

# MODULO 3. IL WALLET **BITCOIN**

L'utilizzo pratico dell'oro digitale



# 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

# ECOSISTEMA BITCOIN

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



## TEORIA DEI GIOCHI



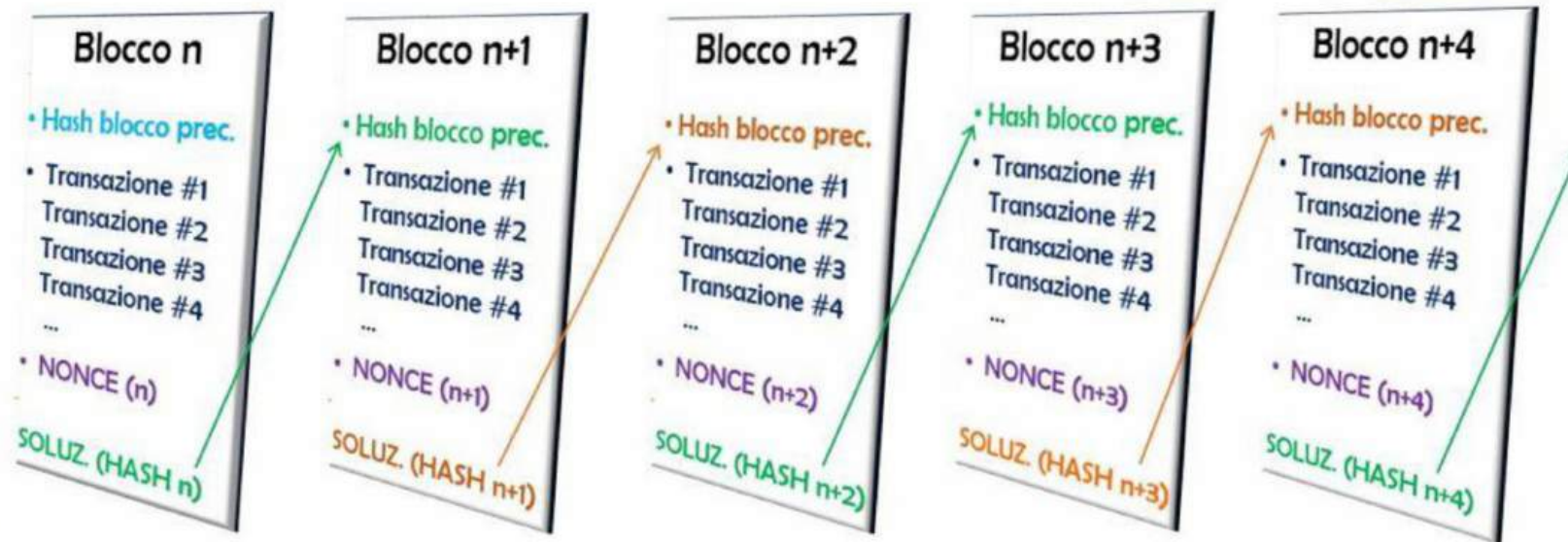
# BITCOIN: LA BLOCKCHAIN

## Risoluzione problema double-spending

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



CONSENSO  
DISTRIBUITO

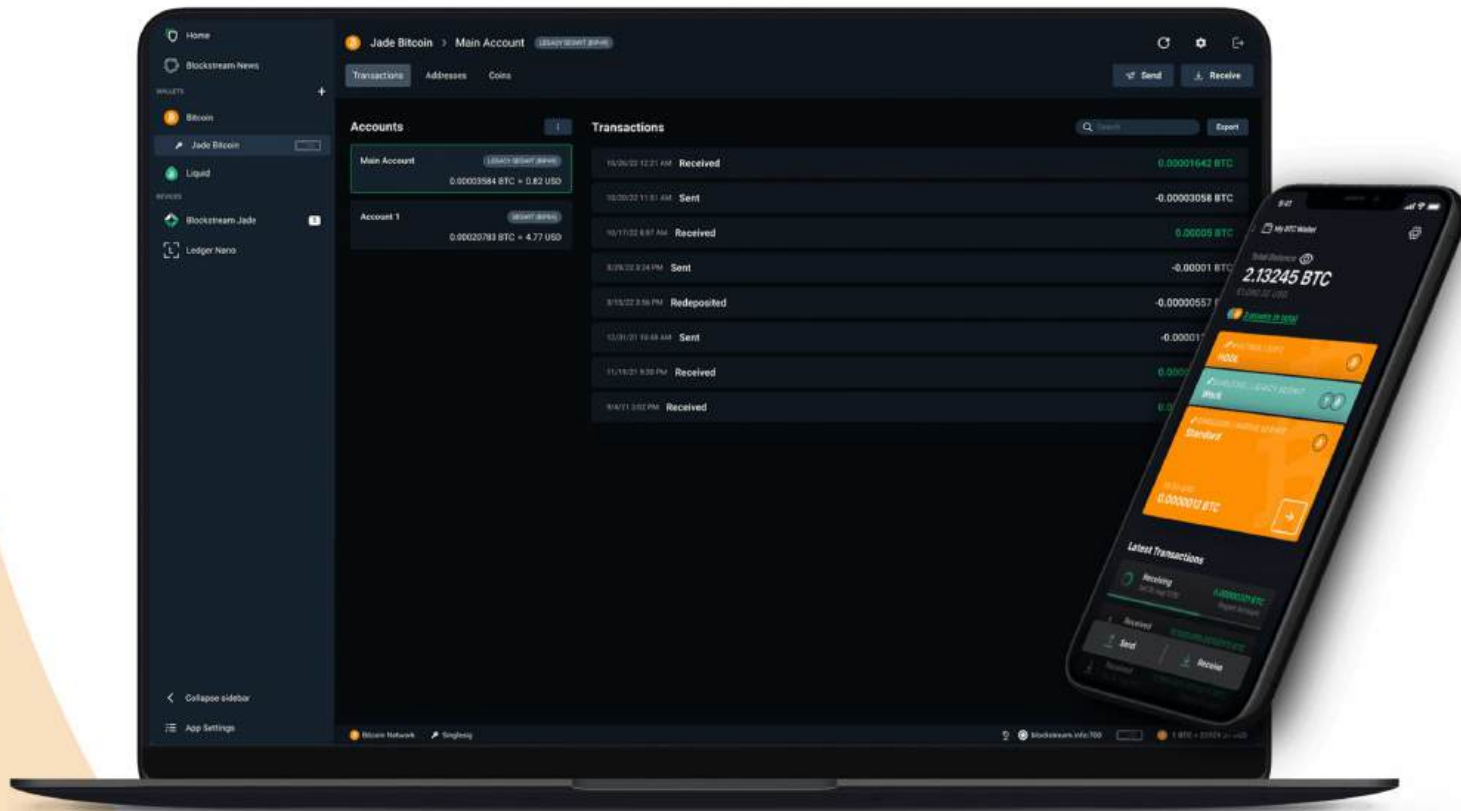


# LE TRANSAZIONI STEP BY STEP

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



# WALLET BITCOIN



# CRITTOGRAFIA ASIMMETRICA

- Coppia di chiavi **Privata** e **Pubblica**
- Chiave **Privata**  $\xrightarrow{\text{DERIVA}}$  Chiave **Pubblica**  $\xrightarrow{\text{DERIVA}}$  **Indirizzo bitcoin**

<https://www.bitaddress.org>

Private Key (Wallet Import Format)

**SECRET**



5KXSPRN5BR1tLV7ro8qtBVGrCiBq3nYJjNhMiHjKDCh3pxXynTV



