

ساخت کلمات بازیابی بیت کوین

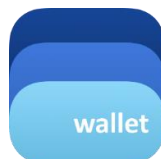
از استاندارد (BIP 39)

به صورت تصادفی

با استفاده از تاس

به همراه تست کیف پول و آدرس ها

با استفاده از کیف پول بلوولت



یک استاندارد برای ساخت کلمات بازیابی کیف پول‌های بیت‌کوین است که توسط اکثر کیف پول‌های HD پشتیبانی می‌شود، همچنین کیف پول‌های سخت افزاری موجود نیز کلمات بازیابی تولید شده توسط این استاندارد را مورد استفاده قرار می‌دهند و شما می‌توانید با ساخت این کلمات با این آموزش، آنها را برای کیف پول مورد نظر خود استفاده کنید.

در این استاندارد یک لیست ۲۰۴۸ تایی از کلمات انگلیسی استفاده و ترکیب ساخته شده این کلمات معمولا به صورت ۱۲ تایی یا ۲۴ تایی (به همراه یک pass phrase دلخواه) ساخته می‌شود.

شروع آموزش:

در این مقاله نحوه ساخت یک کیف پول بیت‌کوین با استفاده از یک یا چند تاس آموزش داده می‌شود. عملکرد آن به این شکل می‌باشد که با استفاده از تاس ما اعدادی از ۱ تا ۶ خواهیم داشت که با تکرار تولید اعداد با تاس یک عدد تصادفی به اندازه ۲۵۶ بیت بدست می‌آوریم.

طبق تعریف بالا و یک آموزش ساخته شده توسط جامعه بیت‌کوین فارسی از استاندارد BIP-39 ما یک جدول با ۲۰۴۸ کلمه متفاوت به زبان انگلیسی داریم، که با عمل تاس اندازی این کلمات را تصادفی انتخاب می‌کنیم، مثلا در ساخت یک کیف پول با کلمات بازیابی ۲۴ تایی، ۲۳ تا از این کلمات را با استفاده از تاس اندازی تصادفی انتخاب می‌کنیم اما کلمه ۲۴ام باید طی مراحل برای ما بدست آورده شود که این عمل توسط چندین سایت و برنامه که به منظور تنها همین کار طراحی شده‌اند به ما داده می‌شود.

آموزشی که بالاتر اشاره کردیم برای ساخت کلمات بازیابی توسط این استاندارد ارائه داده است. که توسط لینک زیر می‌توانید از آن نیز استفاده کنید. این لینک استفاده از تاس و ۲۰۴۸ کلمه را آموزش داده است که سایت نهایی آن تنها کلمه ۲۴ام را می‌دهد و بقیه ۲۳ کلمه توسط شما به طور تصادفی انتخاب می‌شود.

https://bitcoind.me/blobs/tuts/gen_bip39_bitcoin_seed_farsi.pdf

اما ما در این آموزش از سایتی استفاده خواهیم کرد که فقط از ما اعداد ۱ تا ۶ تاس را می‌خواهد، و ما عمل تاس اندازی را به اندازه ۲۵۶ بیت ادامه می‌دهیم. (میتوان از یک تاس استفاده کرد و تقریبا صد بار نیاز به تاس اندازی خواهد بود)

سایتی که از آن برای تولید کلمات بازیابی کیف پول استفاده می‌کنیم به آدرس زیر می‌باشد:

<https://iancoleman.io/bip39/>

توجه

در این مقاله برای ساخت کلمات بازیابی کیف پول، شما نیاز دارید آن را در یک سیستم کاملاً آفلاین و امن استفاده کنید. یک لپ تاپ کاملاً ایزوله و آفلاین، استفاده از tails os و مواردی از این قبیل.

همچنین سازنده این سایت نیز پیشنهاد کرده است که برای ساخت کلمات از حالت آفلاین استفاده کنید. یک صفحه HTML برای استفاده آفلاین طراحی کرده است. که با دانلود آن میتوانید دقیقاً همان صفحه وب آنلاین را به صورت آفلاین اجرا کرده و به ساخت کلمات بازیابی بپردازید.

در مرحله اول لازم به ذکر است که بگوییم این روش به هیچ عنوان یک روش پیشنهادی نیست و صرفاً یک آموزش بوده و استفاده یا عدم استفاده از آن به عهده خود شخص میباشد.

