

Curso Básico

de Criação de
Carteira Para Bitcoin



A base de uma carteira para
bitcoin é a “Entropia”



A Entropia é um conceito da física, mais especificamente da termodinâmica, que traz como definição principal a desordem como resultado para tudo que nos rodeia. De forma técnica, podemos resumir a entropia como uma grandeza onde é possível determinar o número de configurações possíveis de uma aleatoriedade.



Em miúdos é transformar algo simples como um nome, uma data, um número, uma frase em um código.

Importante: “Sempre” esse nome, data, número ou frase gerará a mesma “Entropia”.



E para que servirá a tal da
“entropia”?



**Vamos fazer uma comparação
com a atual conta bancária que
conhecemos.**



Nossa conta no banco possui:

Nome do Correntista;

O Banco propriamente dito;

O código da agência;

O dígito do código da agência;

O número da conta;

O dígito do número da conta;

A senha do caixa eletrônico;

A senha do internet bank;

A biometria e

A assinatura.



Para Visualizarmos:

Nome: Santos Dumont

Banco: Banco do Brasil

Agência: 0321-0

Conta: 12746871-9

Senha: 999999

Senha na internet: 9999



Santos = Dumont



Na carteira bitcoin temos:

O número da carteira.



Para visualizarmos:

bc1qzw7t0a38ky7jhnfmjvusftc50gsaljnhdeg3th



Mas e a segurança disso?

Veremos mais a frente alguns métodos e níveis de segurança.



Vamos então a “criar” a sua
carteira de bitcoin.



Como visto anteriormente, a carteira de bitcoin é gerada através da entropia, veremos agora algumas formas de criar uma entropia.



**Existem 6 formas de entropia
aceitas, são elas:**

- Binária (0 e 1);
- Base6 (0,1,2,3,4,5,6)
- Dados (1,2,3,4,5,6)
- Base10 (0,1,2,3,4,5,6,7,8,9)
- Hexadecimal (0 a 9 e A a F)
- Cartão.



Para isso utilizaremos o site:

[Seed Tool \(bitcoiner.guide\)](http://bitcoiner.guide)

Seed = Semente

Tool = Ferramenta

Pode ser facilmente encontrado
no Google na pesquisa:

Ferramenta de Semente bitcoin

=

tool seed bitcoin ou seed tool bitcoin





Seed Tool

v2.1.0

About

This page offers a space for bitcoiners to experiment and learn how bitcoin wallets are generated using different sources of entropy (randomness). The page also offers many other seed related functionalities, some of which are outlined below. Just like the [tools and libraries](#) used in its creation, this tool is also completely free and [open source](#). If you find this page useful, consider [donating](#) some sats to the lead developer [SuperPhatArrow](#).

Warning

NEVER use the online version of this tool to create or interact with seeds used to manage real bitcoin. While there is nothing in this tool that collects private information or sends it anywhere, there may be other software on your device that does. If the tool detects a network connection, it will display a network symbol in the top corner of the screen. To use this tool offline, use the link below to download the page HTML file and open in any web browser on an offline device or an amnesic operating system like [Tails](#).

Download



Note que há um botão para “Download”.

Mais a frente veremos a sua utilidade em níveis de segurança.

Usage



Some common use cases for this tool include:-

- Learning how entropy is used to derive wallet components
- Generating seeds via dice rolls, coin flips or playing cards
- Verifying entropy inputs (dice rolls etc) applied to external wallets or signers
- Generating **BIP85** child seeds (or check those generated by a signing device)
- Generating **BIP47** payment codes and their corresponding **PayNym** avatars
- Generating BIP47 addresses between any two payment codes
- Verifying wallet address generation from a given seed/passphrase combination
- Testing for a forgotten/incorrect passphrase (if you know a receive address)

Seed Generation/Input



Derived Addresses



BIP47: Reusable Payment Codes



BIP48: Multisig



Mais abaixo temos:

Usage



Some common use cases for this tool include:-

- Learning how entropy is used to derive wallet components
- Generating seeds via dice rolls, coin flips or playing cards
- Verifying entropy inputs (dice rolls etc) applied to external wallets or signers
- Generating **BIP85** child seeds (or check those generated by a signing device)
- Generating **BIP47** payment codes and their corresponding **PayNym** avatars
- Generating BIP47 addresses between any two payment codes
- Verifying wallet address generation from a given seed/passphrase combination
- Testing for a forgotten/incorrect passphrase (if you know a receive address)