Bitcoin Address



**SHARE**

19GBnmEGSpC3hJQExJwQfDAVSEx6agN9X1



# INDIRIZZI **BITCOIN**

Chi li assegna?

## Noi stessi... a caso!

- Generazione entropia

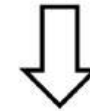


- SHA256, RIPEMD160
- Secp256k1 – ECDSA
- Base58check (bech32)
- Collision-resistant



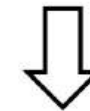
bc1q5shngj24323nsrmxv99st02na6srekfctt30ch

ENTROPIA



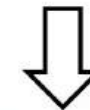
Kwsmqow4bidFNsETYd1NPxZmxDWCHHq54WEnybfXo5vXoqhU8J4x

Chiave privata (**k**)



$$K = G * k$$

Chiave pubblica (**K**)



Indirizzo Bitcoin



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*):

- **bc1**q7cyrfmck2ffu2ud3rn5l5a8yv6f0chkp0zpemf
- **bc1**qqkjdahh55hzrxa79637jkz3ujsq09s2t6eg4f6
- **3**CsPq8YUymGyezXhvcyUXrvpAyawSWfmEr
- **3**Q4o9hGfN4qYaE97CSRdqFBpUznoQMtXWF
- **1**7JC56XYjVf47iHsZHhZgTzhG62HGvbs3a
- **1**AuN3JZtVbYHi5War7qoS75z6VMfvnE1F6



