The Bitcoin Wallet

Never lose control of your Bitcoin

Bal Krishna Poudel

Bitcoin wallets Never lose control of your Bitcoin by Balkrishna poudel

Table of content

Chapter One

What is bitcoin wallet? How does bitcoin wallet works?

See the more Step – How the bitcoin wallet works!

How does the Bitcoin network work? Chapter Two

Types of wallets

Hot wallet Cold wallet Main

different types of Bitcoin Wallets

Software Bitcoin Wallets
Desktop Wallets
Hardware Wallets
Mobile Wallets
Online Wallets

Chapter Three
Create wallets How to create Bitcoin wallet on BLOCKCHAIN? How to create Bitcoin wallet on Coinbase? How to create

Paper bitcoin wallet?

Some of the best bitcoin wallets

1. *BitcoinQt Wallet*
2. *Coinbase Bitcoin Wallet*
3. *Blockchain Bitcoin Wallet*
4. *Trezor Bitcoin Wallet*
5. *Exodus Blockchain wallet*
6. *Mycelium Bitcoin wallet*
7. *Bitcoin Core wallet*

8. *Multibit Bitcoin wallet*
9. *Electrum Bitcoin wallet*
10. *Armory Bitcoin wallet*
11. *Xapo Bitcoin wallet*
12. *Coinkite Bitcoin wallet*
13. *Green Address Bitcoin wallet*
14. *Ledger Bitcoin wallet*

15.

Copay Bitcoin wallet.

Chapter Four

Bitcoin Security Which types of Bitcoin wallet should ideal for use? How to protect our bitcoin against theft? Conclusion

DISCLAIMER

What all about this book

Bitcoin is one of the most popular and widely used cryptocurrencies, and it too requires a wallet to hold it. Unlike physical wallets, Bitcoin wallets come in many types.

In compare to other systems protected by username and password logins, Bitcoin is secured through digital message signatures created with a unique private key and public key. Before losing funds due to preventable mistakes, it’s necessary to understand how our software treats externally-created

private keys - before importing them. Regardless of the specific wallet application being use, private keys kept or maintained outside of a software wallet need to be handled with care to prevent loss and theft. Private keys can be imported into another application.

Most wallets, however, allow the user to be in charge of their own private keys. This means that no one in the entire world can access your account without your permission. It also means that no one can help you if you forget your password or otherwise lose access to your private keys. If you decide you want to own a lot of Bitcoin it would be a good idea to divide them among

several different wallets. As they saying goes, don't put all your eggs in one basket.

The number of different wallets grows dramatically. But in the meantime it's wise to have a central management wallet that doesn't heavily rely on exchange security. I bet you'll even

Have at least three of them before make a conscious choice on one.

However, as with any new, confusing technology, there are an increasing number of fraud attempts and scam artists lurking through the internet, looking to steal a few Bitcoins. Thankfully, Bitcoin has more than a few

options to give each user the right mix of security and accessibility.

In this book, I’m trying to show some features of a bitcoin wallet. If you want to care about your funds. So, this book, definitely help you.

Chapter One

What is Bitcoin wallet?

A Bitcoin or cryptocurrencies wallet closely resembles with our bank account. Like bank account, it lets us send, receive and store bitcoins. Bitcoin

wallet is a tool that allows us to take control of our Bitcoin private keys, and can be used to send, receive and store Bitcoins.

Bitcoin wallets facilitate sending and receiving **Bitcoins** and gives ownership of the **Bitcoin** balance to us. There are many types of wallets available. It is advisable to know these different types of wallet so that we can choose one that suits for us. It's safer than a bank vault and easier than sending an email. For creating an account, bank and financial institutions asked our personal information, document but creating bitcoin wallet, No personal information required. Send and receive any amount

of bitcoin, anywhere, at any time, with total financial privacy is the main characteristic of bitcoin.

How does bitcoin wallet works?

Bitcoin wallets is a piece of software that use to communicate between bitcoin network and we can say- bitcoin networks are used to send and receive transaction.

The best way to understand about the bitcoin wallet is by compare to email address. Once we want to set up email address we need some kind of software that allow to send and receive email to that address. And that software may be app on our phone or may be our laptop and desktop computer that could be login

to. Now with email we use username and password, that how to be internet knows is this really who wants to send and received

Of course we tell everybody to your email address but anybody else knows our password means that would be bad because they, then could send email pretending to be us and causes all kinds of problems. In order to be allowed send the particular email address we have to know the password. And if someone finds out our email and passwords then nothing stopping them to login our email address and sending messages.

And this is very similar to help bitcoin wallet how work. Every bitcoin account

has two elements to its- one is called public Key address (it is kind of our email address) another one called our Private Key which is like our password. So just like email, we can give anyone our bitcoin public address. And anyone from anywhere in the world can send us a bitcoin. There needn't to know anything else about we. All they need to know about the public address and they can send money to us. The bitcoin private key on the other hand we must be protect. It's called our private key.
If someone gets our email passwords that pretty bad because they can send email from our email address. That's way it is quite bad as someone getting our bitcoin private key because they can

steal all our bitcoin by sending them somewhere else bitcoin address. In just like email, once a bitcoin transaction has been sent, it's a one way trip .The only way to get it back would be that person send it back to us voluntarily .So bitcoin literally works like digital cash. Once we handed it over, bitcoin belongs to the other person.

And same goes we received bitcoin if someone send to us it's ours and no one can take it away from us. The only way take it away from us that if they knew our private key. And of course, now we know, never to give these to anyone. So, actually, bitcoin wallets secure our private key.

Now a days there are many different types of bitcoin wallets, they have different characteristics but each works in basically the same way; they store our public (a long string of numbers and characters) and private keys (wallet also contains this key, it's called private key).

Our bitcoins, actually the pieces of code that represent them – are not actually stored in our given wallet. They are stored on the Blockchain, which in turn is stored on node computers all around the world.

See the step-How the bitcoin wallet works!

The First step: - When we create our Blockchain Wallet, a unique master seed is created. This is the nucleus of our specific wallet, and is used to derive every individual bitcoin address that we'll use to send and request bitcoin.

Second Step: - our wallet is encrypted on our device with our personal password. Our password acts as our decryption key to both lock and unlock our wallet — Remember, our wallet cannot be accessed without it.

Third Step: Our encrypted wallet is automatically backed up to by wallet provider clients like coinbase, blockchain.info. Electrum etc. To safely store your wallet, they add another layer

of security by encrypting our wallet a second time. Securely storing our wallet on their servers ensures that we can access our wallet from any (and all) of our different devices.

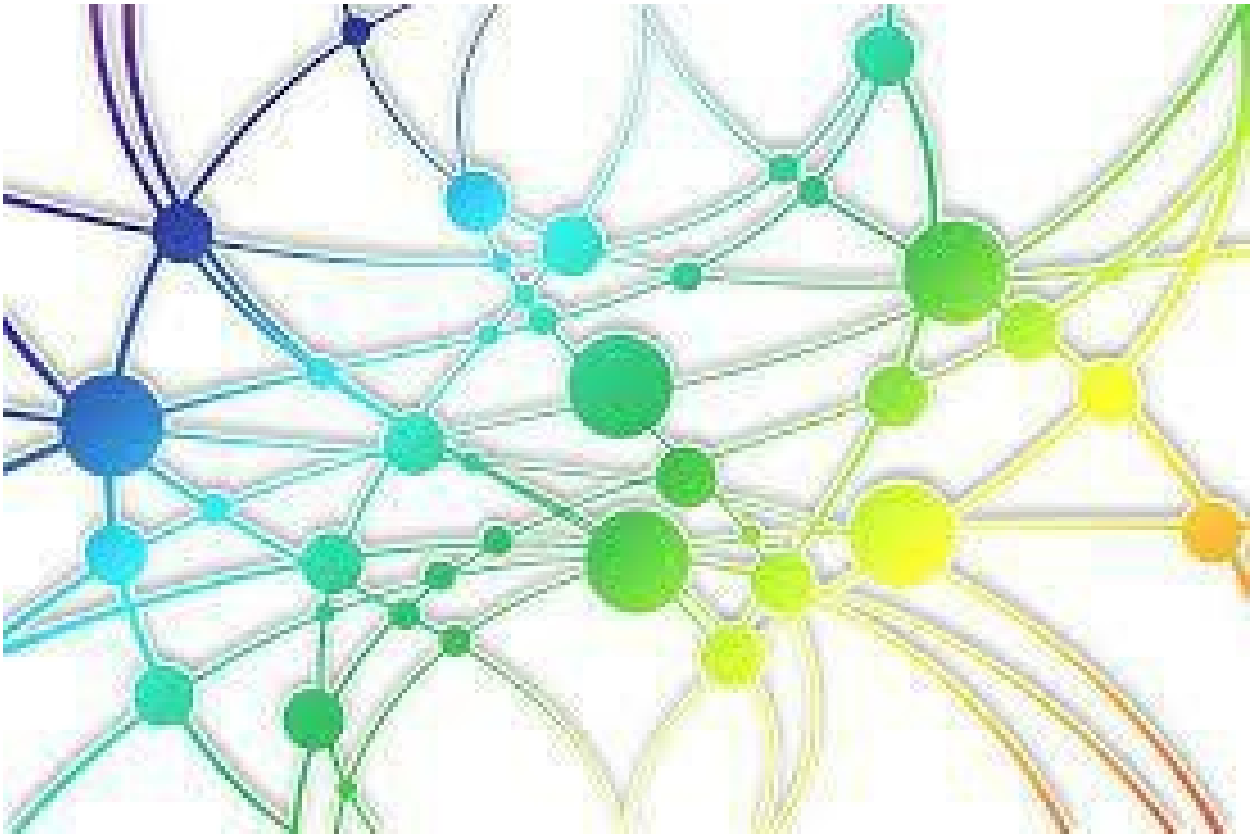
Fourth Step - We access our wallet with our Wallet ID (a unique identifier specific to our wallet) and password, our browser uses their API to download our encrypted wallet backup, before safely decrypting it on our device. And we're able to access in our wallet.

Here, we must know the important part to understand that the wallet doesn't actually contain our bitcoin. Wallet contains *permission to spend* our

bitcoin. And if we lose access to

That permission to spend, then we effectively also lose our bitcoins, because wallets no longer have access to them. That is why it is so important to keep the keys secure. The basic principle is the same for most: wallets hold our keys, not our bitcoins, although the distinction is actually not that relevant for the average user. Bitcoin wallets are a fundamental piece in the path to increase bitcoin use beyond geeks and techies.

How does the Bitcoin network work?



The Bitcoin network is based on a Blockchain, an administration of all transactions between the different bitcoin addresses. Every 10 minutes a new block will be created, containing

all transactions of these 10 minutes plus the previous block. Every transaction will exist forever (as long as the Blockchain exists).

Along with the information of the transaction, other information can be added in a block. It is not possible to change or delete this information. Adding information will create many interesting user possibilities, which do not exist in other payment methods.

Bitcoins can be mined by using special hardware to translate encrypted codes. These codes represent all transactions in a block, and the miner who finds the block first will be rewarded with an amount of bitcoins (currently 12.5). The

financial effort you have to put into mining, like costs for electricity and hardware, is called “proof of work”.

This makes the bitcoin Blockchain super secure, because to alter or delete something in the Blockchain you will have to input a greater proof of work than all of the current miners together. At that moment the total computing power (hash power) that is mining on the Bitcoin network is so incredibly huge, that for a single person, company, or even government, it is impossible to deliver more hash

power to override the current mining operation.

Besides finding new blocks, miners will also earn on transaction fees. The most amount of bitcoins that will ever be found is limited to 21 million, and they will be harder to find because every four years the mining reward will be reduced by fifty percent. The value of bitcoin will not be affected by dilution, because the supply is limited.

Chapter Two

Types of Bitcoin wallets

Similar to real money, we need to have wallet to store Bitcoins. The difference is that in Bitcoin wallet we store not actual Bitcoins, but private keys. Now a days, there are many different types of Bitcoin wallet we can use but all the wallets can be classified into two categories:

Hot Wallet and
Cold Storage Wallet.

Hot wallet

Hot storage wallets can be accessible from anywhere from a web portal. It also called an online storage wallet. Hot Wallets that require the download of software clients to create and use a wallet. Software clients are available for both — desktop platforms and mobile platforms. Desktop software clients like Bitcoin Core usually require downloading the Blockchain, which is more than 100 GB is size.

Cold Storage Wallet

Any type of wallet which is stored offline is termed as Cold Storage Wallet. These kind of wallets are more secure, as they are stored physically and hackers do not have any access to them. It can only be accessed with physical contact to the wallet although they tend to be back ordered pretty heavily. They essentially work like a USB stored wallet or as a way to securely keep track of several paper wallets.

We are going to discuss four main different types of Bitcoin wallets we can use

now a days:

A software Bitcoin wallet – It is a wallet installed on your

actual computer that you actually control yourself. Ideally, only you have access to the private keys that store your Bitcoin.