Seed Generation/Input



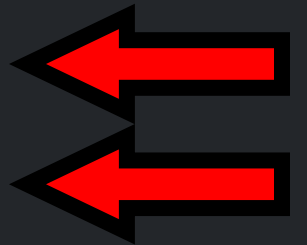
Derived Addresses



BIP47: Reusable Payment Codes



BIP48: Multisig



E utilizaremos apenas esses 2:

Seed Generation/Input

What is Entropy?



Generate



Enter y



Enter it

Gerador
Automático

ng random mnemonic
ated) mnemonic



Generate a Cryptographically Random Mnemonic of

12



words.

GENERATE

BIP32 Root Key

BIP32 Root Fingerprint




BIP32 Root Wallet Import Format (WIF)

No primeiro temos:



Seed Generation/Input

What is Entropy?

-  Generate a cryptographically strong random mnemonic
-  Enter your own (previously generated) mnemonic
-  Enter in your own entropy

Gerador de Carteira Com Base nas Seeds



Warning! Do not try to make up your own mnemonic, you are not as random as you think!

Mnemonic Length 12 ▼

01:	04:	07:	10:
02:	05:	08:	11:
03:	06:	09:	12:

NOTE: You can enter your BIP39 Passphrase below.

Load Seed




BIP32 Root Key



No segundo temos:

Seed Generation/Input

What is Entropy?

-  Generate a cryptographically strong random mnemonic
-  Enter your own (previously generated) mnemonic
-  Enter in your own entropy

Gerador de Carteira Com Base na Entropia

Warning! Entropy is an advanced feature. Your mnemonic may be insecure if this feature is used incorrectly.

Click on the orange button above to learn more.

Enter your own entropy:

Accepts either binary, base 6, 6-sided dice, base 10, hexadecimal or cards

Time to crack (zxcvbn using Filtered Entropy):

Event count:

Entropy type:

Avg Bits Per Event:

Raw Entropy Words:

Total Bits:

Filtered Entropy:

Raw Binary:

Binary Checksum:

Word Indexes:

Mnemonic Length:

12 Words

Entropy method:

Dice [1-6] eg. 62535634

No terceiro, que é o que nos interessa temos:

Seed Generation/Input

What is Entropy?



Generate



Enter y



Enter i

Gerador
Automático

ng random mnemonic
ated) mnemonic



Generate a Cryptographically Random Mnemonic of

12



words.

GENERATE

BIP32 Root Key

BIP32 Root Fingerprint

BIP32 Root Wallet Import Format (WIF)

Usaremos esse primeiro para entender como é gerada a carteira.

Seed Generation/Input

What is Entropy?



Generate



Enter y



Enter i

Gerador
Automático

ng random mnemonic
ated) mnemonic



Generate a Cryptographically Random Mnemonic of

12



words.

GENERATE

**Clique em
GENERATE**

BIP32 Root Key




BIP32 Root Fingerprint

BIP32 Root Wallet Import Format (WIF)

Usaremos esse primeiro para entender como é gerada a conta.

Seed Generation/Input

What is Entropy?

-  Generate a cryptographically strong random mnemonic
-  Enter your own (previously generated) mnemonic
-  Enter in your own entropy



Generate a Cryptographically Random Mnemonic of

12 ▼

words.

GENERATE

BIP32 Root Key

xprv9s21ZrQH143K2cj2koLdAgFT5qrkSVm6kWLqeUxqgEVamTtxwTmCHF1np5pxvJRuwNgM2znMNm3jxkCwAPYMuqfwF1Zh2s2kdSemCyotAZK


BIP32 Root Fingerprint


e5fde7c7


BIP32 Root Wallet Import Format (WIF)

L27VmXpHm15nVGE8xGytnTv3LyKnHbcYXsbHTsfeAq1rdgz7L2EX

Note que foram gerados alguns dados, desça um pouco na página.







Generate a Cryptographically Random Mnemonic of

12 ▾

 words.