# 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!** »

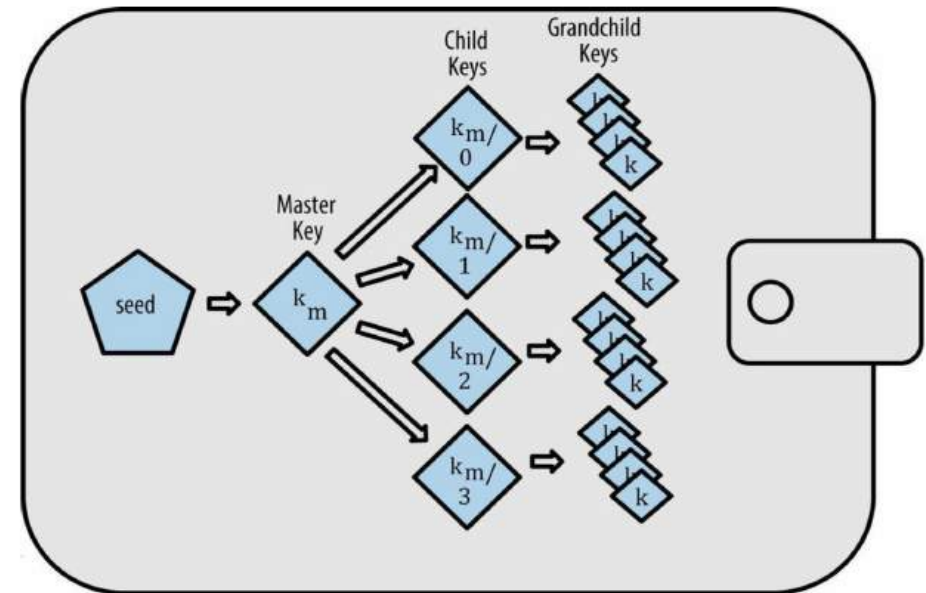
# IL SEED

## 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!



# 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



Breez wallet



Phoenix



Blue wallet



BitPay



Green



BLW



Blink



BRD



Eclair Mobile



Edge



Electrum

paper  
brain  
web



Villaggio **Bitcoin**

# IL SEED

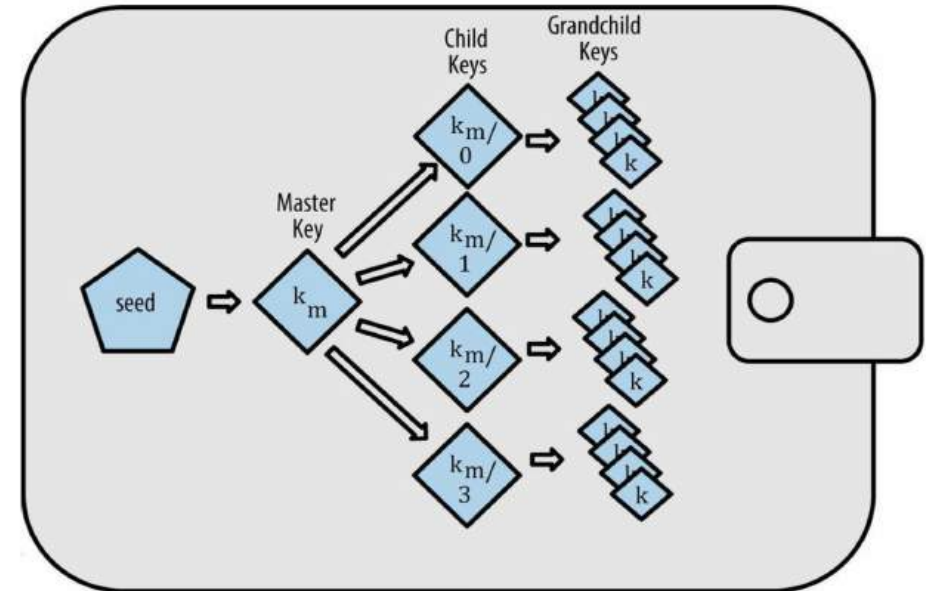
## HD wallet

- 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

• HD wallet vs  
Non deterministic (JBOK)



