

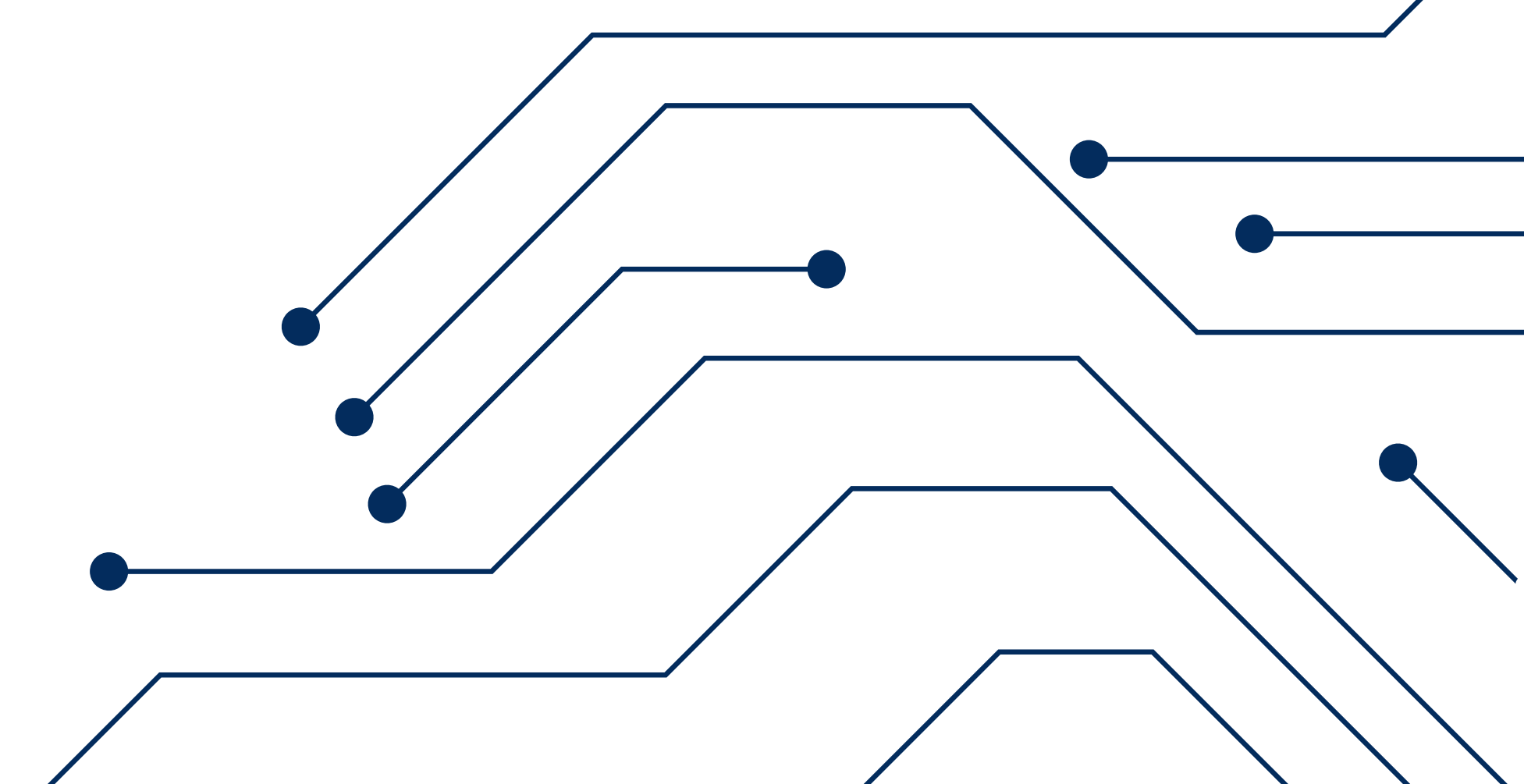