GENERATE

BIP32 Root Key

xprv9s21ZrQH143K2cj2koLdAgFT5qrkSVm6kWLqeUxqgEVamTtxwTmCHF1np5pxvJRuwNgM2znMNm3jxkCwAPYMuqfwF1Zh2s2kdSemCyotAZK

BIP32 Root Fingerprint

e5fde7c7

BIP32 Root Wallet Import Format (WIF)

L27VmXpHm15nVGE8xGytnTv3LyKnHbcYXsbHTsfeAq1rdgz7L2EX


BIP39: Mnemonic code for generating deterministic keys


BIP39 Explained


BIP39 Mnemonic (English)

prefer fee all spice fresh insect tray cart faith half verify budget

Teremos então as 12 palavras que geraram a nossa carteira.







Generate a Cryptographically Random Mnemonic of

12

 words.

GENERATE

BIP32 Root Key

xprv9s21ZrQH143K2cj2koLdAgFT5qrkSVm6kWLqeUxqgEVamTtxwTmCHF1np5pxvJRuwNgM2znMNm3jxkCwAPYMuqfwF1Zh2s2kdSemCyotAZK

BIP32 Root Fingerprint

e5fde7c7

BIP32 Root Wallet Import Format (WIF)

L27VmXpHm15nVGE8xGytnTv3LyKnHbcYXsbHTsfeAq1rdgz7L2EX

BIP39: Mnemonic code for generating deterministic keys

BIP39 Explained

BIP39 Mnemonic (English)

prefer fee all spice fresh insect tray cart faith half verify budget






Clique aqui



Como dito anteriormente, a carteira é gerada a partir de uma entropia.

Seed Generation/Input

What is Entropy?

-  Generate a cryptographically strong random mnemonic
-  Enter your own (previously generated) mnemonic
-  Enter in your own entropy



Warning! Entropy is an advanced feature. Your mnemonic may be insecure if this feature is used incorrectly.

Click on the orange button above to learn more.

Enter your own entropy:

aa90fd761e9b8ff5dc09bd2afc70db354cb237b21b0c145ff307a20ab92e6191c53a84d55943e0a172466f4fd7bb37f55c413c6d53801f9a6ab
be1183756079a

Time to crack (zxcvbn using Filtered Entropy):
centuries

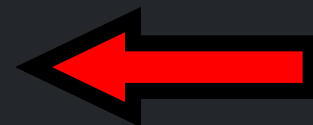
Event count:
128

Entropy type:
hexadecimal

Avg Bits Per Event:
4.00

Raw Entropy Words:
48/12

Total Bits:
512/128 (512 with bias)



Temos então
a entropia
que gerou a
carteira



Essa entropia que sempre retornará as mesmas 12 palavras.

aa90fd761e9b8ff5dc09bd2afc70db354cb237b21b0c145ff3
07a20ab92e6191c53a84d55943e0a172466f4fd7bb37f55c4
13c6d53801f9a6abbe1183756079a

ou

prefer fee all spice fresh insect tray cart faith half verify
budget



Qual dos dois é mais fácil de decorar?

Nenhum!



Agora, partindo do princípio que as 12 palavras são geradas a partir de uma entropia e que essa entropia sempre gerará as mesmas 12 palavras, nos resta saber uma maneira de gerar da forma mais fácil possível a entropia.



E se eu falar que você pode gerar uma das entropias mais seguras que existe, que é a hexadecimal de 128 caracteres de uma maneira que você nunca vai esquecer, você acreditaria?



Pode acreditar!



Com a evolução do sistema de criptografia, que consiste em esconder uma mensagem em outra mensagem que aparentemente não pode ser descoberta, chegamos a um nível chamado ‘Hash’.



Da forma mais simples
possível.

Um “hash” transforma
qualquer quantidade de
informação em um código
de letras e números fixos,
que pode ser o número
zero, uma palavra, um
nome, uma frase ou
qualquer outra coisa.



**Para exemplificar
utilizaremos um hash
chamado de SHA-3 512.**



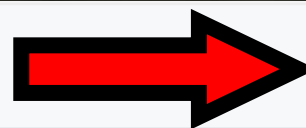
Vamos acessar o site:

github.com

e pesquisar:

carteiradebitcoin





Top Repositories

New

Find a repository...

ap10041973/kitbitcoin

Recent activity

When you take actions across GitHub, we'll provide links to that activity here.