Getting a Bitcoin software wallet is as simple as picking which wallet you would like to use and downloading it. Bitcoin Armory is the most popular, stable and secure software wallet. It is also opensource.

There is also BitcoinQT/Bitcoin Core, which is the original software Bitcoin wallet, and Multibit, which has the advantage of not requiring that the entire Blockchain be downloaded.

That Blockchain download is the main barrier to using a software wallet. It is required downloading for any locally stored software Bitcoin wallet. The file size currently sits at 18GB and is growing.

Software wallets provide more security than web wallets. However, they are only as secure as the computer they are stored on. Malware is beginning to attack Bitcoin holding computers specifically. If a computer is

compromised, any private keys may be as well.

Once you download the wallet software, it will synchronize with the network by downloading the Blockchain. That will take a few hours but once that is done, sending and receiving Bitcoin is as simple as clicking the appropriate buttons and following the on-screen prompts. Of course you will need to know your public key (for receiving) and the recipient's public key (for sending).

Desktop wallets are installed on your computer. These

are full

featured Bitcoin clients, with the highest security level and the widest variety of features. Once you install this wallet on your computer you need to update it by downloading all Blockchain which were created from the very beginning. This can cause some difficulties in using desktop client, as it takes time to download gigabytes of Blockchain. Of course, it is recommended to have powerful hardware if you wish to run desktop client.

Currently desktop wallets are the most secure way of storing private keys. Some of them even allow users to have a

paper wallet in which private keys can be stored. This feature is dedicated to store private keys on the paper or any other offline storage to prevent private keys from being hacked by a person or virus.

Hardware Wallets

Hardware Wallets are stand-alone hardware cold-storage devices that generate keys on the fly while making a transaction. They are USB shaped devices, which have to be plugged into your computer while making a transaction.

Hardware wallets are **secured from**

your regular computer malware because it generates private keys offline, on the device itself. They are extremely convenient to use and do not require the understanding of complex technical details. They also provide sturdy backup options, so you do not lose access to your wallet. They can be also **secured with a password** to combat theft. Overall, as you carry your private keys along with you all the time and it is prone to computer malware, hardware wallets are the **most secure** option.

If you regularly deal in Bitcoins, you should definitely invest in Hardware Wallets like TREZOR or Ledger wallet. It is worth every buck spent and brings

you a great deal of peace of mind. Hardware wallets that can only be accessed with physical contact to the wallet have hit the scene from last year, although they tend to be back ordered pretty heavily. They essentially work like a USB stored wallet or as a way to securely keep track of several paper wallets. Bitcoin is a “trustless” system, meaning you don't have to give every merchant the information they need to steal your money every time you use it. This fundamental function makes Bitcoin inherently safer than fiat currencies.

Mobile wallet. It is almost the same as online wallet,

but it is

supported by mobile device. Due to the fact that you cannot run full Bitcoin client on mobile device, Simplified Payment Verification (SPV) is used here. So security of storing Bitcoins in mobile wallet comes in question.

Online wallets are dedicated to store your digital keys on the

Web. It means that Bitcoin wallet is stored not on your computer, but on some faraway server of service provider. There are different online

wallet providers. And depending on the provider, features of Bitcoin wallet can vary. Some online wallets are created with minimum features, while others can be used as a full-featured Bitcoin wallet. The main advantage of online wallet is that it enables you to enter your wallet in any place of the world. Online wallets are very easy to start using and have simple interface.

Disadvantage of this kind of wallet is security. When you trust your wallet with private keys to online service, there can be 2 cases you should be afraid of: the whole database of the service gets hacked and you as well as all the other users can say “lost” to your funds, or one

of the personnel or this service can get hold of your account.

Online Wallets or Web Wallets are the **easiest to use** amongst all the different kinds of Hot Wallets. Creating an Online Wallet is as easy as signing up for a new account on BlockChain or any other similar service. Also, you can access your wallet from **any device connected to the internet**, so making transactions couldn't get any easier.

But there are certain trade-offs of using an online wallet. Most importantly, your private keys are stored on **another server**, which could lure prying hackers all-around the globe to steal them. For

instance, back in 2014, hackers stole Bitcoins worth $460 million from Mt. Gox, a popular Bitcoin exchange site. Online wallets should be used only for making small everyday transactions. If you hold a large number of Bitcoins, you may want to stay away from online wallets.

Chapter Three

HOW TO CREATE A BITCOIN WALLET?

Bitcoin wallet are often much easier to use, but you have to learn basic steps to handle it, It's very easy and simple to create and use wallets. Once you used to one of the wallets, there are no difficulties to change and create multiple wallets on different wallets.

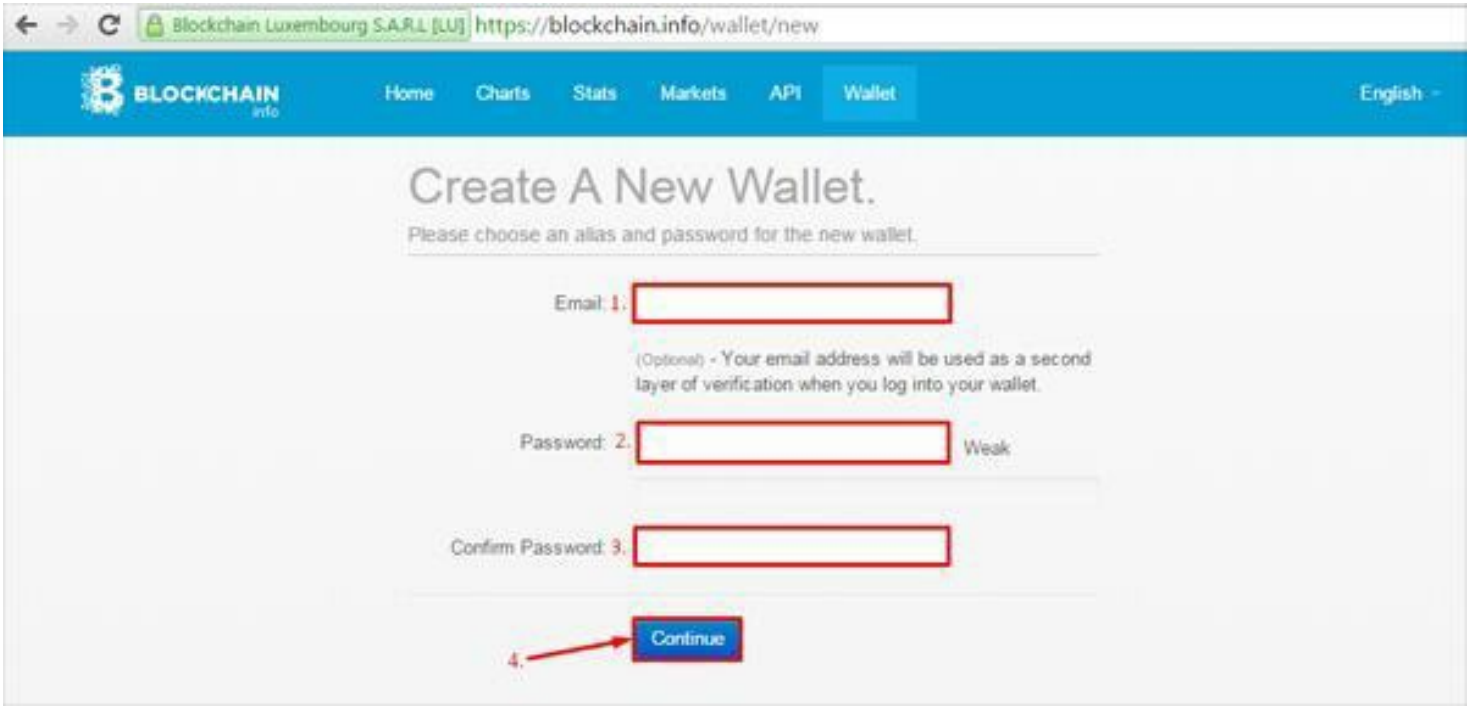
Here are some easy step to create wallets that we recommend for beginners

BlockChain.info:

Follow the link
https://blockchain.info/en/

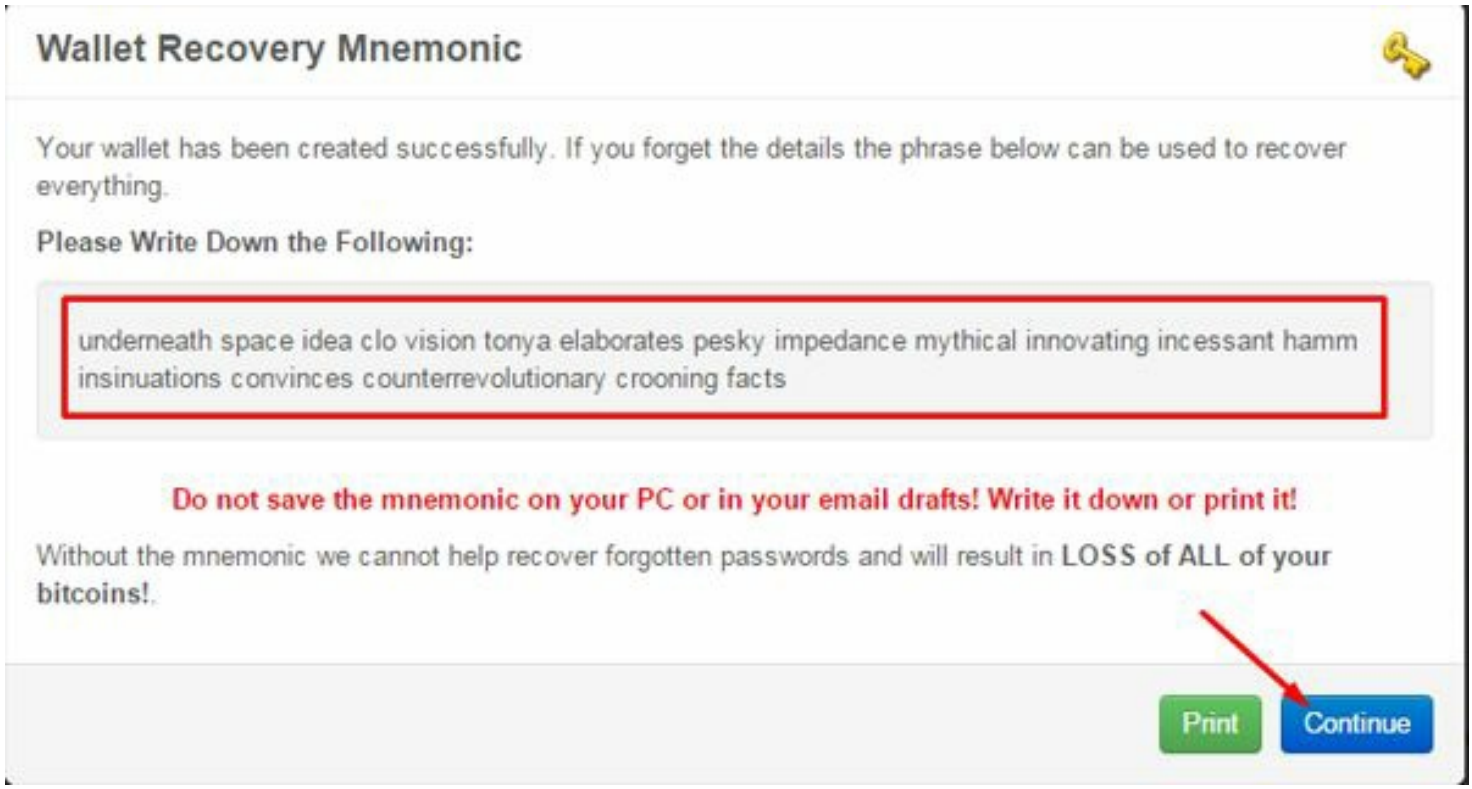
1. Click on “Wallet” button
2. Click on “Create a new wallet” button

1. Enter e-mail.
2. Enter password.
3. Confirm the password.
4. Click on “Continue” button.



Write down, make a screenshot or print the mnemonic password (in the red square on the screenshot). It will help you to recover your password if you forget it!

Click on “Continue” button.



1. Enter your password.
2. Click on “Open Wallet” button.

(Don’t forget to put down your identifier)

Here is your Bitcoin Address or Wallet

Ready.

Blockchain Luxembourg S.A.R.L [LU] https://blockchain.info/

BLOCKCHAIN info

Home Charts Stats Marke

My Wallet Be Your Own Bank.

