



## WEBINAR

*18 novembre 2020*

Zoom Video Conference

# BLOCKCHAIN, BITCOIN & CRYPTOASSET

## ASPETTI TECNOLOGICI E QUESTIONI GIURIDICHE

*Paolo Dal Checco*

*Consulente Informatico Forense*

# Chi sono

- ❑ PhD @UniTO nel gruppo di Sicurezza delle Reti e degli Elaboratori
- ❑ Passato di R&D su crittografia e sicurezza delle comunicazioni
- ❑ Consulente Informatico Forense, Perizie Informatiche per Privati, Aziende, Avvocati, Procure, Tribunali, F.F.O.O.
- ❑ Albo CTU e Periti del Tribunale di Torino, Periti ed Esperti CCIAA TO
- ❑ Piccole Docenze a Contratto @UniTO, @UniMI e @UniGE
- ❑ Tra i fondatori dell'Associazione ONIF ([www.onif.it](http://www.onif.it))
- ❑ Socio IISFA, Tech & Law, Clusit, Assob.It, Lab4INT

# Un ripasso veloce

- La maggior parte delle notizie ed informazioni su Bitcoin e criptovalute si basano su errate percezioni, bufale, leggende metropolitane e scarsa comprensione dello strumento.



# Un ripasso veloce

- **Chiave privata:** 256 bit, il codice da cui viene generato l'indirizzo, passando tramite la chiave pubblica generata da quella privata. Posso dimostrare di averla firmando un messaggio.
- **Chiave pubblica:** 512 bit, derivata dalla chiave privata tramite algoritmo a chiave pubblica/privata ECDSA a Curve Ellittiche. Posso verificare un messaggio firmato con chiave privata.
- **Indirizzi/address bitcoin:** 160 bit, 27-34 caratteri alfanumerici eccetto alcuni. Gli indirizzi vengono derivati dalle chiavi pubbliche dell'utente, derivate dalle chiavi private.

Private Key (Wallet Import Format)