Home

Send feedback

Filter 8

Updates to your homepage feed

We've combined the power of the Following feed with the For you feed so there's one place to discover content on GitHub. There's improved filtering so you can customize your feed exactly how you like it, and a shiny new visual design. ✨

[Learn more](#)

<> Start writing code

Start a new repository for ap10041973

A repository contains all of your project's files, revision history, and collaborator discussion.

Repository name *

name your new repository...

☐ Public

Anyone on the internet can see this repository

Introduce yourself with a profile README

Share information about yourself by creating a profile README, which appears at the top of your profile page.

ap10041973 / README.md

Create

1 - 🙋 Hi, I'm @ap10041973

2 - 📄 I'm interested in ...

GitHub Galaxy

June 18, 19 or 20

Join us virtually to explore our vision for AI-powered development, productivity, and modernization.

Register now



Latest changes

- 2 days ago
GitHub Copilot Compliance: SOC 2, Type 1 Report and ISO/IEC 27001:2013...
- 2 days ago
Dependabot now supports private Cargo

Filter by

- <> Code ...
- Repositories 1**
- Issues 0
- Pull requests 0
- Discussions 0
- Users 0
- More
- Advanced
- + Owner
- + Size
- + Number of followers
- + Number of forks
- + Number of stars
- + Date created
- + Date pushed

1 result (63 ms)

Sort by: Best match ▾



ap10041973/carteiradebitcoin



0 · Updated 19 days ago



Star



Sponsor open source projects you depend on

Contributors are working behind the scenes to make open source better for everyone—give them the help and recognition they deserve.

[Explore sponsorable projects →](#)

ProTip! Press the `/` key to activate the search input again and adjust your query.



Product ▾ Solutions ▾ Resources ▾ Open Source ▾ Enterprise ▾ Pricing

Search or jump to...

Sign in

Sign up

ap10041973 / carteiradebitcoin Public

Notifications

Fork 0

Star 0

<> Code Issues Pull requests Actions Projects Security Insights

main ▾

1 Branch 0 Tags

Go to file

<> Code ▾

ap10041973 Add files via upload

bdf60f · 3 weeks ago 5 Commits

carteiradebitcoin.rar

Add files via upload

3 weeks ago

About

No description, website, or topics provided.

Activity

0 stars

1 watching

0 forks

Report repository

Releases

No releases published

Packages

No packages published



Product ▾ Solutions ▾ Resources ▾ Open Source ▾ Enterprise ▾ Pricing

Search or jump to...

Sign in

Sign up

ap10041973 / carteiradebitcoin Public

Notifications

Fork 0

Star 0

<> Code Issues Pull requests Actions Projects Security Insights

Files

main

Go to file

carteiradebitcoin.rar

carteiradebitcoin / carteiradebitcoin.rar

ap10041973 Add files via upload

bdff60f · 3 weeks ago History

Code Blame 893 KB

Raw Copy Download Edit







View raw

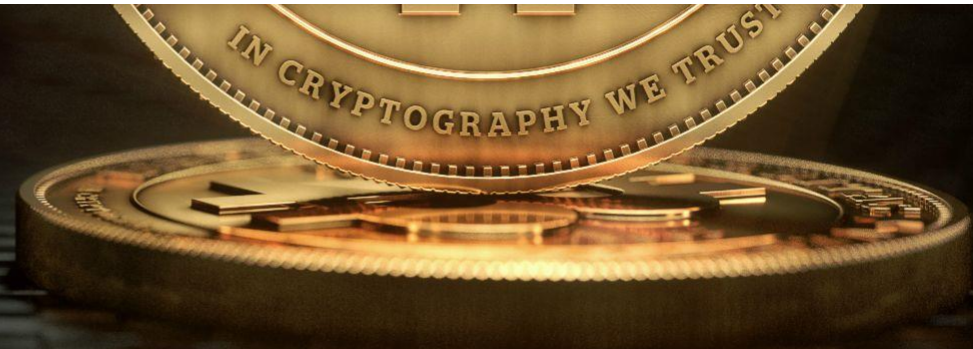


**Após o Download e
descompactação do
arquivo .rar temos:**





Nome	Status	Data de modificação	Tipo	Tamanho
 Converte Texto para Binário e Hash.html		03/09/2024 23:24	Microsoft Edge H...	4 KB
 Seed Tool v2.1.0 .html		30/11/2023 22:44	Microsoft Edge H...	6.739 KB
 sha3.min.js		11/02/2024 19:45	Arquivo JS	10 KB



**Pronto, temos tudo o que
precisamos para gerar a
carteira.**

**E o mais importante, off-
line – o que veremos mais
adiante.**



Vamos lá, agora já temos a página do Seed Tool e um gerador de entropia.