Wallet Home | My Transactions | Send Money | Receive Money | Import

Total Transactions	0	
Total Received	$ 0.00	
Total Sent	$ 0.00	
Final Balance	$ 0.00	

This Is Your Bitcoin Address

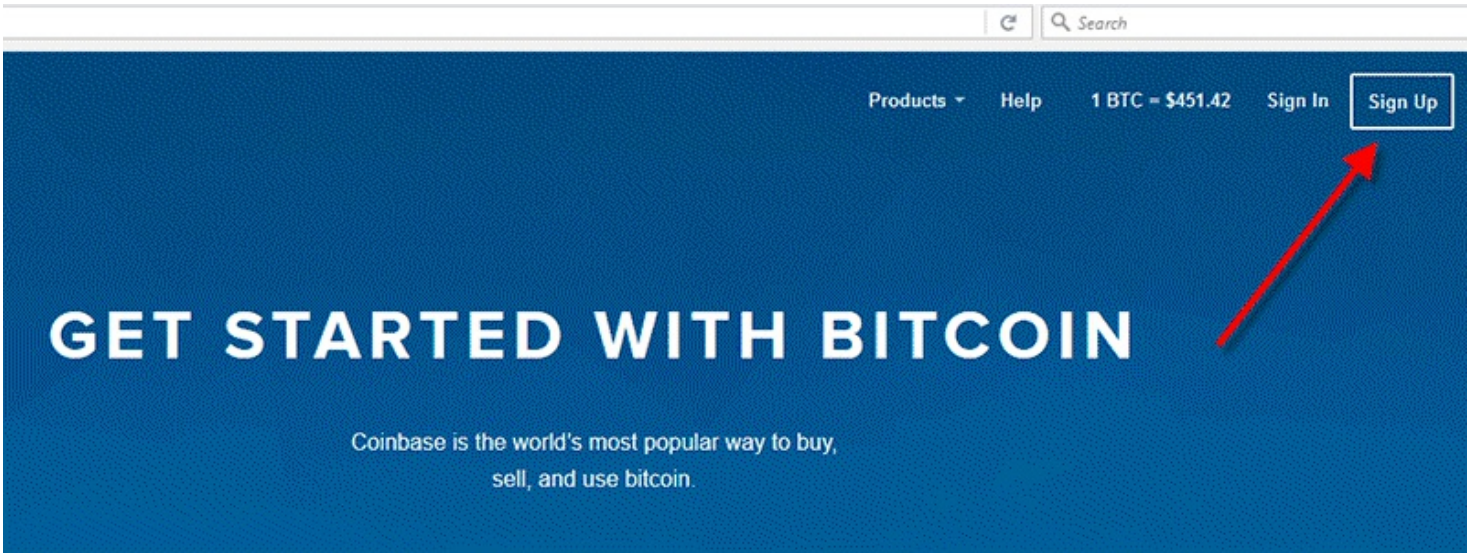
19wPos1Uo8yt7CaNvVCZQhuAtau8hd11rY

Share this with anyone and they can send you payments.

CREATE A BITCOIN WALLET ON COINBASE

STEP #1:

1. Go to https://www.coinbase.com/ and click on **Sign Up**



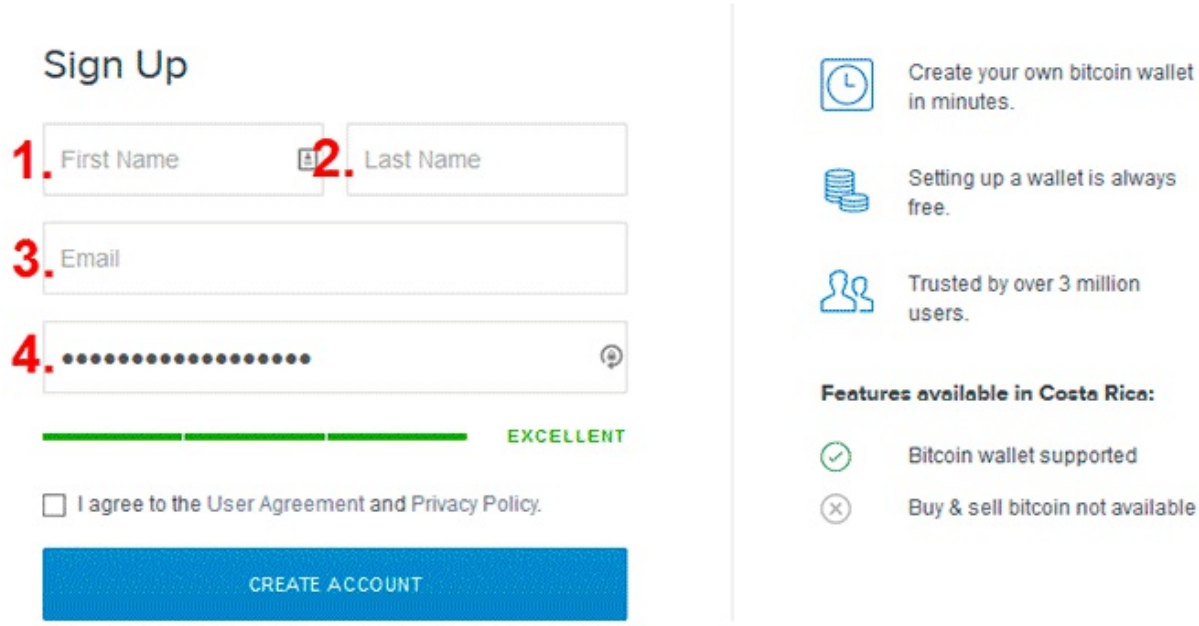
STEP #2

1. Fill in your “First Name”, “Last Name” and “Email”.

2. Create a secure Password, (minimum

10 characters long). Don't Forget Your Password, Write it down and keep it in a secure place.

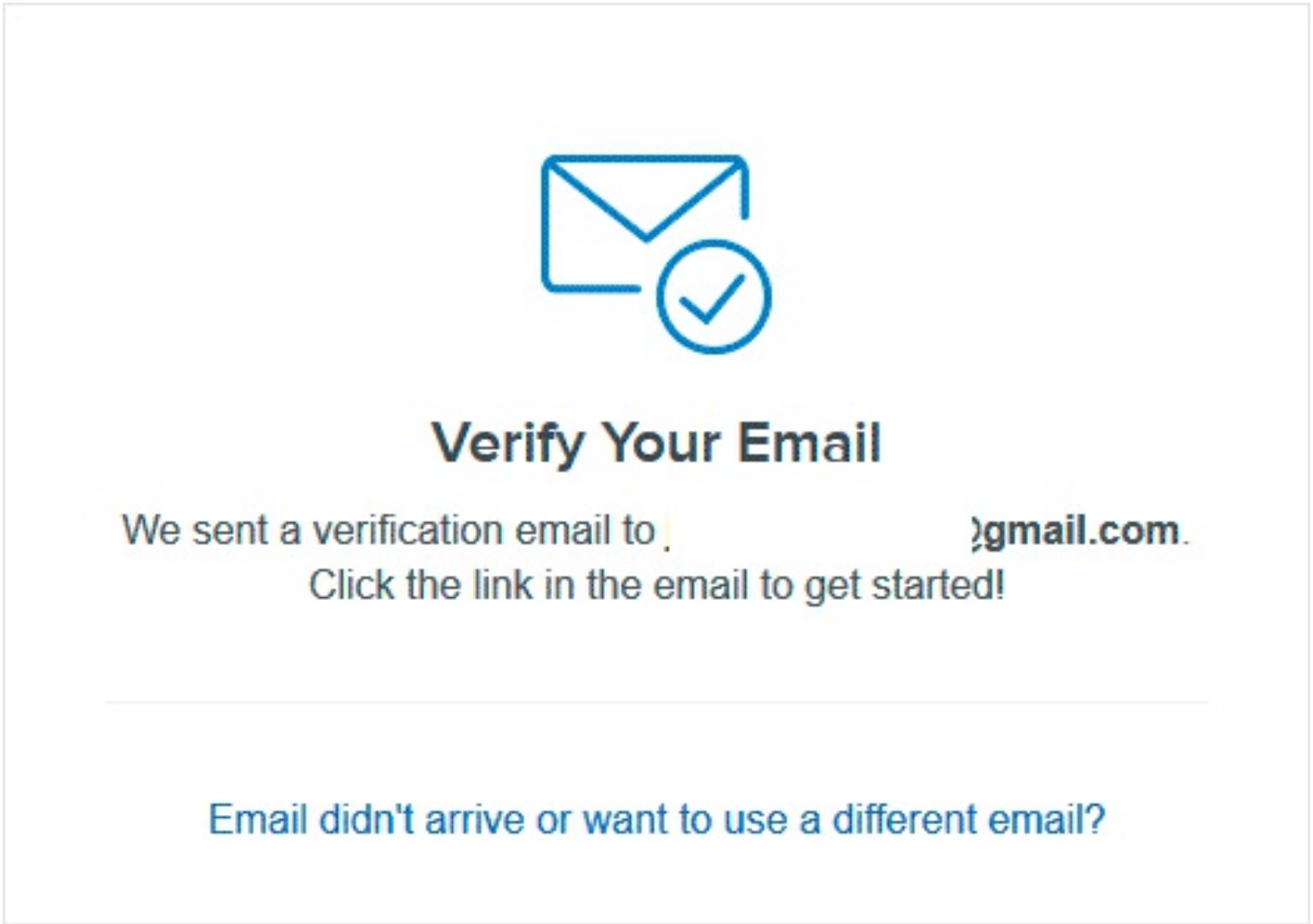
3. Click on "**CREATE ACCOUNT**"
WARNING: Forgotten passwords are UNRECOVERABLE and will result in **LOSS of ALL of your bitcoins!**



STEP #3
– Verify your email address.

1. A verification email will be sent to

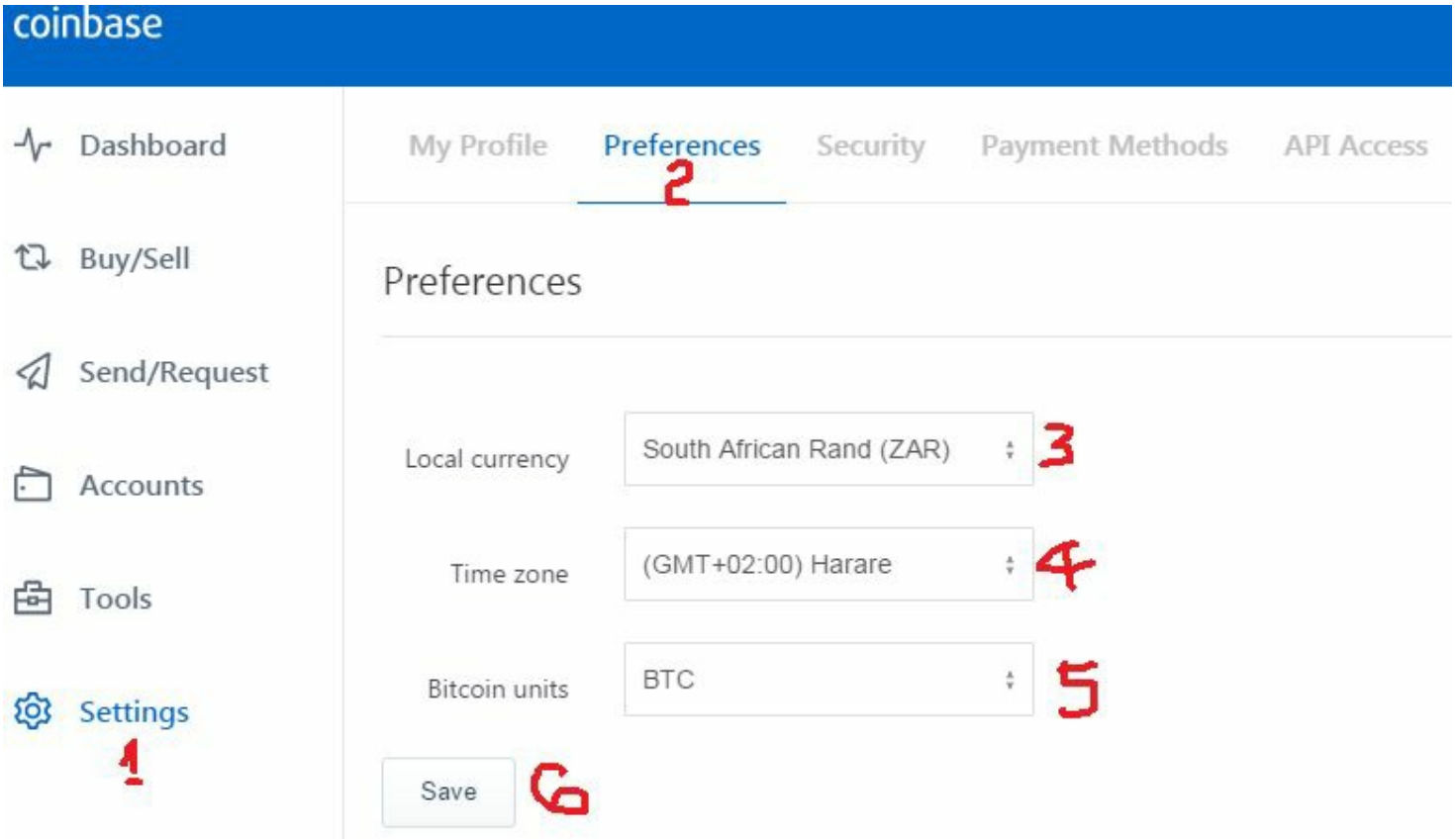
your email address you registered with, click the verification link.
2. Once you confirm your Email you are already logged into Coinbase.