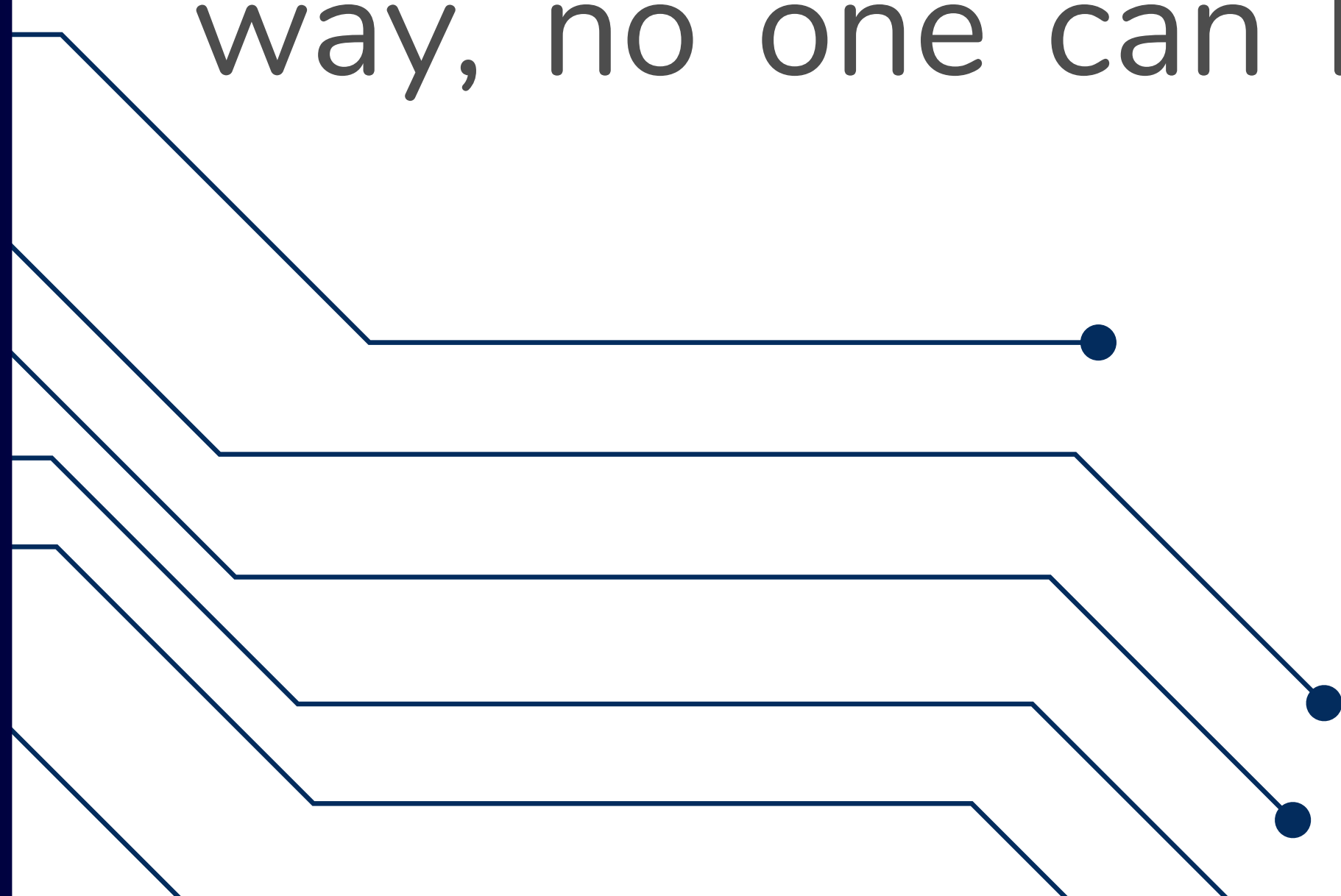
INTRODUCTION TO CRYPTOCURRENCY WALLETS