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



# 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



Breez wallet



Phoenix



Blue wallet



BitPay



Green



BLW



Blink



BRD



Eclair Mobile



Edge



Electrum

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": ""  
}
```



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



# IL WALLET: TIPOLOGIE

• HD wallet **vs**  
Non deterministic (JBOK)

• Lightweight wallet (SPV) **vs**  
Full node

• Custodial **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



Breez wallet



Phoenix



Blue wallet



BitPay



Green



BLW



Blink



BRD



Eclair Mobile



Edge



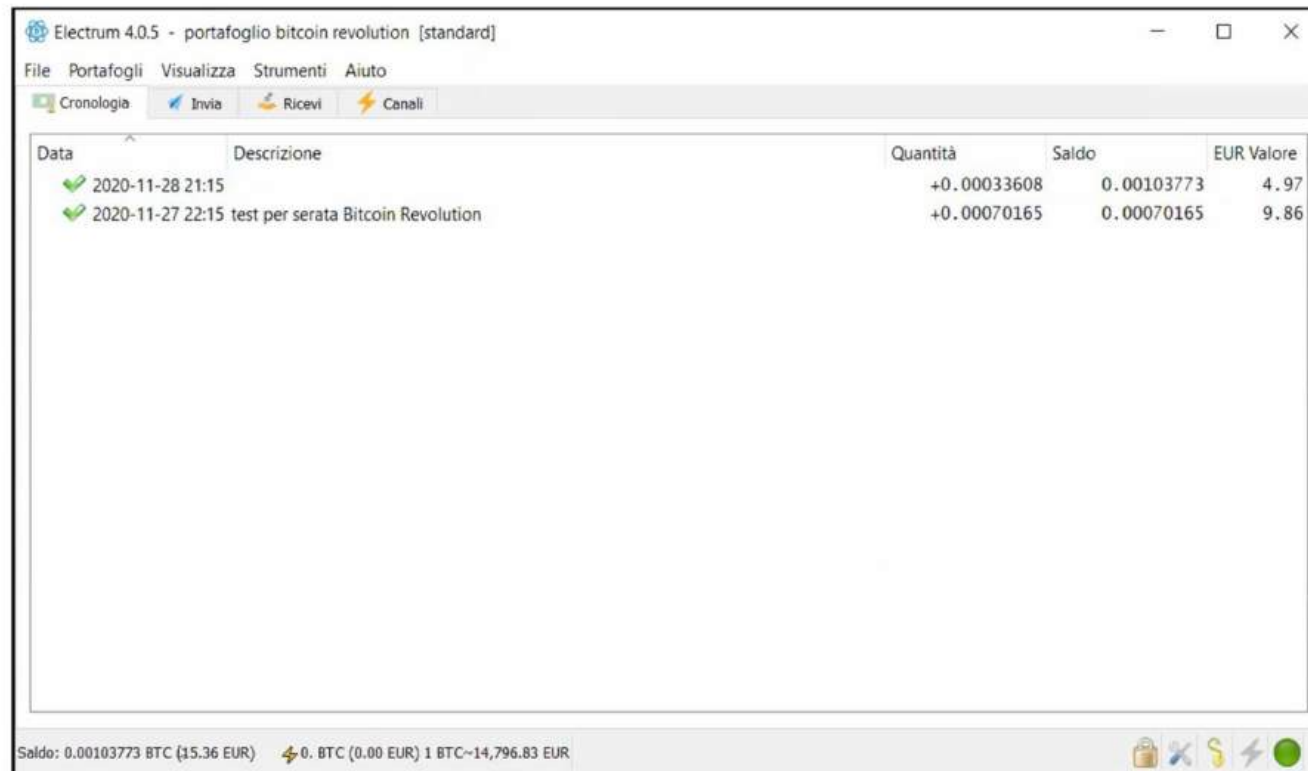
Electrum

paper  
brain  
web



Villaggio **Bitcoin**

# DESKTOP WALLET



Electrum 4.0.5 - portafoglio bitcoin revolution [standard]

File Portafogli Visualizza Strumenti Aiuto

Cronologia Invia Ricevi Canali

Data	Descrizione	Quantità	Saldo	EUR Valore
✓ 2020-11-28 21:15		+0.00033608	0.00103773	4.97
✓ 2020-11-27 22:15	test per serata Bitcoin Revolution	+0.00070165	0.00070165	9.86

Saldo: 0.00103773 BTC (15.36 EUR) 0 BTC (0.00 EUR) 1 BTC ~14,796.83 EUR



Specter wallet