**SECRET**



5KkrPXWACDU6JnRi6kuEokPr1rEFAF6pJdLQzExxSFwD5oicaVP

Bitcoin Address

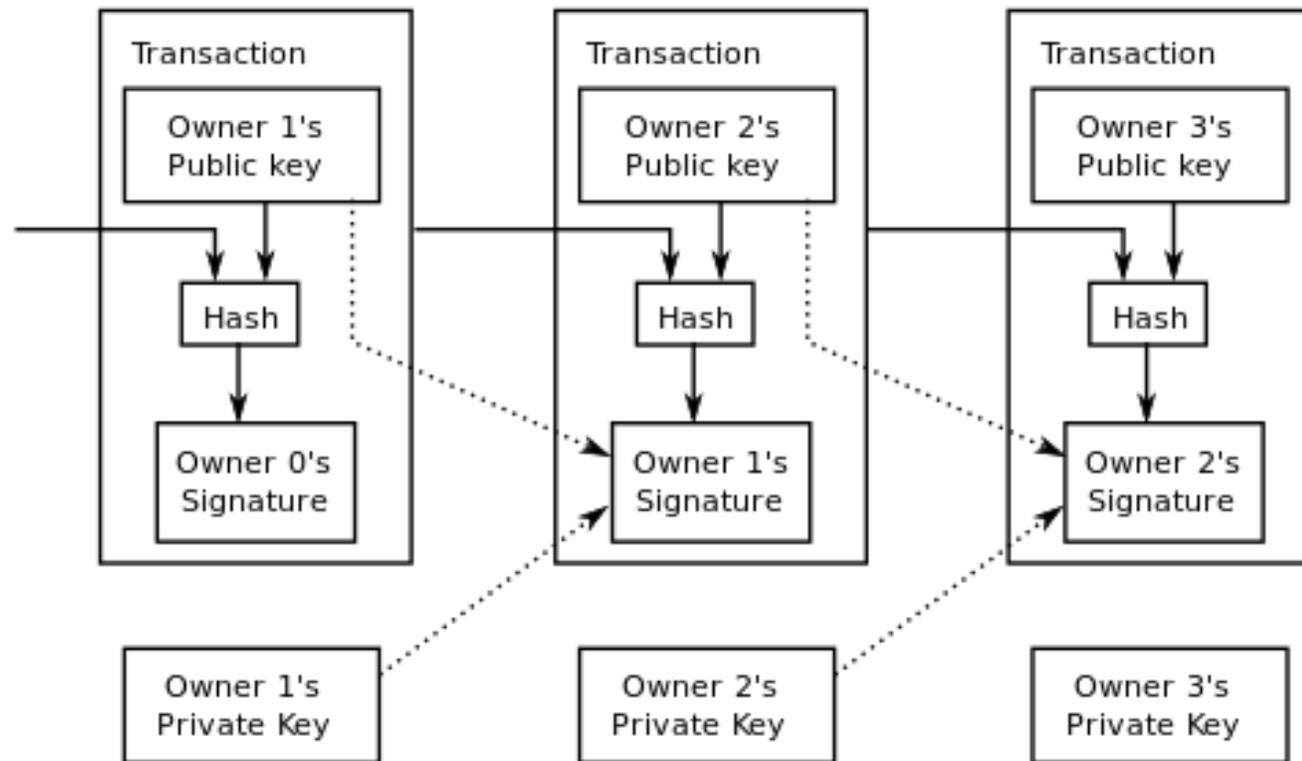


**SHARE**

12St5js5pT18iMybf1TxghbAzLsH4yqYng

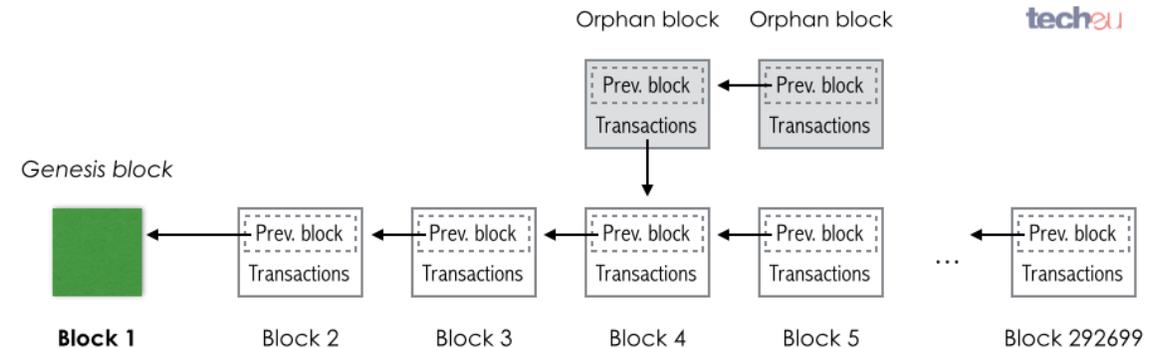
# Un ripasso veloce

- **Transazione:** passaggio irreversibile di una certa quantità di bitcoin da un indirizzo all'altro, che viene trasmessa dal client alla rete, inserita nella blockchain e diventa pubblica



# Un ripasso veloce

- **Blockchain:** il libro mastro delle transazioni, pubblico, condiviso, decentralizzato, viene composto autonomamente in base al concetto di “proof of work”
- **Wallet:** Il portafoglio che raccoglie i diversi indirizzi/address bitcoin, più facile da gestire rispetto a lavorare direttamente con gli indirizzi. In genere protetto da password. Può essere gerarchico deterministico.



