



**UTN.BA**

UNIVERSIDAD TECNOLÓGICA NACIONAL  
FACULTAD REGIONAL BUENOS AIRES



**ciie**

Centro de Investigación  
e Innovación Educativa

# Direcciones y billeteras Bitcoin

## 4.2 Almacenamiento de claves

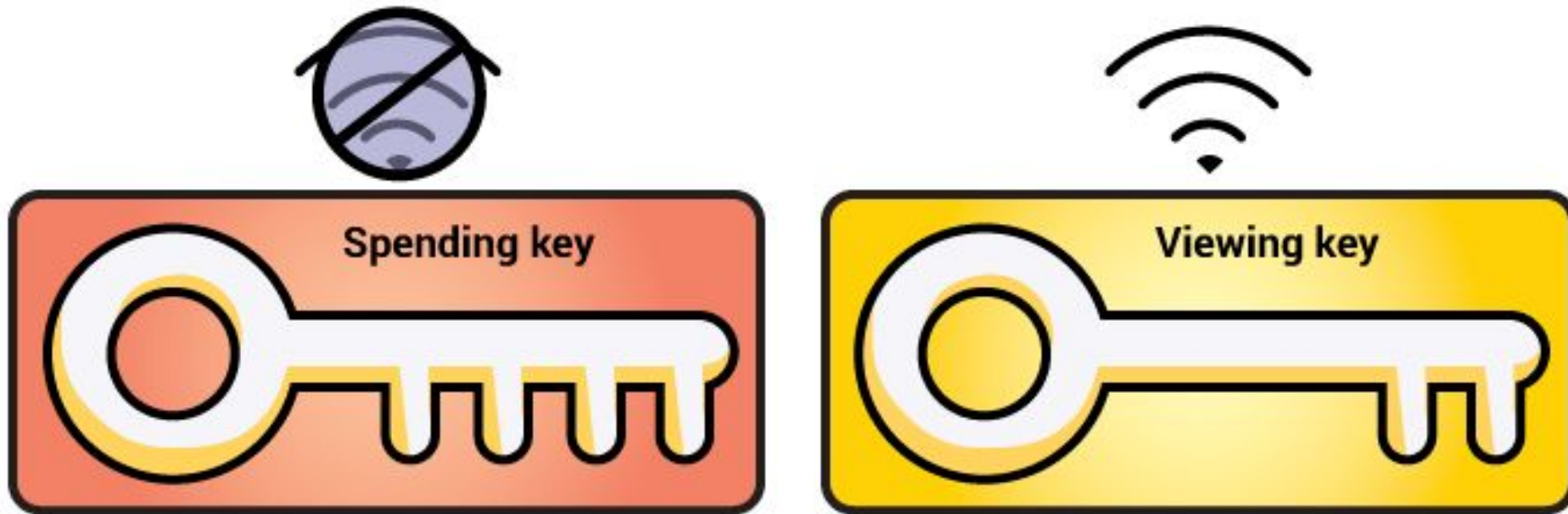
# Para realizar una transacción Bitcoin

- Se necesita cierta información de público conocimiento (la lista de transacciones sin gastar, conocida como Utxo), que se encuentra en la blockchain.
- La clave secreta para firmar el mensaje.

Como conclusión podemos sacar que el manejo de las claves secretas es lo fundamental para ser seguros usando Bitcoin.

# Almacenamiento Online vs Offline

Key Security: Compartmentalizing



# Hay 3 cualidades que son fundamentales

- La disponibilidad: No todas las formas de almacenar las claves privadas ofrecen la misma disponibilidad de gastar Bitcoin inmediatamente.
- La Seguridad: Esta es tal vez la cualidad más importante a tener en cuenta. Cada forma de almacenar nuestras claves tiene un distinto nivel de seguridad. Depende del uso que vamos a darle a nuestros BTC vamos a elegir una forma de almacenar las claves.
- La cantidad: Para elegir una forma de almacenar BTC es fundamental saber de cuanto BTC estamos hablando. Cada persona siente el riesgo y el dinero de forma distinta por eso esta cualidad es subjetiva.

# Almacenar BTC, en un archivo en una computadora o celular

- Es muy conveniente debido a que los BTCs están disponibles en tu celular o PC.

Dispositivo se pierde/borra → las claves se pierden → Los BTC también

- Los BTCs están igual de seguros que lo que hagas en tu celular.

Dispositivo comprometido → las claves se filtran → Los BTC son robados.

- Solamente llevar una cantidad con la que nos sentimos cómodos. Una buena comparación es llevar la misma cantidad de BTC que llevarías efectivo.

A lo sumo perdemos/roban una poca cantidad.

# Almacenamiento en Computadora o celular



# Almacenar BTC en una billetera hardware

¿Qué es una billetera hardware? Una hardware wallet es un tipo especial de billetera de Bitcoin que almacena las claves privadas del usuario en un dispositivo de hardware seguro offline.





# Almacenar BTC en una billetera hardware

- Es flexible dado que se pueden hacer transacciones con/sin los dispositivos físicos.
- Las claves se generan solamente dentro del dispositivo y nunca se transmiten a internet.
- Si disponemos de un buen lugar para almacenar la wallet (como una caja de seguridad) entonces se puede utilizar para una cantidad considerable de BTC y su conexión con el celular para bajas cantidades.



# Almacenamiento en una billetera hardware




# Almacenar BTC en una billetera papel

¿Qué es una billetera de papel? Es un método obsoleto para almacenar Bitcoin que fue popular entre 2011 y 2016. Funciona al tener una única clave privada y una dirección de Bitcoin, generalmente generada por un sitio web, que se imprime en papel.



*Open Source JavaScript Client-Side Bitcoin Wallet Generator*

A screenshot of the bitaddress.org web application interface. It has a green header with navigation tabs: "Single Wallet" (selected), "Paper Wallet", "Bulk Wallet", "Brain Wallet", "Vanity Wallet", "Split Wallet", and "Wallet Details". Below the header is a "Generate New Address" button and a "Print" button. The main content area is divided into two columns. The left column is titled "Bitcoin Address" and contains a QR code, the word "SHARE" in green, and the address "19DAVRViZHF6uBHWp2Davnj9WYwXL0wMhw". The right column is titled "Private Key" and contains a QR code, the word "SECRET" in red, and the private key "Kz7PteDXwDabRdpdH9tZNFF8LmZFx2BksTCAZsLC8A3Mk2pwg1CV".

Nota: No usar estas claves públicas y privadas , no mandar BTC.

# Almacenar BTC en una billetera papel

- No es muy conveniente porque hay que estar en posesión del papel para transmitir la transacción.

Si papel se pierde/gasta → las claves se pierden → Los BTC también

- Los BTCs están seguros si la wallet fue generada correctamente y si almacenamos el papel con seguridad.

Si acceden a la wallet → las claves se filtran → Los BTC son robados.

- Si disponemos de un buen lugar para almacenar la wallet (como una caja de seguridad) entonces se puede utilizar para una cantidad considerable de BTC.

Un atacante tiene que poder acceder y vulnerar la seguridad.

# Almacenamiento en una billetera papel



# ¿Cómo generar una billetera en papel de forma segura?

1. Ir a la web [www.bitaddress.org](http://www.bitaddress.org)
2. Desconectar la conexión de internet.
3. Generar la billetera en papel.
4. Tener la impresora conectada a través de cable únicamente.
5. Imprimir la billetera en papel.
6. Reiniciar la PC.