Bitcoin Core



BitPay



Electrum



Wasabi

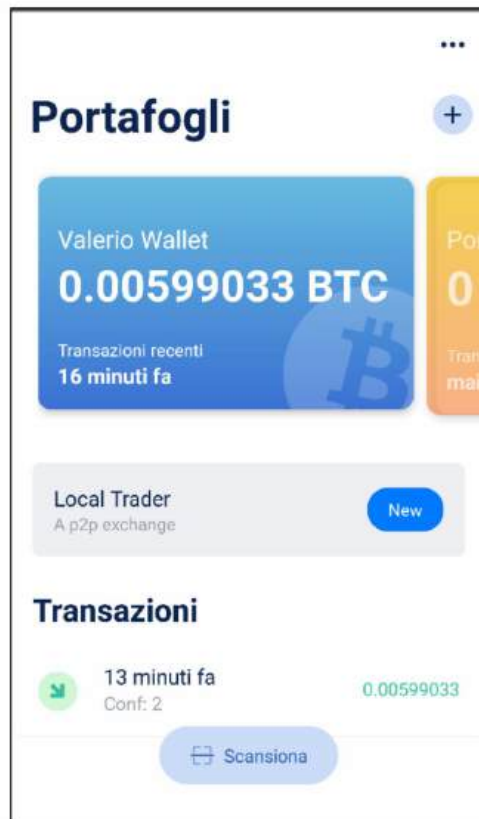












Sparrow



Green

# MOBILE WALLET



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

# HARDWARE WALLET



 BitBox02

 Coldcard

 KeepKey

 Ledger Nano S

 Trezor Model T

 Trezor One

 Portal



 Jade



# HARDWARE WALLET

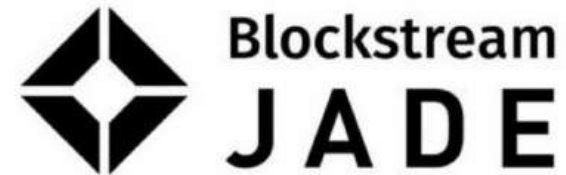
VILLAGGIO BITCOIN  
RIVENDITORE UFFICIALE

## JADE

- ◆ FUNZIONALITÀ QR AIR-GAPPED
- ◆ VIRTUAL SECURE ELEMENT
- ◆ BIP39 PASSPHRASE
- ◆ MULTISIGNATURE WALLETS

...E ALTRO ANCORA!

DISPONIBILE ORA  
SUL NOSTRO **ONLINE SHOP**  
[WWW.VILLAGGIOBITCOIN.IT](http://WWW.VILLAGGIOBITCOIN.IT)



# 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.VILLAGGIOWITCOIN.IT](http://WWW.VILLAGGIOWITCOIN.IT)



Villaggio **Bitcoin**

# HARDWARE WALLET



**Portal**  
hardware wallet



# WALLET: altre tipologie

## Paper wallet



## Brain wallet



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

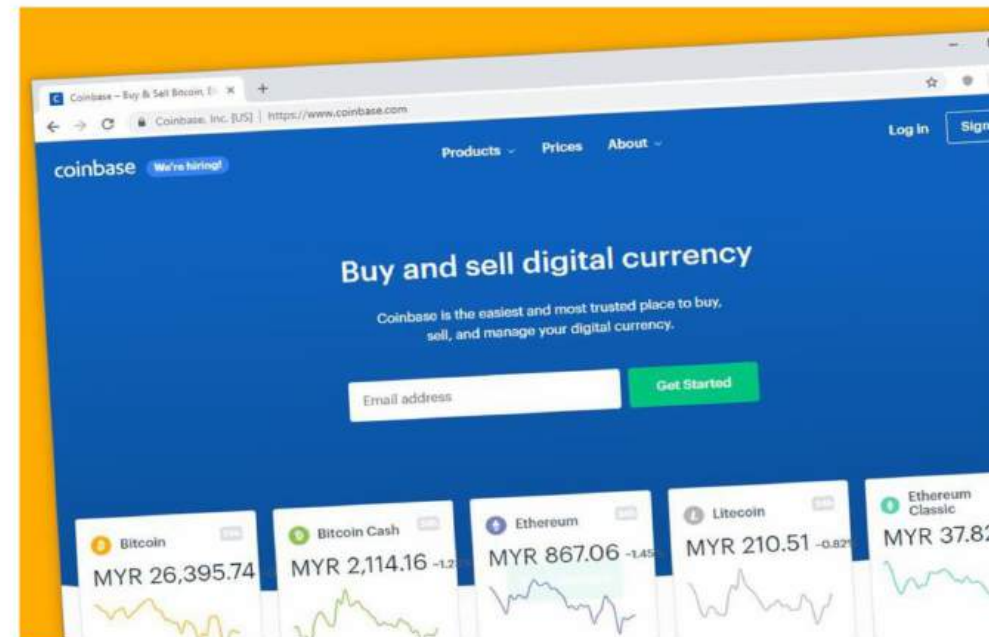


# WEB WALLET







**CUSTODIAL!**

Exchange e piattaforme «crypto»



# HOT or COLD WALLET?

WALLET TYPE	HOT	COLD
Mobile wallet		
Desktop wallet		
Hardware wallet		