# Quando non si ha nulla da nascondere

- La blockchain è «trasparente», mantiene i legami tra le transazioni
- Si riesce facilmente a fare aggregazione (clustering) degli indirizzi
- Gli utenti non si nascondono dietro indirizzi IP anonimi (VPN, Tor, etc...)
- Le transazioni non avvengono tramite mixer/tumble
- Gli utenti mantengono gli stessi wallet

# Quando si vogliono nascondere le tracce

- Le transazioni sono slegate tra di loro
- Non è possibile aggregare indirizzi e ricostruire wallet
- Gli indirizzi IP utilizzati dagli utenti sono anonimi
- Vengono utilizzati sistemi di anonimizzazione come mixer/tumbler
  - [bitcoinmix.org](https://bitcoinmix.org)
- Vengono utilizzati wallet che mixano i bitcoin
  - Samurai Wallet con Whirpool
  - Wasabi Wallet
- Gli utenti cambiano continuamente indirizzi e wallet

# Come vengono “ripuliti” i bitcoin

## How To Clean Your Coins

Step 1

**Deposit  
Bitcoin**



Step 2

**Withdraw  
Bitcoin**

- Tumblers/Mixers via web anche su Tor con Onion address
- Attenzione che non tutti i tumbler funzionano
- Attenzione che non si sa chi ci sia dietro i tumbler

# Come vengono “ripuliti” i bitcoin



## MIXER PER BITCOIN

---

Bitcoin Mixer (Blender) è qualcosa che ti aiuta a rimescolare i tuoi bitcoin utilizzando i nostri algoritmi e a proteggere la tua identità.

# Come vengono “ripuliti” i bitcoin

The screenshot shows the flyp.me website interface. At the top, there is a navigation bar with the logo 'flyp.me' and links for 'ABOUT US', 'API', 'FAQ', 'CONTACT US', 'HOW IT WORKS', 'TOP CRYPTOCURRENCIES', and a language selector set to 'English'. The main heading reads 'Accountless Crypto Exchanger.' with the tagline 'Simple, Fast and Private. No registration.' Below this is a transaction form. On the left, under 'I HAVE', the amount '0.02768336' is shown next to a Bitcoin icon and 'BTC'. Below this, it says 'Min: 0.00000972 BTC · Max: 0.02768336 BTC'. On the right, under 'I GET', the amount '1463.305976' is shown next to a PPC icon and 'PPC'. Below the transaction details, there is a 'HOW IT WORKS' section with a question mark icon and the text 'Price is final. All fees included. You get what you want.' To the right of this section are two input fields: 'PPC WALLET ADDRESS' with the placeholder 'Enter destination wallet address' and a QR code icon, and 'BTC REFUND WALLET ADDRESS (OPTIONAL)' with the placeholder 'Enter refund wallet address' and a QR code icon. At the bottom of the form is a large button labeled 'FLYP NOW'.

# Come venivano “ripuliti” i bitcoin in origine

**WITHDRAW BITCOIN**

Withdraw to this address:

Amount to withdraw:  Your balance: 0.00480000

Minimum amount: 0.001 BTC

A 0.0001 BTC transaction fee will be deducted from your withdrawal amount. This will be paid as a fee to the Bitcoin network and ensure priority handling of your withdrawal. You can't withdraw unless you have made at least one deposit and all your deposits have received confirmations from the Bitcoin network.

**CASH OUT**

HOW TO PLAY VERIFICATION CONTACT

SATOSHI CIRCLE SATOSHI SLOT

ONLINE

**SATOSHI DICE**  
THE BIGGEST BITCOIN GAME IN THE UNIVERSE

**BET NOW!**

PLAYED TODAY  
**40 Games**

WON TODAY  
**2 BTC**

RECENT BETS

- 1BHJNKnd bet  
0.01 btc (12 minutes ago)
- 1BHJNKnd bet  
0.01 btc (12 minutes ago)
- 1BHJNKnd won  
0.0122506 btc (19 minutes ago)
- 1BHJNKnd won

COINS!