نگهداری کلمات بازیابی از مهم ترین بحث های نگهداری بیت کوین میباشد. طبق جمله مشهور

Not your keys, Not your Coins

اگر شما در نگهداری این کلمات کوتاهی نکنید تمامی بیت کوین خود را از دست خواهید داد.

لینک دانلود صفحه آفلاین این سایت در بخش ریلیز گیت هاب نویسنده قرار دارد:

Offline Usage

You can use this tool without having to be online.

In your browser, select file save-as, and save this page as a file.

Double-click that file to open it in a browser on any offline computer.

Alternatively, download the file from the latest GitHub release - <https://github.com/iancoleman/bip39/releases/latest/>

از این لینک فایل را دانلود و در این سیستم آفلاین و ایزوله آن را اجرا کنید:

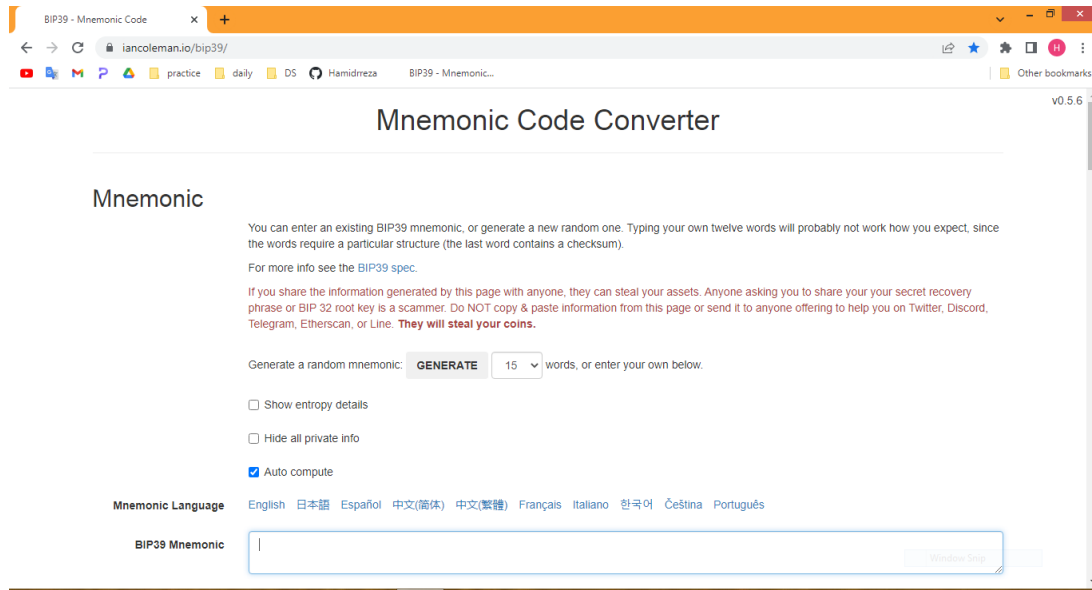
<https://github.com/iancoleman/bip39/releases/>

سازنده این صفحه امضای PGP خود را قرار داده است تا صحت درست بوده فایل را هر شخص بتواند بسنجد، و برای نحوه سنجش فایل و احراز صحت امضا و فایل میتوانید از آموزش زیر استفاده کنید.

https://archive.org/details/pgp_20201225

پس از احراز صحت فایل میتوانید آن را باز کرده و در ادامه به ساخت کلمات بازیابی کیف پول بپردازیم.

بعد از باز کردن فایل آفلاین داندلود شده به صفحه زیر برخورد میکنیم:

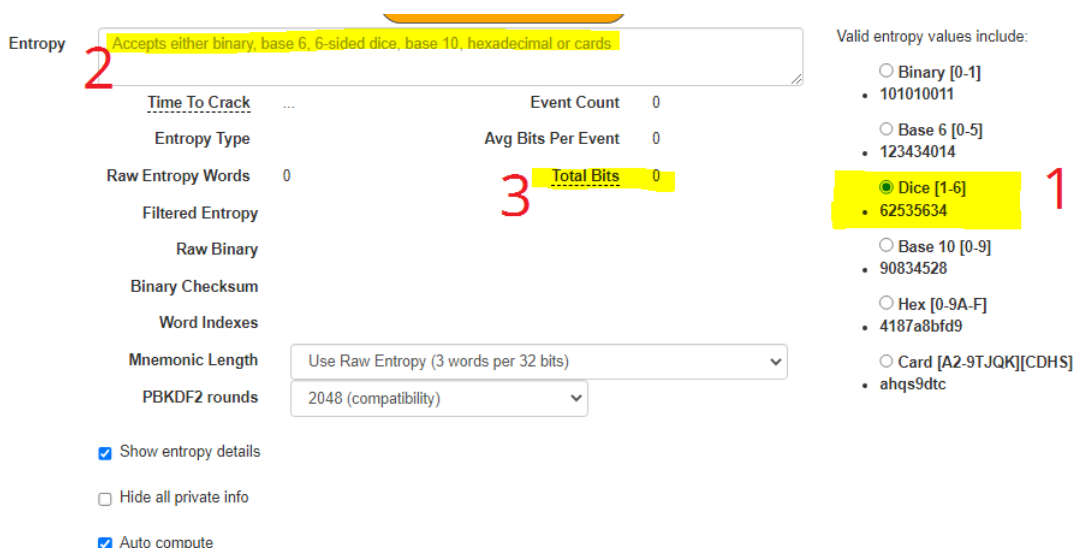


در کادر پایین صفحه کلمات بازیابی برای ما نمایش داده خواهد شد.

حال برای اینکه بتوانیم به تنظیمات بیشتری دسترسی داشته باشیم و تاس اندازی را شروع بکنیم باید تیک گزینه show entropy details را فعال کنیم.

☒ Show entropy details

بعد از فعال کردن در بالای این گزینه فضایی به شکل زیر باز میشود:



صفحه باز شده بعد از فعال کردن تیک show entropy details

در ابتدا تیک مرحله ۱ که مربوط به تاس میشود را فعال کنید.

بعد از فعال کردن آن در کادر مرحله ۲ باید به صورت متوالی و تصادفی (کاملاً تصادفی) تاس بیاندازید و نتایج را در آن بنویسید تا زمانی که در مرحله ۳ به عدد ۲۵۶ بیت برسید. که در تصویر زیر آمده است.

Entropy

153216543165423661523455555234615324154356426154236514365124356143162341543614
652412355162514365123443145631456245314345451652142546145641465146525431655162
54415551

Time To Crack	centuries	Event Count	164
Entropy Type	base 6 (dice)	Avg Bits Per Event	1.67
Raw Entropy Words	24	Total Bits	256
Filtered Entropy	15321054310542300152345555523401532415435042015423051430512 43501431023415430140524123551025143051234431450314502453143 4545105214254014504140514052543105510254415551		
Raw Binary	01111100100 10110100101 01100000111 01101111110 11000011111 00011011100 01000011010 11001010110 01011001110 00101101001 01100110110 00100011000 11011110100 10101011001 01101100110 10100110101 00100111010 11010101001 10010101000 01010000100 01010001101 01101001101 00101000111 101		
Binary Checksum	10101010		
Word Indexes	222, 1393, 529, 1594, 1164, 1014, 774, 648, 1674, 741, 932, 227, 275, 2023, 1289, 1395, 1617, 1186, 270, 1327, 566, 1691, 1157, 682		
Mnemonic Length	24 Words 4		
PBKDF2 rounds	2048 (compatibility)		

☒ Show entropy details

سپس به روی باکس مرحله ۴ کلیک کرده و با گزینه‌های زیر روبرو میشوید که میتوانید از آن تعداد کلمات بازیابی مورد نظر خود را انتخاب بکنید.

Mnemonic Length

PBKDF2 rounds

☒ Show entropy details

☐ Hide all private info

Use Raw Entropy (3 words per 32 bits)

Use Raw Entropy (3 words per 32 bits)

12 Words

15 Words

18 Words

21 Words

24 Words

در این آموزش از ۱۲ کلمه استفاده میشود و گزینه 12 Words را انتخاب کرده‌ایم.

BIP39 Mnemonic

bridge purchase drama shrug muscle learn general extra spend frequent innocent broom

☐ Show split mnemonic cards

BIP39 Passphrase (optional)

pass!

BIP39 Seed

10e19d536ae0a1c5ac27266f92a369485a6f94388576b86d041fa818ba19c8b51274dc4a8faeaae0d6ac9ad3f1d2447660b02758918611263704c0baf2f48b60

Coin

BTC - Bitcoin

BIP32 Root Key

zprvAWgYBBk7JR8GkF4bGjbP5t6ZxrFByKkt4dj4PwTU7WNqC1gjbKP6Aj3WWV8geGRUA6r6q2Uy2RDuE289ZdsoCjZKLUpI6i5R8DFmK6BPAA8n

☐ Show BIP85

مطابق تصویر بالا این صفحه برای ما ۱۲ کلمه بازیابی کیف پول را طبق مرحله ۵ نشان میدهد. این کلمات را جایی یادداشت و در حفظ آنها نهایت تلاش خود را میکنیم زیرا دسترسی به این کلمات یعنی دسترسی به دارایی شما.