STEP #4

1. You may need to verify/change the **Currency to USD** (or your country's

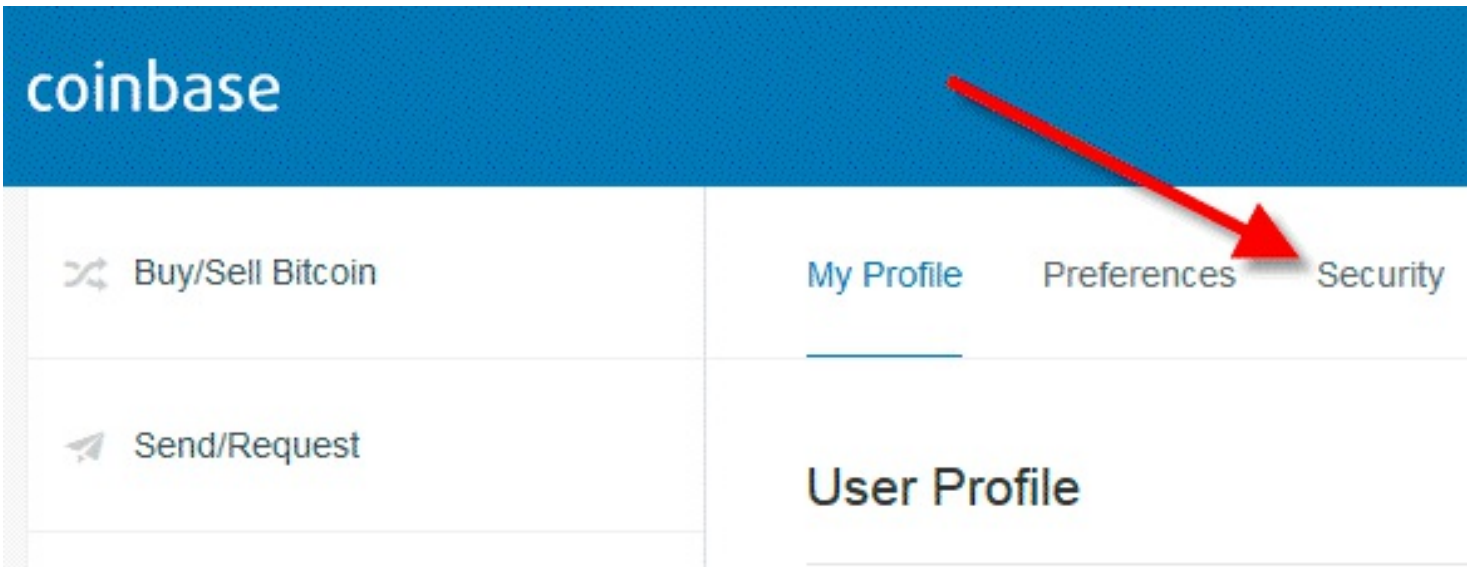
currency) and to **BTC**.
2. Click on **Settings** and then click on **Preferences**. Click the **Save** button.



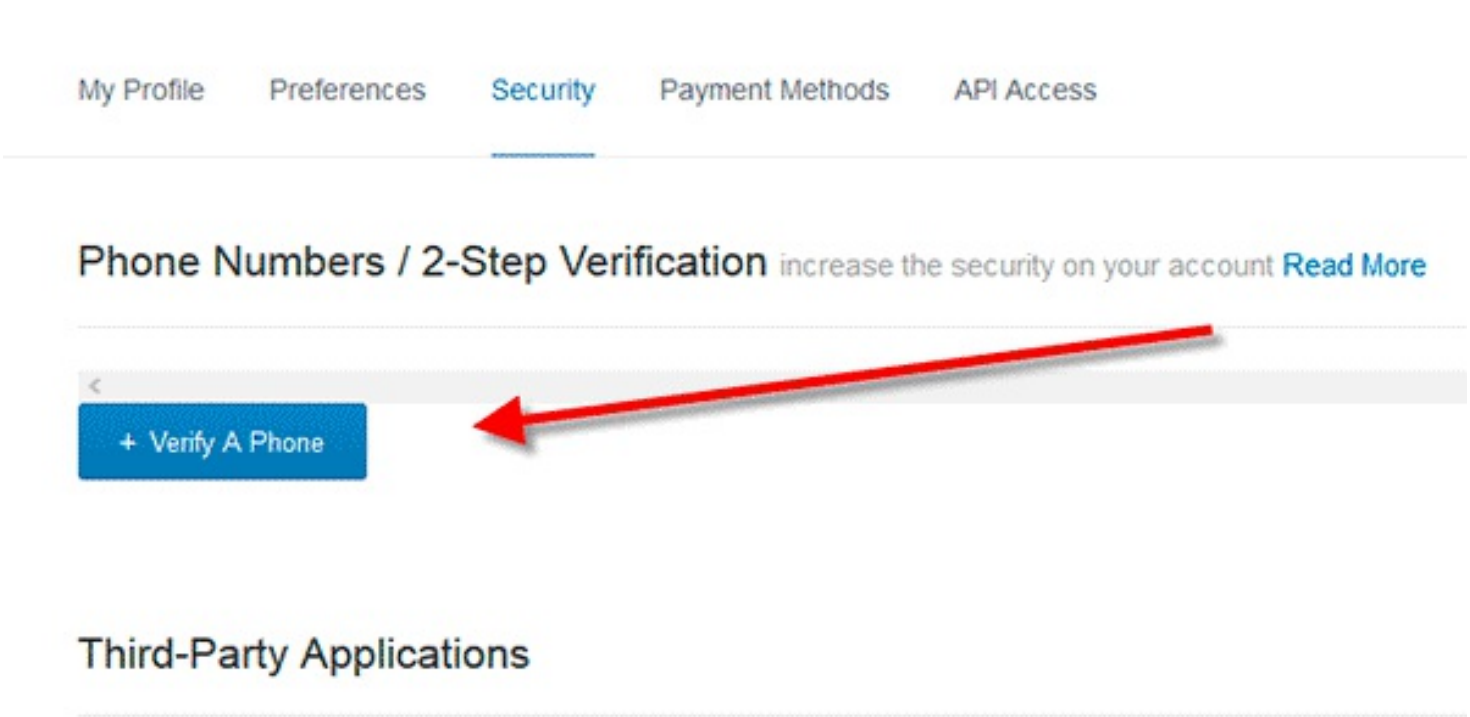
STEP #5

Securing your Coinbase Wallet.

1. Click on the **Security** tab.

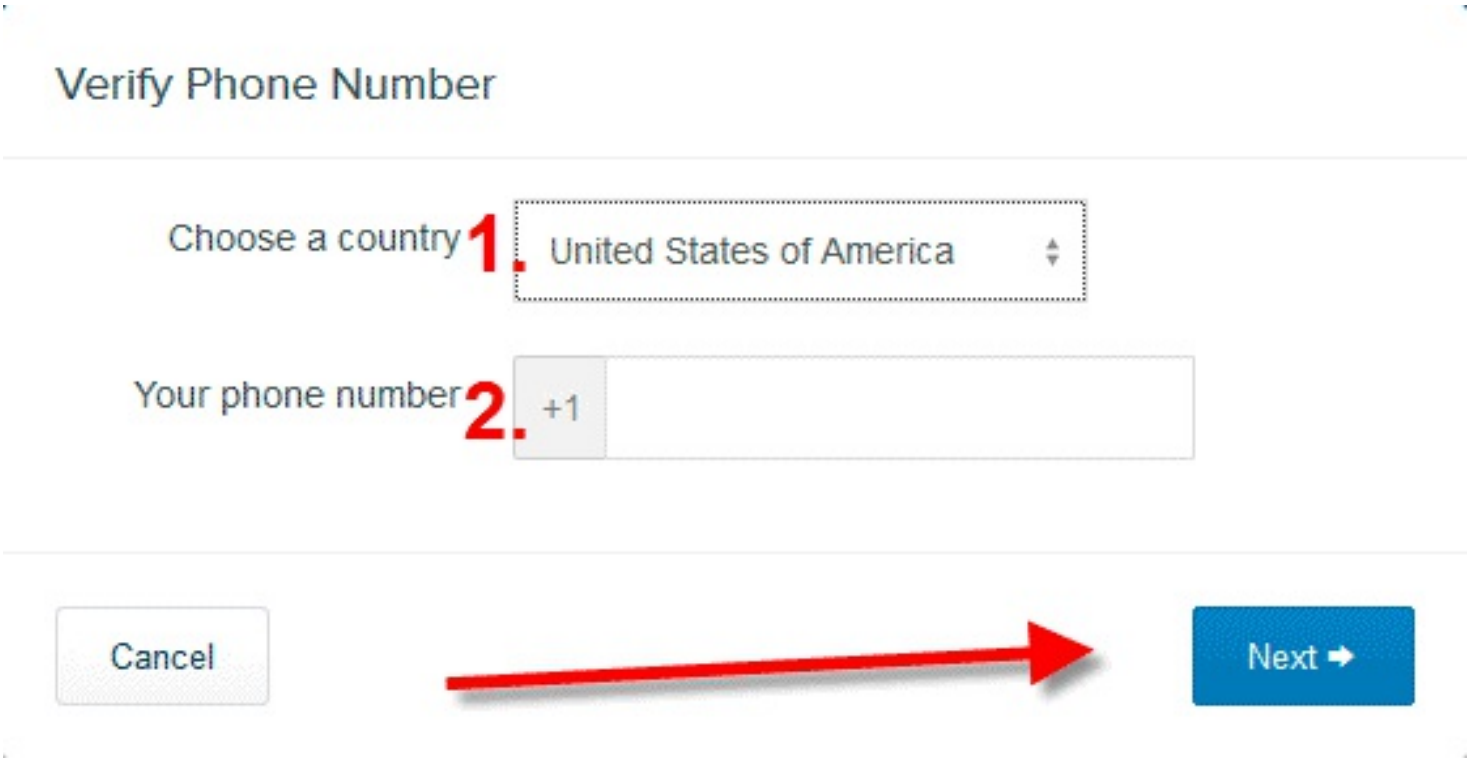


Click on "**Verify A Phone**"