Paper wallet		
Brain wallet		
Web wallet		<b>TOTALMENTE CUSTODIAL</b> <b>I bitcoin non sono vostri!</b>

# 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

# 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**)

TRANSACTION FEES			
No Priority	Low Priority	Medium Priority	High Priority
12 sat/vB	85 sat/vB	93 sat/vB	101 sat/vB
\$1.11	\$7.85	\$8.58	\$9.32



# IMPOSTARE LE FEE DI TRANSAZIONE

The screenshot shows the Electrum 4.4.6 desktop application interface. The main window displays a transaction confirmation dialog titled "New Transaction". The dialog shows the following details:

- Amount to be sent: 0.00048246 BTC (25.00 EUR)
- Mining Fee: 3.6 sat/byte x 209 bytes = 0.00000752 BTC ≈ 0.39 EUR
- Fee target: 0.80 MB from tip (with a slider and "Mempool" dropdown)

Buttons for "Cancel", "Preview", and "OK" are visible at the bottom of the dialog. The main window also shows the "Pay to" field with the address "bc1qxm319auzxxjefktgvmhrj71qhtxpr1e7u3syd", the amount "25 EUR", and a status bar at the bottom indicating a balance of 0.00117088 BTC (60.67 EUR) and a notification for an update to Electrum 4.5.5.