در مرحله ۶ میخواهد که به صورت اختیاری یک کلمه pass phrase انتخاب بکنیم که پیشنهاد میشود این کار را انجام بدهید زیرا باعث امنیت بیشتر کیف پول شما میشود و در اینجا از کلمه pass1 استفاده شده است.

در مرحله ۷ یک root key برای شما نمایش داده میشود که با اضافه کردن pass phrase خواهید دید که root key عوض میشود و با هر تغییر کوچکی در pass phrase میبینید که باز هم root key عوض میشود که نشان دهنده تغییر در ماهیت (آدرس ها) کیف پول شما با هر کلمات متفاوتی خواهد شد.

تا اینجا کیف پول ساخته شده است و میتوان آن را در کیف پول های مختلف مثل بلوولت یا سامورایی ولت و ... اضافه کرد.

حال به بررسی آدرسهای این کیف پول ساخته شده میرسیم، که در پایین صفحه قابل مشاهده میباشد.

Derivation Path

BIP32 BIP44 BIP49 BIP84 BIP141

8 9

For more info see the BIP84 spec.

Purpose 84

Coin 0

Account 0

External / Internal 0

The account extended keys can be used for importing to most BIP84 compatible wallets.

10 Account Extended Private Key xprvAcmZeBnp4ZsucfqJCQ7sRD4A53Kmgw7C5FaFY7nmEAKSRjC6K5Ln9PGnzhC5PKzA3Ycm4Q2E1Za1yjdbyPecnr1qvDbEx5PBHMF9JlePDV

11 Account Extended Public Key zpub66qMM3hKhtvSCq9umJResnLztdSAG6Pq3SUVrLWCNnVrJXXErcf2hBbGqy2gPykvCeMCxb1xq3pSamiNWoycct14u1pDXhfdTPvhvJmoqnC

The BIP32 derivation path and extended keys are the basis for the derived addresses.

BIP32 Derivation Path m/84'/0'/0'/0

BIP32 Extended Private Key zprvAfkG3MYduQPEq5iZqZyx5GYSD6jsdNct5qrbQYc6eCGCMi34EatUx9M87Q2KdMcSRN8ZxZ5g6FNBWfPzD8yHDsr3weQ2xdMhvDAEP5bP

BIP32 Extended Public Key zpub6tKCSs5XjmwY3Zo34m6zKDDGzEwEH66UFJmTPnxDejFYzgrabYqSHGdCRDkRdhtVIM8rhT9XhbxH3YdBpavRLtm6SUIRgTaaa1m7yuCj9y

همانطور که گفته شد در پایینتر صفحه به تصویر بالا میرسیم.

میتوان از استانداردهای مختلف آدرسهای بیت کوین مثل native Segwit یا Legacy استفاده کرد. با انتخاب مرحله ۸ به آدرسهای Legacy بیت کوین که با عدد ۱ شروع میشوند دسترسی و با انتخاب مرحله ۹ به آدرسهای native Segwit دسترسی خواهید داشت. اینجا ما از مرحله ۹ استفاده میکنیم.

در مرحله ۱۰ کلید خصوصی و مرحله ۱۱ کلید عمومی (zpub) کیف پول را نشان میدهد. با استفاده از کلید عمومی (مرحله ۱۱) کیف پول را میتوان درون بقیه کیف پول‌های آنلاینی که از قابلیت watch only پشتیبانی میکنند مثل بلوولت اضافه کرد و دارایی بیت‌کوین خود را مشاهده کرد.

در مرحله آخر ساخت کلید بازیابی کیف پول بیت‌کوین باید از صحت کلید عمومی (zpub) و آدرسهای دریافت اطمینان حاصل بکنیم.

در آخرین بخش صفحه ساخت کلید بازیابی توسط تاس به بخش آدرسهای دریافت میرسیم. که به صورت تصویر زیر است:

Derived Addresses

Note these addresses are derived from the BIP32 Extended Key

☐ Encrypt private keys using BIP38 and this password: Enabling BIP38 means each key will take several minutes to generate.