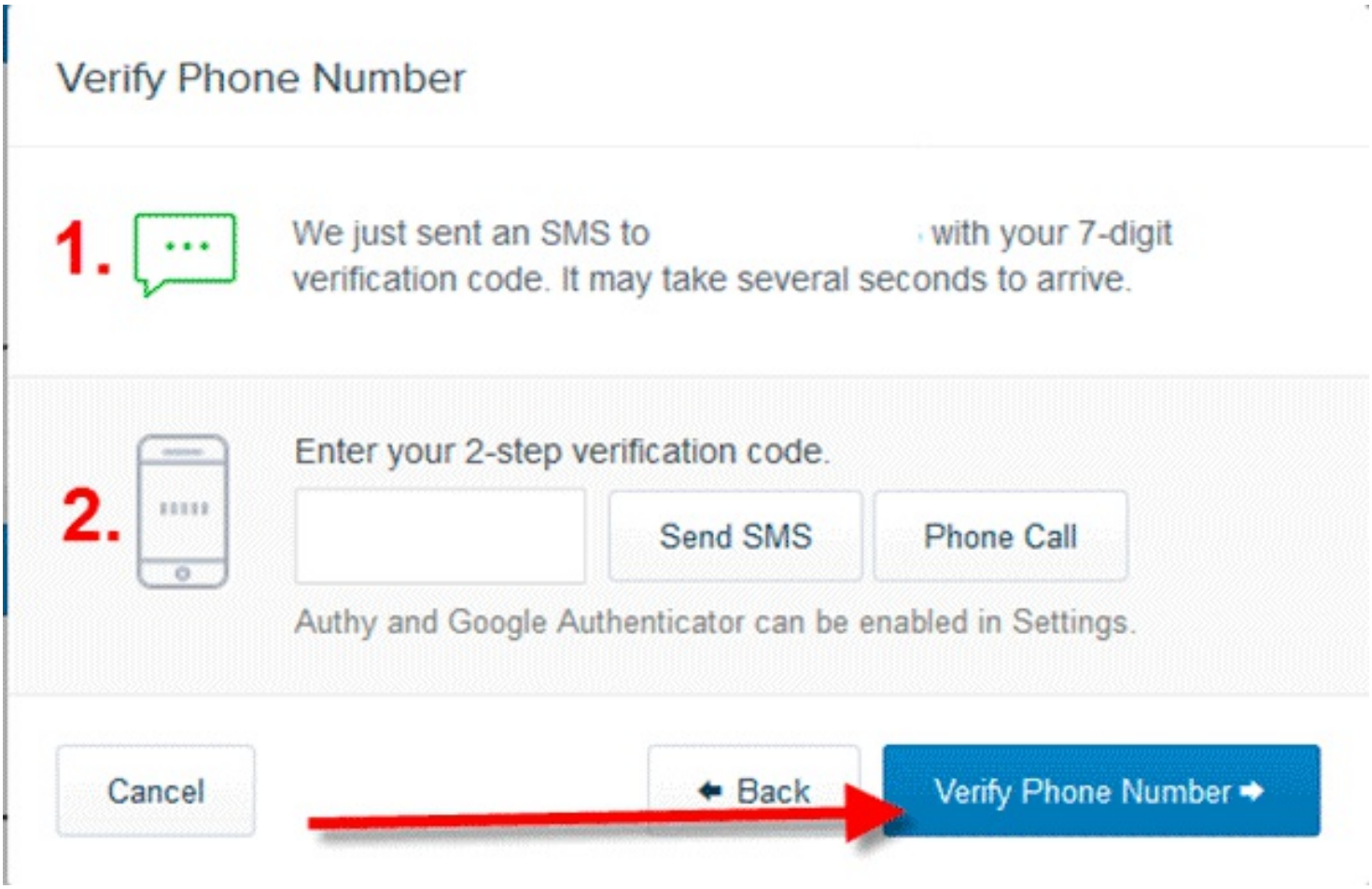


3. On "**Choose a country**" drop down menu and select the country where your phone number is associated with.

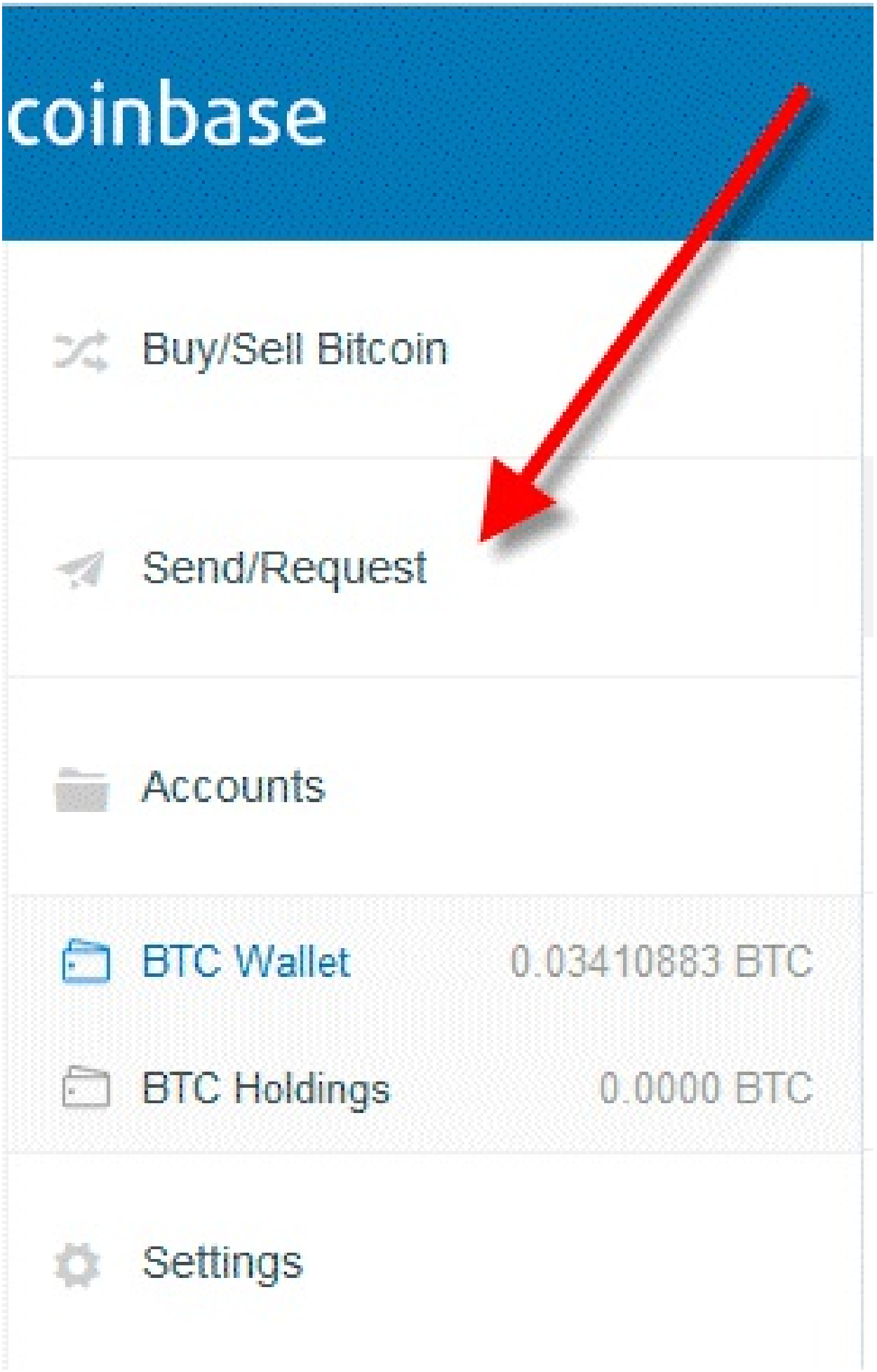
4. Put "**Your phone number**" in the space provided and click "**Next**".



5. Receive your code on the phone, enter the verification number and click on "**Verify Phone Number**"



Your wallet is ready. And you simply Send and received money from your wallet.


coinbase
Buy/Sell Bitcoin
Send/Request
Accounts
BTC Wallet
0.03410883 BTC
BTC Holdings
0.0000 BTC
Settings

How to Create Paper Wallet?

In simple terms, a paper wallet is just a physical and offline means of storing bitcoins. By making a paper wallet, you're just printing your private keys and bitcoin addresses on a paper. Seeing it this way, a paper wallet is a document containing copies of your public and private keys, thereby making up a physical wallet. These paper wallets also have QR codes so that you can scan the QR code to feed the keys into a virtual wallet to make transactions on the go.

The greatest benefit of using paper

wallets for cold storage is that you don't need to store your keys in digital format. So there are no potential threats such as hacking or malware attacks.

If you need a bitcoin wallet, learn how to make one at Bitcoin.org. Go to bitaddress.org, Click on 'Paper Wallet' and use these settings: Addresses to generate: 1

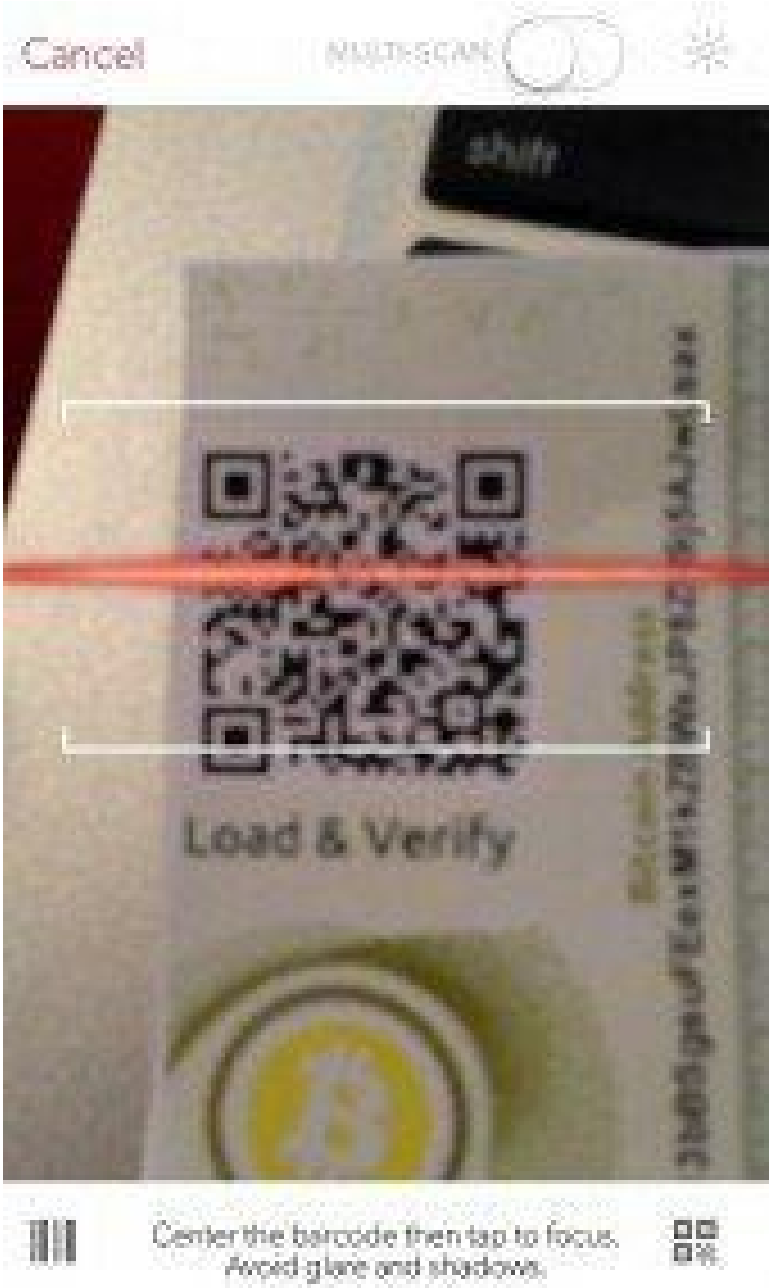
 BIP38 Encrypt? **Highly advised to check***, but not required. If you check this off, make sure to remember the password, as **it is nearly impossible to recover your bitcoins if you forget your password**.

☐ Passphrase: If you checked BIP38, enter a **strong, hard to guess** (mix lowercase and capital letters and numbers, and try to use at least eight but preferably more characters) password. If you didn't check off BIP38, skip this box.

2. Click on the ‘Print’ button in the top right. If you don’t see this button, just print the entire page. 3.* Cut out the white, non-used part of the wallet.

4.* Download a QR code scanner on your mobile device. I used RedLaser. 5.* Scan the QR code above the ‘Load & Verify’ text (if you have art turned off, scan the QR code on the left). This is your deposit address to store the bitcoins in the wallet. I highly suggest you copy this address and send it to yourself via email, to ensure you don’t make a mistake while typing it in. There is no worry about security in this step; your wallet address can be accessed by anyone and coins cannot be stolen from

you by just giving your wallet address. Send however many bitcoins you want to this address from a wallet you own that already has bitcoins stored. Your bitcoins are now stored in the paper wallet!



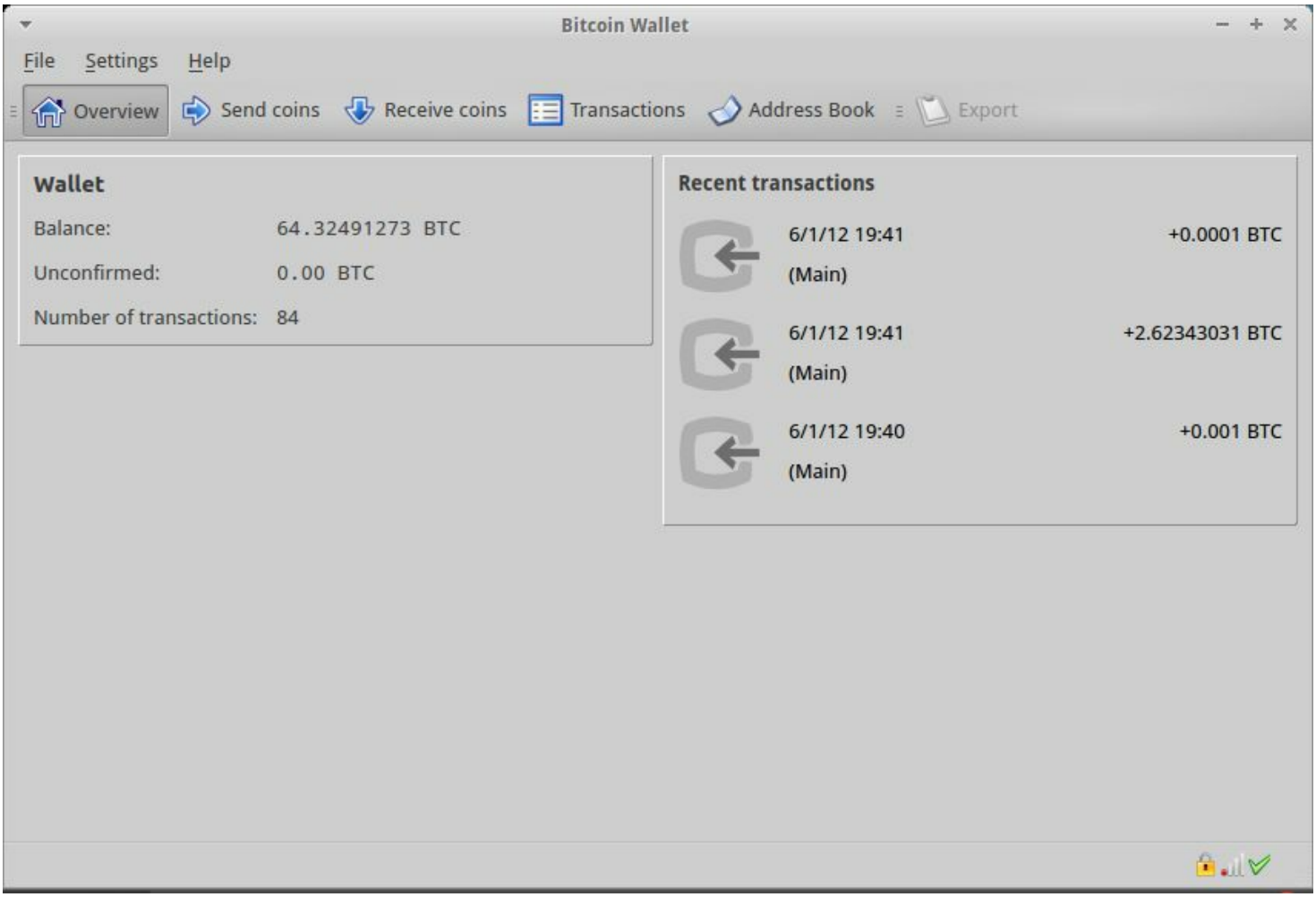
Scan the code on the right side of your bitcoin paper wallet, above the “Spend” text. Go back to bitaddress.org and go to the ‘Wallet Details’ tab. Enter the code