Cryptocurrency wallets are basically software that contains the cryptographic keys to the cryptocurrencies one owns. The way it works is that cryptocurrencies must be stored on a wallet in order to transact on an exchange or simply to be held onto. Without the keys to the wallet, which are usually 10-12 different words in a particular order, one would have no way to access the cryptocurrencies on the wallet.

Wallets can either be cold storage or hot storage. The difference between the two is very simple. Cold wallets are stored offline using devices like a Ledger Nano or Ellipal wallet. These wallets store cryptocurrencies offline so that they can't be hacked into or taken control of. The only person that can access the cryptocurrencies stored on cold wallets is the person that has the keys to the cold wallet. Hot wallets, however, are more easily hacked if not used correctly. A hot wallet could be a wallet on an exchange like Coinbase.

All wallets will display your specific keys to that wallet only once, and it is your responsibility to write it down somewhere that it is safe. This way, no one can log into your wallet without your keys unless they

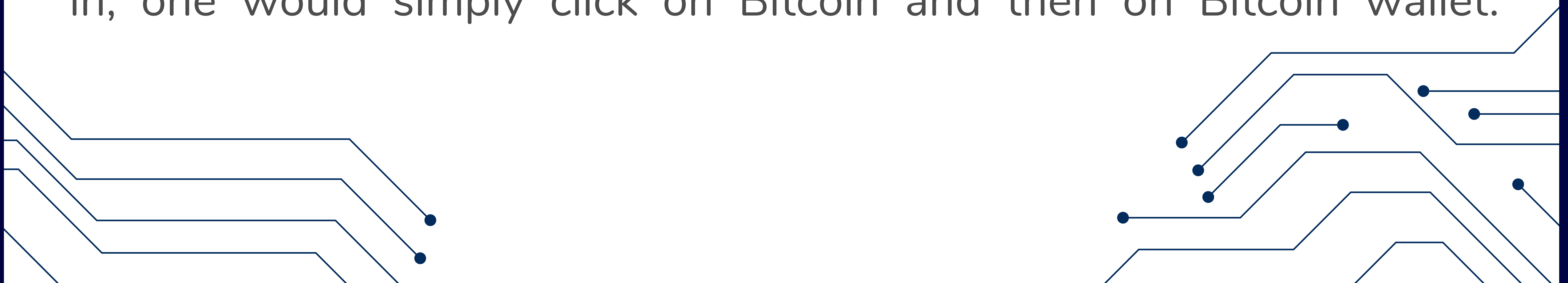


have your username and password for hot wallets that is. Cold wallets can't be accessed at all because they aren't connected to the web and only the owner can access the cryptocurrencies stored on the wallet.

Cryptocurrency wallets not only store your cryptocurrencies for you, but also act as your address from which you can send your cryptocurrencies to exchanges or to other addresses. Essentially, if your cryptocurrencies are stored on a wallet, you will lose access to the cryptocurrencies if you lose your keys or login information.

Wallets are always recommended to use two factor authentication when logging in for security purposes. It is always a good idea to have as much security employed on your cryptocurrency wallets as possible. They can become a target for hackers if left too unsecured.

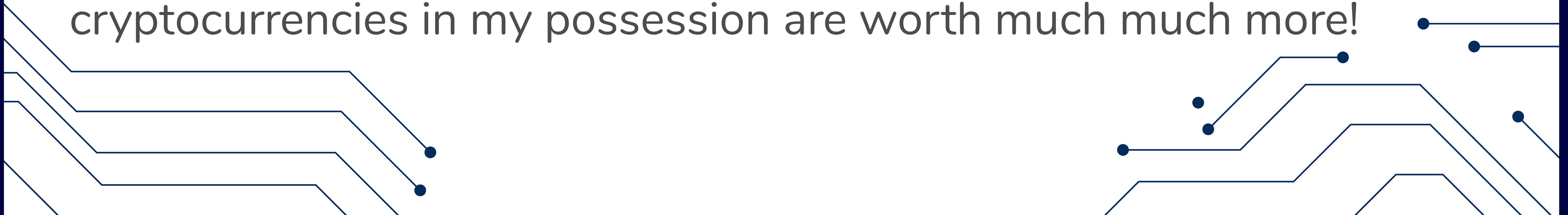
Setting up a wallet for a specific cryptocurrency is usually as easy as searching which exchanges or wallets that specific cryptocurrency is available on. For example, if one wanted to just start a Bitcoin wallet, it would be as simple as signing up for a Coinbase account. Once logged in, one would simply click on Bitcoin and then on Bitcoin wallet.



Coinbase would then display the Bitcoin wallet address that the individual could use to transfer Bitcoin to.

Other newer cryptocurrencies are sometimes harder to find a wallet for. For example, recently I wanted to buy \$HBAR or Hedera Hash graph, and I signed up for a wallet through their website, but have still been waiting to get one created. So, I downloaded Atomic wallet instead which allows for \$HBAR wallets within the application. Now, I have my \$HBAR stored on Atomic wallet with no problems. If I wanted to sell it at any time, I would simply go to the exchange I can sell it on, copy my \$HBAR address from that particular exchange, and send it to the exchange to get ready to put it on the market.

I've found that it's best to keep cryptocurrencies off exchanges as much as possible. By storing your cryptocurrencies on a cold wallet like Nano Ledger or Atomic wallet, it is much safer than leaving it on an exchange that could get hacked or taken down any day. I try to only send my cryptocurrencies to exchanges if I am planning to sell or use them to buy other cryptocurrencies on that particular exchange. But, typically my plan is to HODL or hold on for dear life until the cryptocurrencies in my possession are worth much much more!

Decorative circuit lines with blue dots at the ends, located at the bottom of the page.