☐ Use hardened addresses

Path	Address	Public Key	Private Key
m/84'/0'/0'/0/0	bc1q1nwuw5vhktrz000gj6kflxdslegst6dtagzf35	02732ce82fb9fa39c9863d85d08d752396ddf9739513136b541418435c3d6de7fd	L3H4wH9jWfKjYwe8f2bUREfSziG
m/84'/0'/0'/0/1	bc1q8541t873t5dmpwmsa00flw3dmj949c0qlrnx	023abf6954ccc08f01f5187da00f9b2b4ba8f974c38c48fb65c79ec0bffd44d30	L4hswYhJgP9HzHVLQ754KabFgV6U
m/84'/0'/0'/0/2	bc1qdtj2x4xmy4vn2amuj7v4y5j1czt5ngl9xd	02a4ad67d72d696f23e0b1d4e1fbb7d6854d1601942f5a3bc4fe3daf2d05d34f7	Kzg48Y7vFRNceXNoTswiVL4QYnWn
m/84'/0'/0'/0/3	bc1qwgj93see3xs8j3jvyn8m6esuekekvhwcy7t7c6f	0279946389a670ea2bfc43af1931d75f025455cf519ecd5dad94367b42c4c29b	L221u5kHaW5DTSKnfFYXDCP1xBUN
m/84'/0'/0'/0/4	bc1qm045xat90wlg22ysecj8pukc6shsdtgeeagg4	0221ec19985235a3f78a82a31f8b2d3bcfdadf7bf415248a4abc7cca25ddb5e336	KwPwLGk2o4Pqdz6mko8DYJpMybFd
m/84'/0'/0'/0/5	bc1qxmfwry4k3qfnk2wpjrc58rsqa9awg65r2ayau	02f65518c70286c67279b14f7576d3cd5899246480a2f665b9e7b86ed5e55db47b	Ky4cVt6wXr9ymLupzdX621WVwHx
m/84'/0'/0'/0/6	bc1q69g678pntqn3s9gle8j1cvk7qf8rm6zvactt6	0387a1768d01b3c45cf9d968a3f3156a4dc607fe0166176cbfd54091f6cdfb3e76	L5UwQQtiZ58KoLnTTMGhCjmlVaaZE

در این تصویر آدرسهای دریافت به همراه کلیدهای عمومی و خصوصی آنها به صورت کامل نشان داده میشوند.

پس از ساخت کلمات بازیابی به صورت تصادفی با تاس، وقت این میرسد که بررسی کنیم و ببینیم آیا این کلمات، کلیدها و آدرسها اعتبار دارند! به منظور این کار این کلمات بازیابی را داخل کیف پول بلوولت اضافه کرده و به صورت دستی به ارزیابی کار خود میپردازیم.

در این آموزش ما کیف پول تولید شده خود را به دو صورت برای ارزیابی میتوانیم در بلوولت اضافه بکنیم.

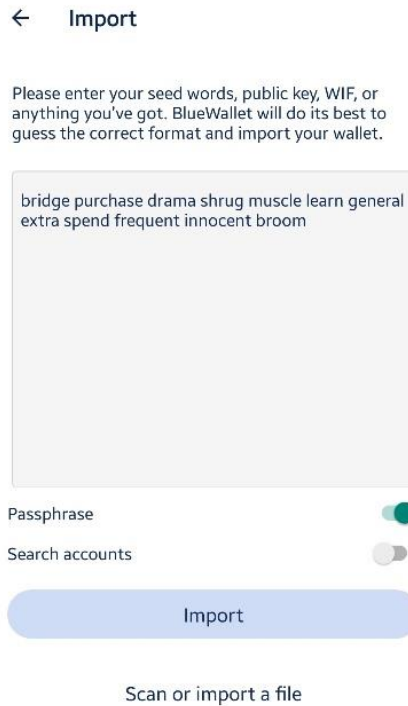
- ۱: کلمات بازیابی تولیدی را به بلوولت اضافه بکنیم
- ۲: فقط zpub را به کیف پول بلوولت بدهیم و از بلوولت به عنوان watch only wallet استفاده بکنیم.

هدف این آموزش استفاده از روش دوم است. زیرا با وارد کردن کلمات بازیابی شما آن را یک دستگاه آنلاین وارد کرده‌اید و هدف ما تولید این کلمات به صورت آفلاین و ایزوله میباشد و نباید در هیچ دستگاهی که به اینترنت متصل میشود وارد کنیم.