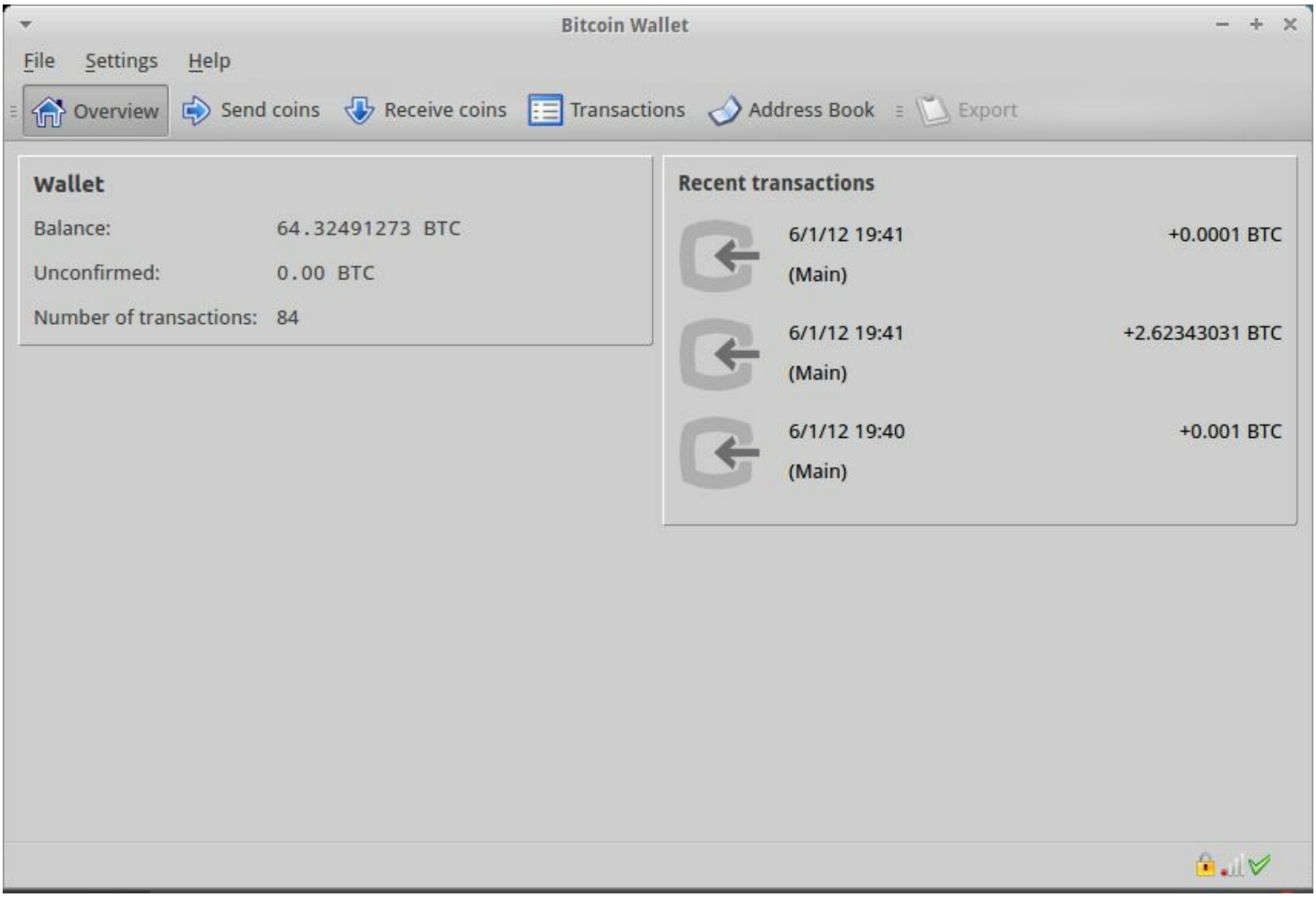
you received from scanning, making sure not to make any misteaks. Enter your password when you're requested to and voila, you have your private key!
9. Import the private key into whichever wallet you're using. Each wallet contains different methods for importing private keys. If you don't know how to import your private key, google "import bitcoin private key (your wallet program's name here)". Good luck!

Some of the Best Bitcoin Wallet

There are different types of Bitcoin wallets available, the first step in getting started with Bitcoin is choosing a secure Bitcoin wallet. So, choosing among them can be quite daunting. Amidst the growing number of Bitcoin wallets, how do you choose which wallet is best suitable for your needs? In this section, I attempt to trim down to the features you need to look for when selecting a Bitcoin wallet.

BitcoinQt Wallet


Bitcoin Wallet
File
Settings
Help
Overview
Send coins
Receive coins
Transactions
Address Book
Export
Wallet
Balance: 64.32491273 BTC
Unconfirmed: 0.00 BTC
Number of transactions: 84
Recent transactions
6/1/12 19:41
(Main)
+0.0001 BTC
6/1/12 19:41
(Main)
+2.62343031 BTC
6/1/12 19:40
(Main)
+0.001 BTC



2009, and continuously worked on by the core Bitcoin development team since then, this is the first Bitcoin client ever created. The client is a fully fledged node of the Bitcoin network, meaning that it can connect to other nodes and help verify and relay transactions, although it cannot mine.

Because it is a full node, the client must download the entire (currently 6 gigabyte) Blockchain to operate, which take up to a few days the first time you can start the client and several minutes to an hour every time you start the client afterward if you do not keep it running constantly. Your private keys, the mathematical data that makes it possible for you to spend the bitcoins that have been sent to one of your Bitcoin addresses, are stored in a “wallet.dat” file on your computer (which users are encouraged to back up), and the client offers the option of keeping your wallet.dat encrypted.

This client is arguably the most

trustworthy, since its development is certainly the most heavily scrutinized and is overseen by very well-known and established members of the Bitcoin community. So the probability of it having security holes is pretty low and one reason for it being so popular in the bitcoin wallet.

Its features include the basic sending and receiving functionality, as well as a feature that allows you to digitally sign a message with one of your addresses, allowing anyone who knows that the address belongs to you to verify that the message was not modified or forged (the verification functionality is also present in the client).

Coinbase Bitcoin wallet

Coinbase is the leading exchange service today in buying and selling Bitcoins. It was founded in 2012 and since then has received over US$37 million in venture capital funding.

Coinbase is one of the most popular Bitcoin exchange services used globally. They also provide a mobile and a web wallet. Coinbase gives you a little more flexibility than Bitcoin.info, as it allows users to **manage their own private keys**. It also **supports multisig** wallets wherein, up to 5 users can own a shared wallet.

Pros: Beginner friendly, ability to add funds from within the wallet. Established and respectable company.
Cons: Company has some control over your funds (depends if you're using Vault). Not supported worldwide (yet).
Click here to visit Coinbase's website

Blockchain.info Bitcoin wallet

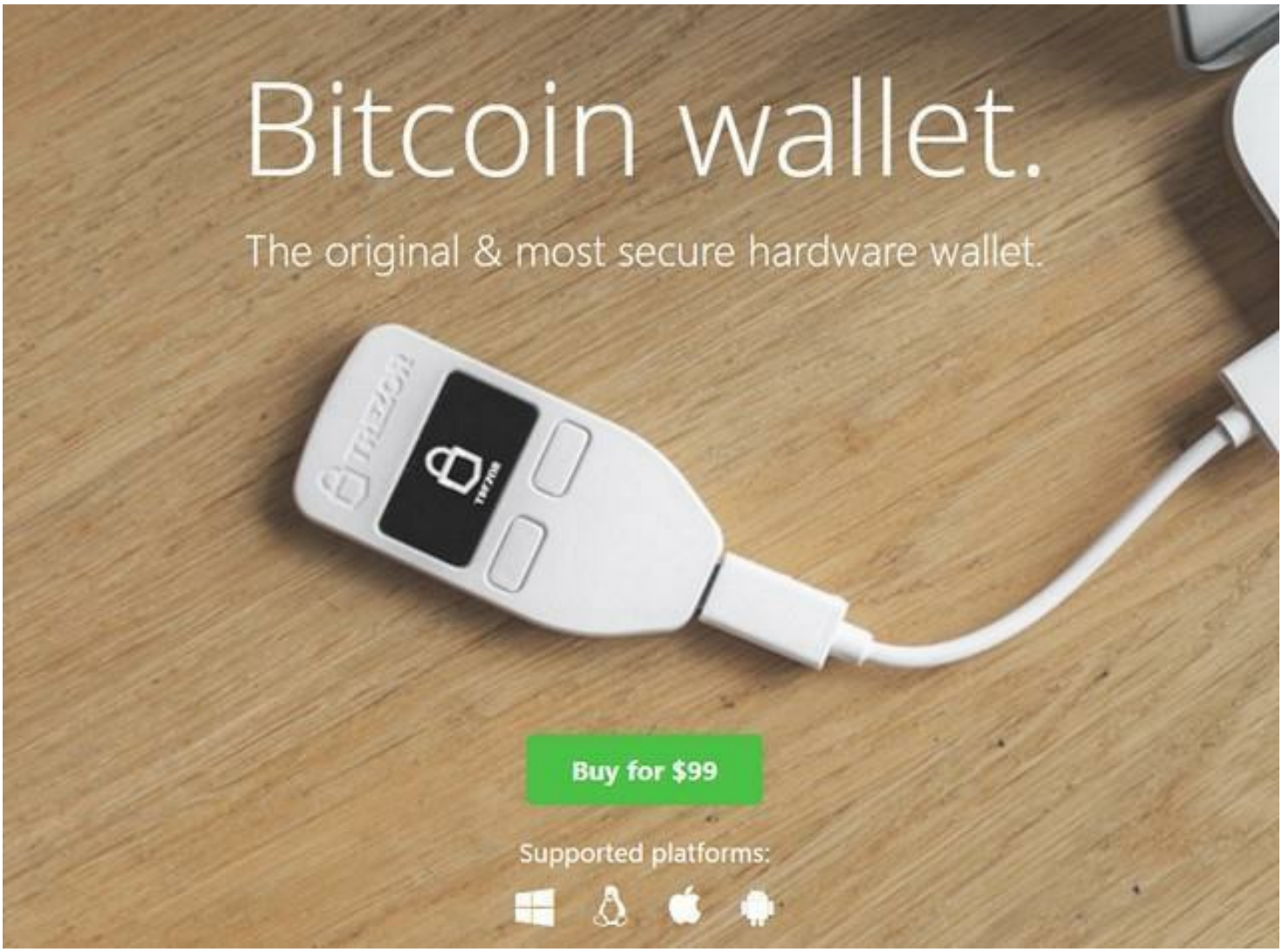
The most popular Bitcoin wallet today, Blockchain.info allows you to send / receive Bitcoins through your browser or mobile phone. Blockchain.info is famous for their Blockchain explorer

service, but it also offers a wallet service. If **convenience** is the only factor you are looking for in wallets, this online wallet would be a great fit for you. You can connect to the **TOR network** for added anonymity. This is what's known as a hybrid wallet – meaning the company stores your wallet online but they do not have access to your private keys. However since the wallet is loaded from their servers some trust in the company is still needed. Recommended for beginners who are trying out Bitcoin.

Pros: An established and trusted company in the Bitcoin community, good interface, available for mobile and web.

