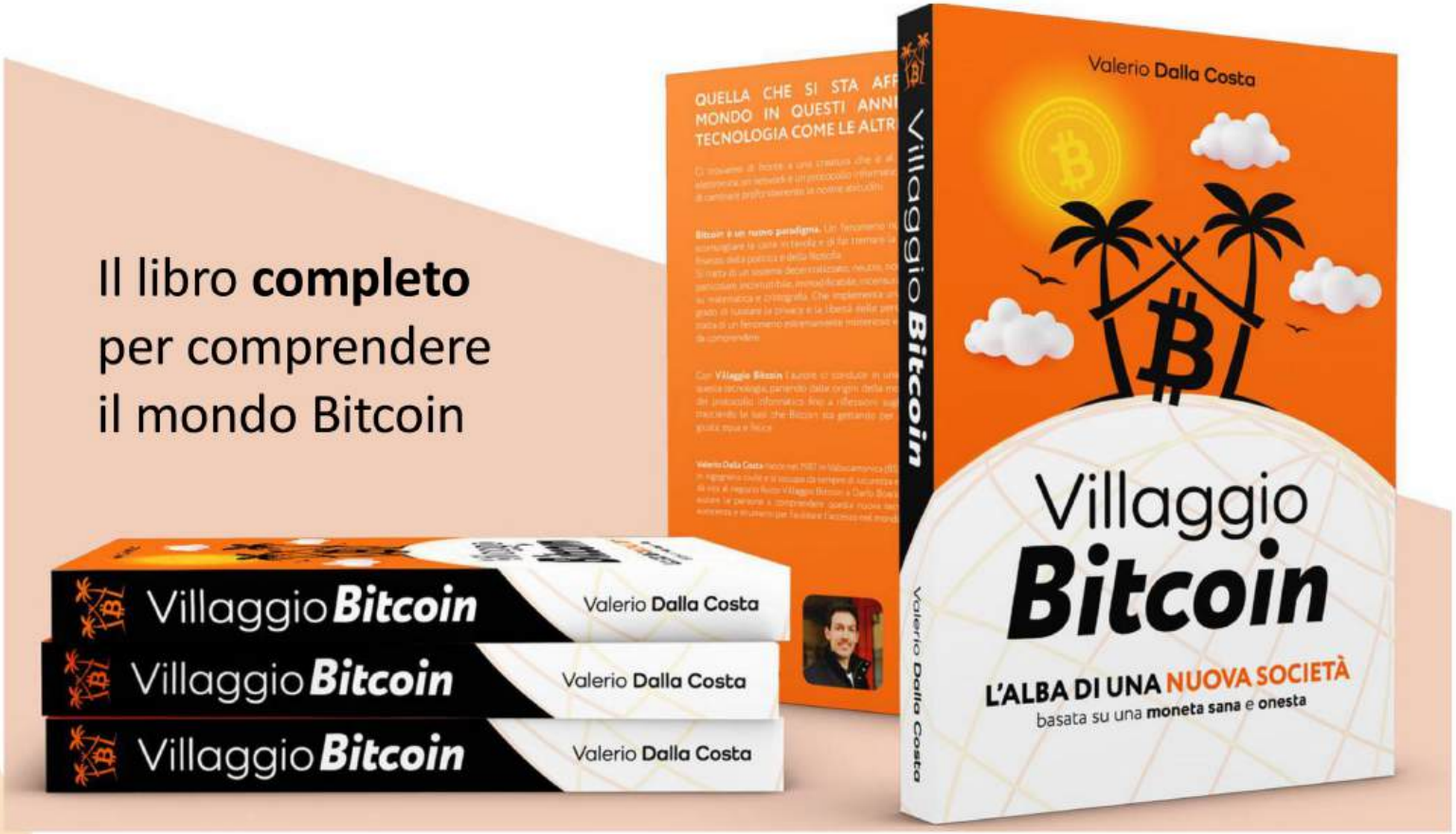
Modulo 3

Modulo 4

Bitcoin book

Villaggio Bitcoin

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



AVAILABLE ON:

amazon

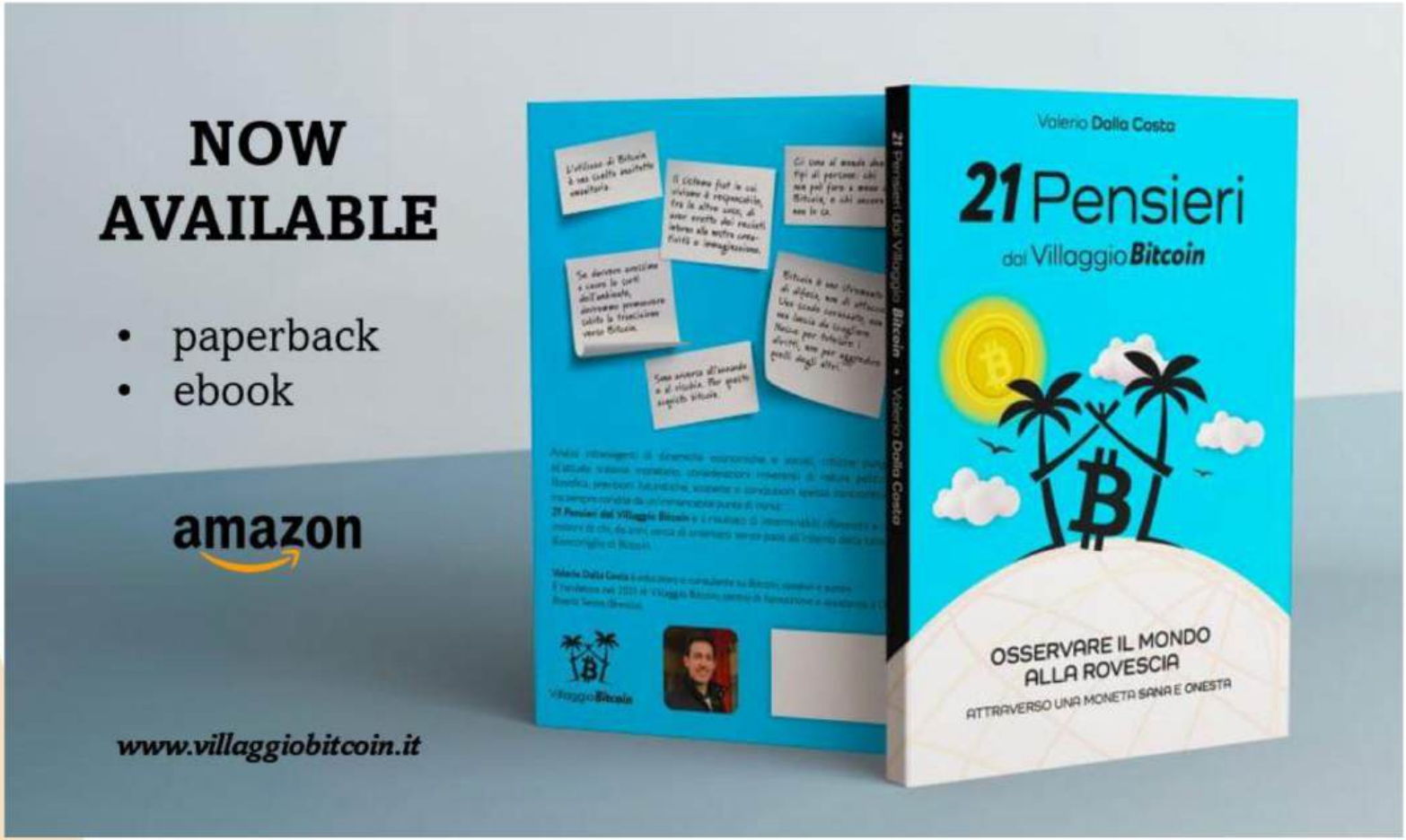
USEMLAB
ECONOMIA E MERCATI

VillaggioShop
villaggiobitcoin.it

Villaggio Bitcoin

Bitcoin book

21 Pensieri



Un testo per interpretare il fenomeno **Bitcoin**

amazon

VillaggioShop

villaggiobitcoin.it

Villaggio Bitcoin