وارد کردن کلمات بازیابی به بلوولت به هر دو صورت:

در ابتدا وارد بلو ولت شوید و گزینه + را به منظور اضافه کردن ولت جدید انتخاب کنید.

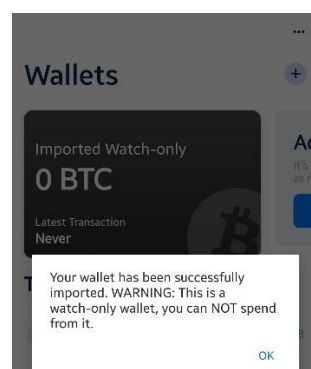
در پایین صفحه باز شده گزینه import wallet را انتخاب کنید و کلمات بازیابی را به این بخش اضافه کنید. همچنین zpub را نیز میتوانید به منظور استفاده watch only اضافه کنید.



پس از وارد کردن کلمات بازیابی کیف پول شما به شکل تصویر زیر اضافه میشود:



و اگر zpub را وارد کنید کیف پول شکلی چنین خواهد داشت:



و به شما میگوید که از یک کیف پول watch only استفاده میکنید و نمیتوانید موجودی آن را خرج کنید. (در این حالت فقط با کیف پول میتوانید دریافت داشته باشید و موجودی دارایی خود را بررسی کنید که این روش پیشنهادی برای کسانی است که میخواهند برای بلند مدت بیت کوین خود را نگهداری کنند)

پس از وارد کردن کیف پول در بلوولت، میتوانید از گزینه بالا سمت راست صفحه به تنظیمات کیف پول رفته:

← Wallet Save

name

Imported HD SegWit (BIP84 Bech32 Native)

type

HD SegWit (BIP84 Bech32 Native)

transactions

Display in Wallets List

transactions count

0

Show addresses

Export/Backup

Show Wallet XPUB

Sign/Verify Message

Delete

با انتخاب گزینه show wallet xpub میتوانید همان zpub کیف پول خود را بررسی کنید و تطابق بدهید.

همچنین با گزینه show addresses به آدرسهای دریافت دسترسی خواهید داشت، و میتوانید آدرسهای دریافت تولیدی با تاس را با آدرسهای بلوولت تطابق داد که به صورت زیر میبینیم که آدرسها یکی هستند.

Addresses	
	Receive Change
1 bc1qlnwuw5...gst6dtagzf35	Receive
0 BTC	Transactions: 0
2 bc1q8854lt...mj949c0qlrnx	Receive
0 BTC	Transactions: 0
3 bc1qdtj2x4x...jlczt5ngl9xd	Receive
0 BTC	Transactions: 0
4 bc1qwgj93s...kvhcwy7t7c6f	Receive
0 BTC	Transactions: 0
5 bc1qm045x...shsdtgeeqgq4	Receive
0 BTC	Transactions: 0

bc1qlnwuw5vhktr000gj6kflxdslegst6dtagzf35

bc1q8854lt873t5dmpwnsa00flw3dmj949c0qlrnx

bc1qdtj2x4xmy4mv4vn2amu7v4y5jlczt5ngl9xd

bc1qwgj93see3xs8jjvyn8m6esuekekvhcwy7t7c6f

bc1qm045xat90wlgy22ysecj8pukc6shsdtgeeqgq4

حال متوجه خواهیم شد که کلید عمومی و آدرسهای دریافت کلمات بازیابی تولید شده توسط تاس به صورت سالم تولید شده‌اند و در کیف پول موبایلی نیز تطابق کامل دارند.

این آموزش جهت آشنایی و آزمایش برای کاربران علاقه‌مند به بیت‌کوین ساخته شده است و هیچگونه پیشنهادی برای انجام این روش نمیشود و خود شما باید برای ساختن، نگهداری و نحوه استفاده از کیف پول بیت‌کوینی خود تلاش کنید.

لازم به ذکر است بگوییم که ذات انسان به دنبال راحتی بوده و استفاده از روشهای صحیح ساختن کیف پول، نگهداری و مسئولیت‌پذیری از بیت‌کوین را (شاید) کاری دشوار بخواند. مراقب دارایی خود باشید.

این راهنما برای "استفاده عموم" منتشر میشود و بازنشر آن به هر شکل آزاد است.

سازنده:

حمیدرضا

Follow me on



Twitter: @hamid_rreza



Nostr:

npub1jjw63779gl2lan6yu2fz3w67ruja40mnh8s3npvhesx82m4yvlsq4wg49z



WOS: spicyinvoice19@walletofsatoshi.com