Cons: 3rd party trust required, hard to make completely anonymous payments.
Click here to visit Blockchain.info's website

TREZOR Bitcoin wallet

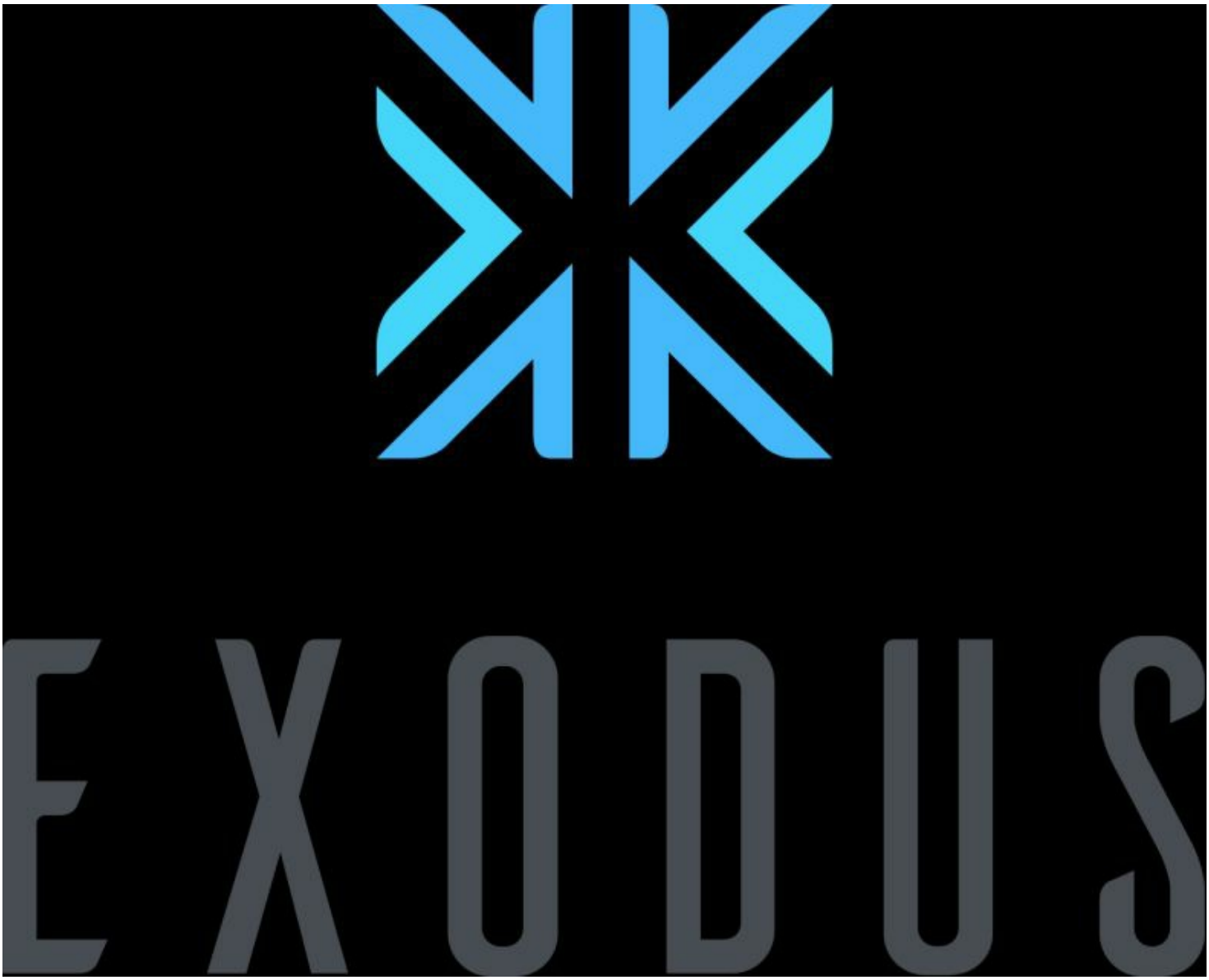


TREZOR is the perfect solution for storing a large amount of Bitcoins in order to keep them out of harm's way. The combination of world class security with the flexibility of any other web wallet make it ideal for beginners and experts alike. The company has been

gaining a nice amount of traction and reviews throughout the last year

Pros: Extremely secure wallet, easy to use and intuitive interface, supports additional wallets.
Cons: Hasn’t established a big enough user base yet, TREZOR device needs to be on you in order to send coins.
Click here to visit terzor website

Exodus Blockchain wallet



Exodus is a relatively new wallet (launched July 2016) that allows you to store not only Bitcoins but also Litecoins, Dogecoins, Dash and Ether. It’s unique in its beautiful design and intuitive user interface. You can also

trade cryptocurrencies from within the wallet. Currently the wallet is available only in a desktop version.

Pros: Easy to use, allows to trade crypt's from within the interface, self-hosted, awesome support from the founders.
Cons: Limited only to desktop at the moment, relatively new Company.

Click here to visit the Exodus website

Mycelium Bitcoin wallet

Dubbing itself as the “Default Bitcoin wallet”, Mycelium is a semiopen-source Bitcoin wallet. Its code is open to everyone for review, but you cannot

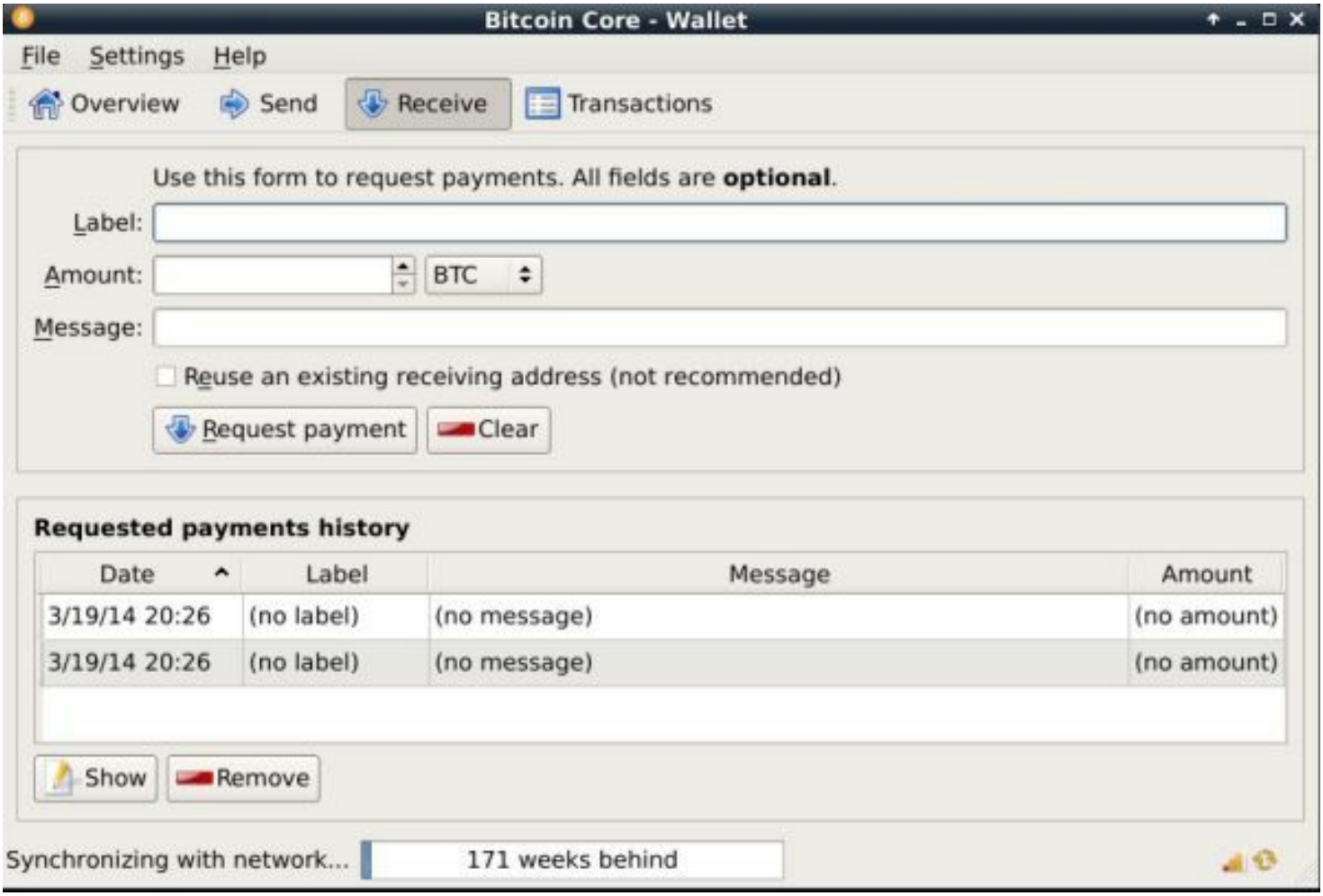
modify or redistribute it. It does not support multisig accounts, but the developers say it's on the roadmap. The data sent over the network is encrypted to offer the strongest level of security. For enhanced privacy, it also allows you to connect to the TOR network. It also allows you to back up your account and even PIN protect the wallet on your mobile.

Pros: Advanced privacy features make this app great for people looking to stay anonymous, and advanced security features will help keep your Bitcoin wealth secure.

Cons: No web or desktop interface, so

you'll have to use your smart phone to access this app. Mycelium is also better for more advanced users, so keep that in mind.

Bitcoin Core wallet



Looking for a desktop solution for your Bitcoin wallet? If so, Bitcoin Core is worth a consideration. Bitcoin Core offers a lot of security and privacy features, and supports complete

transparency. Bitcoin Core is well-regarded for being a stable system, though it can use up a lot of memory and space on your computer. Still, for modern computers the hardware requirements are rather low.

Pros: Features plenty of security and privacy features and offers a highly stable system.

Cons: No mobile app and no web interface makes it difficult to use this wallet without having your own personal computer on hand. It also requires a lot of free space to store the whole Blockchain.

Multibit Bitcoin wallet

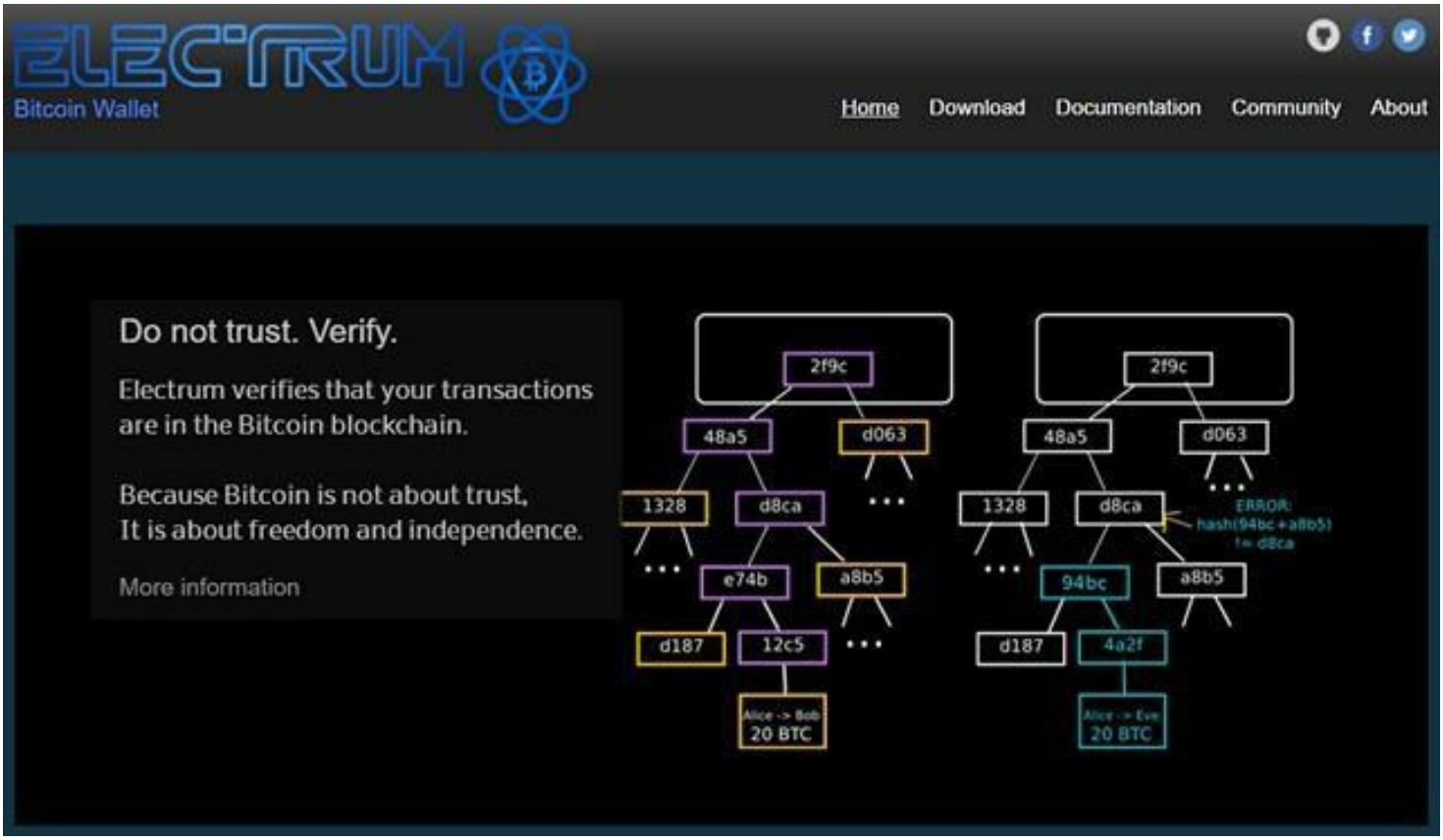
Multibit is a fast, lightweight client that comes in a variety of languages and can be set up and put into use within only a few minutes. Compared to other advanced wallets, Multibit is known for being user friendly, though could still be a bit difficult for newbie users. This is a

good choice for people looking for a fast and flexible Bitcoin wallet.