The screenshot shows the Invia mobile application interface. The main screen displays a transaction confirmation screen with the following details:

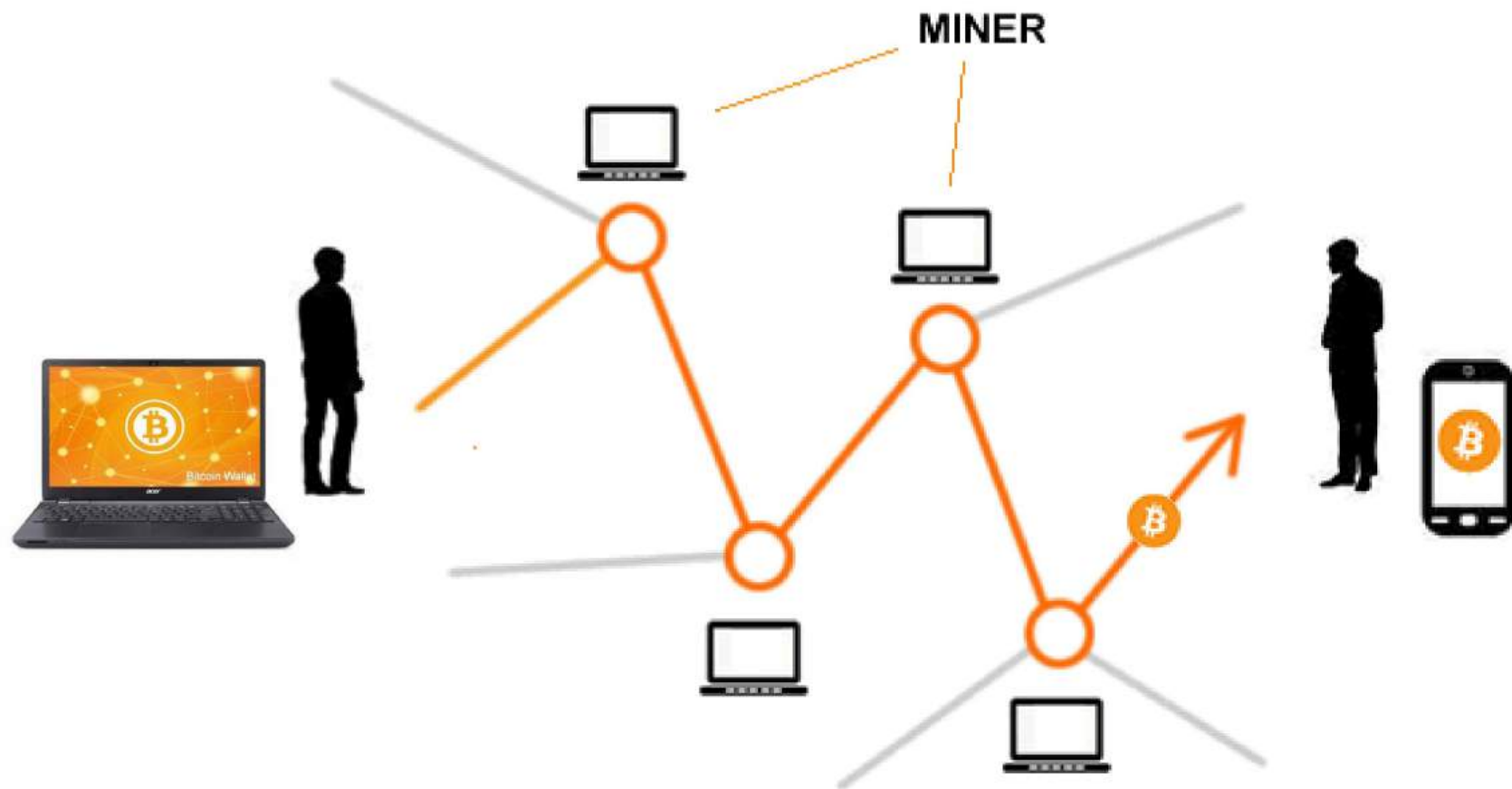
- Amount: € 25 (0.00048039 BTC)
- Address: uzzjefktgvmhrj71qhtxpr1e7u3syd
- Commissione: €0.82

Buttons for "Avanti" and "Scansiona" are visible. Below the main screen, there are three transaction fee options:

- Rapida**: €0.82, ~10m, 7 sat/vByte
- Media**: €0.47, ~3h, 4 sat/vByte
- Lenta**: €0.12, ~1g, 1 sat/vByte

A "Personalizzato" option is also visible at the bottom.

# IN ACTION!





# IL SEED



The screenshot shows the Electrum wallet interface with a dialog box titled "Electrum - Seed" open. The dialog displays the generated seed words: "venue left can conduct staff find decide lens donkey shoulder town bachelor". Below the seed, there is a warning section with the following text:

Please save these 12 words on paper (order is important). This seed will allow you to recover your wallet in case of computer failure.

**WARNING:**

- Never disclose your seed.
- Never type it on a website.
- Do not store it electronically.