Isso tudo off line, muito importante isso.

E mais importante ainda, ter um ambiente seguro, veremos mais adiante.



O Seed Tool já vimos anteriormente e também onde fica a entropia que irá gerar as sementes. Vamos agora então ver como gerar a entropia.



Abrindo o arquivo

Converte Texto para
Binário e Hash.html

Teremos a seguinte tela:



Olha que maravilha, de acordo com o texto digitado temos a conversão para binário e diversos hash's.

Talvez não tenha ficado claro ainda, mas vamos a um exemplo para vermos na prática como funciona.

Converte Texto para Binário e Hash

Digite o texto:

01) Texto em Binário:

02) Texto criptografado SHA3-512:

03) Texto criptografado SHA3-384:

04) Texto criptografado SHA3-256:

05) Texto criptografado SHA3-224:

**Voltemos ao nosso
protagonista o Sr.:**

Santos Dumont

**Na caixa “Digite o texto:”
digite:**

Santos Dumont

**Cuidado para não colocar
espaço no final, isso muda
tudo.**

Converte Texto para Binário e Hash

Digite o texto:

01) Texto em Binário:

02) Texto criptografado SHA3-512:

03) Texto criptografado SHA3-384:

04) Texto criptografado SHA3-256:

05) Texto criptografado SHA3-224:

Pronto, agora com a tecla tab do teclado após pressionada duas vez estaremos no campo “Texto Criptografado SHA3-512:”

Com as teclas CTRL+C copiamos o conteúdo.

Converte Texto para Binário e Hash

Digite o texto:

Santos Dumont

01) Texto em Binário:

01010011 01100001 01101110 01110100 01101111 01110011 00100000 01000100 01110101 01101101 01101111
01101110 01110100

02) Texto criptografado SHA3-512:

aa90fd761e9b8ff5dc09bd2afc70db354cb237b21b0c145ff307a20ab92e6191c53a84d55943e0a172466f4fd7bb37f55c413c
6d53801f9a6abbe1183756079a

03) Texto criptografado SHA3-384:

db4d1063724dff0b2f1cf4fe8ceb388eac468b705b8c0c8c42a147b3fd0da5b890f4d71b5791aaca995c3332ef2245ee

04) Texto criptografado SHA3-256:

7d2ec0331405ba6038c55d2099009d5e18daf77dc45474845ad6915afbfc0f84

05) Texto criptografado SHA3-224:

d20430a4304b82d3731ce60a036fe6b403eeef90eebe0810757cafbe

**Agora voltemos no
Explorador de arquivos e
vamos abrir o arquivo**

[Seed Tool v2.1.0 .html](#)

clicando duas vezes nele.



Pronto, agora clicamos em
Seed Generation/Input
depois no ícone de dado,
e colamos com CTRL+v no
campo

Enter your own entropy:



**Rolamos a página para
baixo e.....**



Bingo!


BIP39: Mnemonic code for generating deterministic keys



BIP39 Explained

BIP39 Mnemonic (English)

prefer fee all spice fresh insect tray cart faith half verify budget

Compact SeedQR 



BIP39 Passphrase (recommended)

No passphrase entered!

BIP39 Seed

ce29d24b33770a641209520a75e366db379e3e8040015326872646f874e3e97c4d6611e03623451332b3b03259014c67424e7315f257bee3c358ddc
e852dedbe

Select a Bitcoin Tool

None



Derived Addresses



A tradução de “Libertas Aequitas Veritas” para o português é “Liberdade, justiça e verdade”.

Essa expressão latina é uma combinação de três conceitos importantes: “libertas” significa liberdade, “Aequitas” significa justiça e “Veritas” significa verdade. Juntas, essas palavras expressam a ideia de que a liberdade é alcançada apenas quando há justiça e verdade.