Recently Multibit was issued a new version called Mulitbit HD. Multibit HD has a much cleaner interface and it's also fully deterministic.
Pros: Fast, lightweight, and easy to set up.

Cons: Privacy features are known to be weak and security features could be improved.

Electrum Bitcoin wallet



This fast, lightweight desktop app is a good choice for someone using older and less powerful computers for their bitcoin storage. The most processor intensive parts of the wallet are handled

by remote servers. Electrum is well regarded for its advanced security and privacy features, and users can even recover their wallet with a secret pass phrase, though some people would prefer a wallet that doesn't rely on remote servers.

Pros: While many apps are processor intensive, Electrum is known for being fast and light weight.
Cons: Not friendly for newbies, and the reliance on external servers could present security threats.

Armory Bitcoin wallet review

Armory is one of the most reputed and secure Bitcoin wallets available in the market right now. It is complete with all the features you can think of – it is **open source**, includes **multisig support**, and it can make transactions using the **TOR network**. It also offers a rock-solid encryption and backup mechanism.

Pros: Very flexible and adaptable to just about any situation. Offers industry leading security features.
Cons: Requires advanced user knowledge and is not known for being user friendly.

Xapo Bitcoin wallet

Xapo is a web-based wallet system, so all's you need to access it is a web browser and Internet connection. Xapo is known for having reasonably advanced privacy and security features, especially for a web-based wallet. The company supports payments through a debit card system, making it easy to spend your Bitcoins. The app is also friendly for newbies, so if you're new to Bitcoin, give Xapo a close look.

Pros: Xapo debit card system allows you to use Bitcoin ATMs and spend at merchants across the world.

Cons: Web-based wallets face extra security threats, and you won't be able to manage your Bitcoins without a Internet connection.

CoinKite Bitcoin wallet

CoinKite is another newbie friendly, online only app that allows you to spend your Bitcoins at various merchants and

provides ease of use with numerous other features. CoinKite does require you to surrender control of your Bitcoins to the company itself. The service does feature some advanced security and privacy features, and also payment services that make it easy to spend your coins.

Pros: Easy-to-use and easy to access system that allows you to spend your Bitcoins with little effort.
Cons: Surrendering Bitcoins for third-party control carries a lot of risks and extra security hazards.

Green Address Bitcoin wallet

A user favorite, Green Address allows you to access your Bitcoins through a variety of methods, including online, through a mobile app, or through a

desktop client. Better yet, Green Address's is well regarded as being user-friendly. This makes Green Address one of the most flexible wallets around. Supports multi-signature features and has strong security and privacy features.

Pros: Very flexible and very easy to use, making Green Address a top choice for newbies

Cons: Requires the use of a remote app loaded from another location, and shared control over your Bitcoins (meaning the thirdparty has to approve payments).

Ledger Bitcoin wallet

Ledger is French start-up specializing in building hardware wallets for cryptocurrencies. It manufacturers various wallets like the Ledger Nano, Nano S and Ledger Blue. These wallets connect to your computer via USB and help in validating transactions when coupled with a software wallet.

Much like TREZOR, Ledger is a cold wallet designed for users who want increased security. The wallet is actually a physical device that connects to your computer and acts as another source of protection. Meaning, you can't send Bitcoins from your wallet without

owning the physical device.

Pros: Beginner friendly, very secure, great support.
Cons: Costs money, More security = less usability (this is an issue with all cold wallets).
Click here to visit Ledger's website

Copay Bitcoin wallet

One of the best Bitcoin wallets out there, it was created by Bitpay. Copay is a multisig wallet which means that a single wallet can have multiple users. This can be ideal for a corporate account where for example, 2 out of 3 signatures are required in order to confirm a transaction. The wallet also has a desktop, mobile and web interface and is completely independent and open source. **Pros:** Multisig wallet – allows for improved security, great design, supports multiple devices.

Cons: No support, can be a bit

overwhelming for beginners.

Click here to visit Copay's website

Chapter Four

Bitcoin Security

It is very important to think about the safety of the bitcoins you own. An online wallet can always be hacked using mall ware or key lockers, and this can cost you all your bitcoins. It is, especially for big amounts of bitcoins, always advisable to keep them in cold storage. Using a hardware wallet you can keep your bitcoins in cold storage and still make easy transactions.

All Bitcoins are known to remain in association to particular addresses alone and the only tangible items within the bitcoin Blockchain are the sender address, receiver addresses and the

amount to be transferred. The sender can always transfer their funds between many accounts to which they hold private keys to, the receiver address may change depending on the receiver (the keys to the accounts/wallets they hold access to) and the amount may be varied upon will.

Bitcoin to be transferred or already transferred remains within the Blockchain itself at all times. They cannot be removed or added, except by receiving the mining fee for mining the blocks which only adds to the network.

The easiest extra piece of security is to password protect the wallet by

encrypting it, but virus writers are starting to steal bitcoin wallets by searching for them on people's computers, so they could presumably use a key logger to steal the password too.

A much more secure way to store a bitcoin wallet is behind an **air gap**. The wallet can be stored on a USB drive that is not connected to any computer, or printed or written onto a piece of paper. These **paper wallets** are often created on a computer not connected to the internet which is wiped before and after the process, to ensure that no malware can access the wallet. Some bitcoin exchanges store their wallets behind an air gap in an actual **bank vault**, to add

extra physical security.

Which Type of Bitcoin Wallet Should Ideal for Use?

If you are taking a buy and hold strategy then the safest thing to do is to keep both a paper copy of your keys and keep another copy or so of your bitcoin location absolutely away from anything that touches the internet. This minimizes the risk of loss from outside sources. But the limiting factor with this strategy is it is hard as can be to spend your bitcoins and you also must be absolutely certain you will not lose those keys!

Holding the private key on self-such as a paper wallet is more suitable for a person concerned about security, privacy and selfsufficiency.

If you use Bitcoin to make small transactions frequently or you are little off-tangent when it comes to technical skills, Online Wallets are the easiest to use. If possible, you should replace online wallets with the more secure mobile or desktop wallets. If you do not like the idea of trusting third-parties with your private keys, then Paper Wallet is the way to go. Remember, you'll be in charge of keeping the paper wallet safe all the times. Shelling out some money and investing in a

Hardware Wallet is perhaps the most secure option available right now.

Mycelium is another great wallet. Keys to my mycelium bitcoin wallet are stored on an NFC chip Card which can be accessed only by bringing it within the vicinity of a NFC reader even after which, the key is encrypted again for additional security and the key to this encryption is online spread across different platforms forming a trailing pattern.

However, if you do decide to store your private keys with you on person, it is recommended that you keep it offline and off your computer and any hardware or software that could be compromised

since a private key if lost cannot be recovered. This means that you would lose access to your bitcoins forever unless you remember your key. Holding the private key with you on person would impel that you take complete authority for the security and anonymity over your account.

Personally I use Coinbase - Buy and Sell Bitcoin as an exchange to buy, hold, sell and transfer bitcoins and Ether since I'm way too careless and don't really worry about security to that extent. Insurance from the company, I find is much more reliable than selfasset management. "Exchanges" may be hacked now and then, given that Coinbase - Buy and Sell

Bitcoin itself has been hacked a couple of times to expose private keys of various people, but the determining factor is that the company does have insurance against such activities given in which case, you are safe.

How to protect our bitcoin against theft?

Bitcoin transactions are **irreversible**, since there is no official authority acting as an intermediary that is able to undo them. This is critical when the people involved on either side of the transaction don't know each other, since only the recipient of the payment can return it in the event of an error. For this reason, it is important to take extra precautions to **increase privacy**,

Be careful with online services

You should be wary of any service

designed to store your money online. Many exchanges and online wallets suffered from security breaches in the past and such services generally still do not provide enough insurance and security to be used to store money like a bank. Accordingly, you might want to use other types of Bitcoin wallets. Otherwise, you should choose such services very carefully. Additionally, using two-factor authentication is recommended.

Protect your identity

It is also important to be careful when sharing information about your transactions in **public spaces** like the

web, either voluntarily or unwittingly, so as to avoid revealing your identity together with your Bitcoin address.

Backup your wallet

Stored in a safe place, a backup of your wallet can protect you against computer failures and many human mistakes. It can also allow you to recover your wallet after your mobile or computer was stolen if you keep your wallet encrypted.

Make a *backup* of your virtual wallet

With regard to physical storage, as with any critically important *backup* policy, it is recommended to make frequent **updates**, use different media and

locations, and keep them **encrypted**.

Small amounts for everyday uses

A Bitcoin wallet is like a wallet with cash. If you wouldn't keep a thousand dollars in your pocket, you might want to have the same consideration for your Bitcoin wallet. In general, it is a good practice to keep only small amounts of bitcoins on your computer, mobile, or server for everyday uses and to keep the remaining part of your funds in a safer environment

Don’t forget about two factor authentication

When using *online* storage services, it is

important to undertake an extensive selection process to determine which are truly reliable. Even then, you have to bear in mind that any provider could end up being subject to the discovery of **vulnerabilities** in its systems.

As such, it is recommended to use **two factor authentication** and *online* services that support the use whenever possible, of **hardware wallets**.

Offline wallet for savings

An offline wallet, also known as cold storage, provides the highest level of security for savings. It involves storing a wallet in a secured place that is not connected to the network. When done

properly, it can offer a very good protection against computer vulnerabilities. Using an offline wallet in conjunction with backups and encryption is also a good practice. Here is an overview of some approaches.

Consider using multi-signature addresses

For corporate transactions, or any transactions that require a high level of security, it is possible to use multi-signature addresses, which involve the use of more than one key, the keys usually being stored on separate equipment in the possession of the authorized staff.

This way, an attacker will need to **compromise all the equipment** on which the keys are stored in order to be able to steal the *bitcoins*, making their task more difficult.

Keep your software up to date

Using the latest version of your Bitcoin software allows you to receive important stability and security fixes. Updates can prevent problems of various severity, include new useful features and help keep your wallet safe. Installing updates for all other software on your computer or mobile is also important to keep your wallet environment safer.

Although it is impossible to guarantee total protection of our assets from digital theft, this shouldn't stop us from enjoying the use of the technology. So long as we make sure to take the necessary precautions, there's no reason not to take advantage of the benefits offered by cryptocurrencies as they make inroads into our economy.

Conclusion

One of the biggest benefits to bitcoin is that you aren't trusting anybody with your value. Bitcoin ownership can be refined down to purely remembering a private key - no physical information. That's powerful. It's hard to even grasp how powerful that is. A t*hought* that can be worth vast amounts of value.

You don't have to have a bank with a password and several people managing it. You don't need an exchange run by some guy and his IT department. You can make yourself the supreme holder and manager of that value.

Regardless of what kind of electronic payment system you are using if you want to spend digital money then you need to have a digital wallet. Bitcoin differs from every other online payment system. Bitcoin has no central provider and anyone can build a bitcoin wallet. Consequently, there are several dozen bitcoin wallets to choose from and they all vary in terms of ease of use, security and advanced features which makes it important to carefully consider these bitcoin wallet

The fiat banking system (USD, Euro, etc) is like a walled garden. Not much can happen to your money in normal every-day use and your bank is responsible for

the security of your funds. If something goes wrong you can usually call someone (the bank or the credit card company) to fix the issue or even initiate a charge-back. You don't have to worry about backups or special procedures when handling your money.

This all changes with bitcoin. The problem is that the average user is not used to this radical shift in responsibility and as a result a lot of money can be lost by simple mistakes. And there is no one you can call to have it fixed. With bitcoin it is literally: "Be your own bank". And this also implies caring about security.

I hope this book has given you the

confidence to start your journey to bitcoin and cryptocurrencies market. Make sure you understand the concept of money and bitcoin and take advantage of newly emerging virtual currency. Have you benefited from this material? Leave your comments and valuable review on Amazon.

Thank you

Balkrishna poudel

DISCLAIMER

This book is created to inform readers about Bitcoin wallets and it related security. Although, I am trying to collect best and latest information and knowledge about bitcoin wallets and its security with possible option, but these materials are only responsible for the information purpose. Cryptocurrencies can be risky. Everyone is responsible for his / her own actions. I am not responsible for any form of damage, lost or theft when you get involved in it.