The background shows the wallet's history and balance. The balance is 0 BTC (0.00 EUR) and 1 BTC (~51,784.51 EUR). The status bar at the bottom includes icons for a lock, tools, a seed, and a globe.

Date	EUR Value	EU
2021-11-25 01:00	-9.98	
2021-11-23 21:00	9.81	



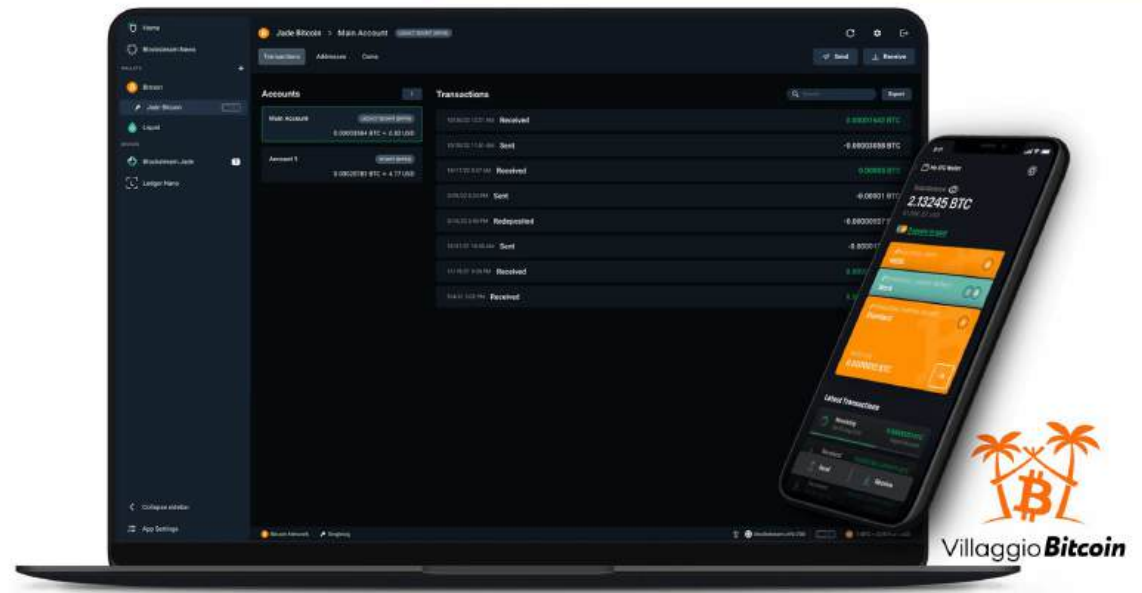
# SICUREZZA E PRIVACY



**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**



[www.villaggiobitcoin.it](http://www.villaggiobitcoin.it)



351 6755119



[info@villaggiobitcoin.it](mailto:info@villaggiobitcoin.it)



[t.me/villaggiobitcoin](https://t.me/villaggiobitcoin)

# Corso base su **Bitcoin**



Villaggio **Bitcoin**

## Modulo 1



## Modulo 2



## Modulo 3



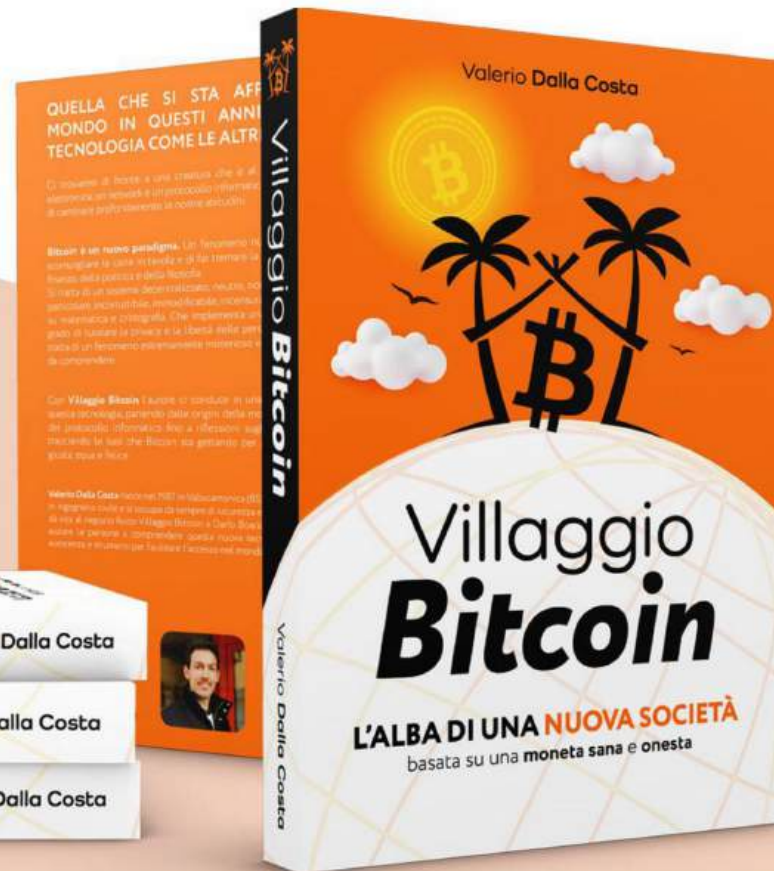
## Modulo 4



# Bitcoin book

# Villaggio Bitcoin

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



AVAILABLE ON:

amazon

USEMLAB  
ECONOMIA E MERCATI

VillaggioShop  
villaggioitcoin.it



# Bitcoin book

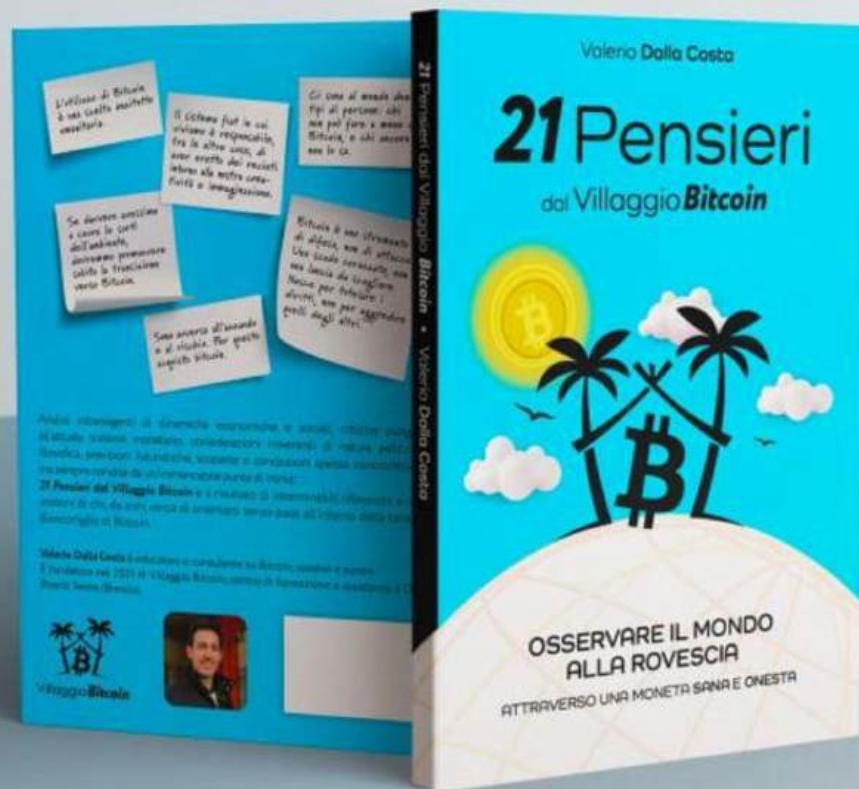
## 21 Pensieri

**NOW  
AVAILABLE**

- paperback
- ebook

**amazon**

[www.villaggiobitcoin.it](http://www.villaggiobitcoin.it)



Un testo per interpretare il fenomeno **Bitcoin**

**amazon**

**VillaggioShop**

[villaggiobitcoin.it](http://villaggiobitcoin.it)



Villaggio **Bitcoin**