Your Balance (0.0048 unconfirmed)

**DEPOSIT** **0.00000000** **CASHOUT**

Your Personal Deposit Address

**1Bw2Y4L4FKgjHPkBCtmf3Nu6e7mrPrqn3e**

# Le transazioni sono comunque complesse

12EFijBVj3PEQZyoBBVr3ocQe1XFYJqxqz (€ 3,159.91 - Output)  
 1AiN1RrXmBhZSPZdoi8goABP7UTZgrbFL (€ 2.74 - Output)  
 1NTaCpQQ3v6QZauVTxSeyDMeQFeVKtuLCW (€ 2.88 - Output)  
 145dDzvALbGUcJnhM1LRTGXU8EsaVQEvFa (€ 2,812.75 - Output)



1FBmDBUgS1gTSd7G8AE4H3wrHz81M1NcNL - (Spesi)	€ 333.16
1CozRs4pzTFFZjbKGd2XNRJpeqMWqts7Wp - (Spesi)	€ 2.74
1Bgvrh2i3FNFRreXukACZgfVpKk1f1LuZt - (Spesi)	€ 381.21
1BDbraoxzHJGdoP5xXW3hXTch55cCBPCsQ - (Spesi)	€ 2.82
1CnsCszPrnRGyvmokLbVfVNGfPB8LBJAs - (Spesi)	€ 368.27
1NVcLcK34d1UXADadwsNobXZxmYDfzcZZT - (Non spesi)	€ 2.74
1KgznlvPB2EVhFQk1KAn2jugkwHhVfXqon - (Spesi)	€ 349.21
14shDhLhJ4czVxwA6yDhimFpcvKnggb65V - (Spesi)	€ 3.01
13yUQQwUuAkQEWSMmRYbbL9skzDSNYHTC9 - (Spesi)	€ 2.47
1AL6QDpoKDSr6TQ3zeVwYgQTcQ2QkCU2yi - (Spesi)	€ 348.56
1EBC2k92WtHbDWVY5wkZyL3NCeHLdeoUGb - (Spesi)	€ 3.01
1N53PG9SsXqf9NNjsMNZR2Bk76UcpAqWqe - (Spesi)	€ 348.84
1K2YSRBAUiR2Xwjy171jUfoWP4xhy5MKfp - (Spesi)	€ 369.20
1Kh3QaxseBiRcsjojYHkdHRMNmgdDQgjAt - (Spesi)	€ 353.46
1GY844iv59QSACfD7XomGcf4iZeCnv2YRZ - (Non spesi)	€ 341.82
1LkRypTeoD5c2wgnvTAWy9VGDWcU4xcfr - (Spesi)	€ 366.81
1zFBsknwMiPMs2h5ZNyWy8SWMysHts5fU - (Spesi)	€ 342.22
15xzXZCVyVuNkzthSXjc4NWPYZqKGWjFCM - (Spesi)	€ 343.16
1DWaA1n54bGeCs2AXTpV9x4a7GbvSKjQE8 - (Spesi)	€ 3.04
13YamD7pp8wxKhue4AcMIT1Q92R3sS7knp - (Spesi)	€ 347.17
1QELDPd1uuAqQY5hL1oVWWa8TtHuUEghPN - (Spesi)	€ 347.47
192BKs5fAGs74oGXRNVYZErc87RkpcMtvN - (Spesi)	€ 324.26
15nrUxmtYTgkxGaPzhXH2HfGDFFLnUuj6W - (Spesi)	€ 328.22
1N6Ubr1Ziqf9Rf7XXYhGvPdk9CZgSczR9p - (Spesi)	€ 365.34

4 Conferme

€ 2.74

**Grazie per l'attenzione!**

Paolo Dal Checco  
paolo@dalchecco.it  
@forensico

[www.dalchecco.it](http://www.dalchecco.it). [www.bitcoinforensics.it](http://www.bitcoinforensics.it)  
[www.ransomware.it](http://www.ransomware.it)

