Yo, I'm here to clear up some major misconceptions about crypto wallets, especially when gamestop releases theirs. Misunderstanding might even lead to you getting scammed. I'm gonna try to keep it very simple and might cut some corners and some inaccuracies for the sake of simplicity and understanding.

I'm gonna do a **crayon style explanation** and the equivalent in *blockchain terms.*

Anyway, feel free to add, or ask questions (AMA Style).

BASICS: where my crypto at, ser?

Your Tokens, Coins, and NFTs are saved on the blockchain. Imagine a public list, like a shareholder register, or, simpler, a list of scores on the Game Crayon Control test.

On this list, there are entries, depicting the scores of all people that partaked in the GCC test, and who scored how much. But, you don't want anyone to know, how much you scored, so everyone uses a pseudonym.

https://preview.redd.it/nvtisfa7h6q81.png?width=830&format;=png&auto;=webp&s;=3e3bb6e870fa128b6ed92f9ab60442ee971234b2

On the blockchain, each token or NFT is a smart contract. The smart contract keeps track of the holders, and how much of a token (or, in case of NFTS, which token) each holders has. A holder is identified by their address, which start with 0x (zero - X).

https://preview.redd.it/bilfquh9h6q81.png?width=835&format;=png&auto;=webp&s;=fe2f92f11cb31853ee8d3057f6a7f82fd4e13f19

\\\

BASICS: where am i???

Y**ou get a pseudonym by a pseudonym generator. This generator has a system that always creates a specific (and constant) pseudonym, given specific (and constant) answers to questions.**

Going trough this list, like a Choose-Your-Own-Adventure, your favourite color is "green", you are born on "March, 10th, 1942", and you Surname is "Drsosten". You get the name "Ken B Shawn", and you got a score of 69 (nice) on the GCC test. Bazrillions of names and combinations make it impossible to find out what your color, brithday, and name is.

https://preview.redd.it/op8garnbh6q81.png?width=842&format;=png&auto;=webp&s;=85a2887e88f9814ec9ff0da5f25d895c9caad180

Your address is 0x0ae7b628c71a2. The 0x address is created deterministically from you seed phrase. These are 12 or 24 words, taken from a dictionary of 2048 specific english words (more [*here*](https://en.bitcoinwiki.org/wiki/Mnemonic_phrase)*). Your seed phrase creates always the same address, (and enables you to create more addresses). The seed phrase is also your mnemonic phrase, or recovery phrase.*

NEVER SHARE YOUR SEED PHRASE

*This process is very safe. It's impossible to reverse engineer this process, so no one can find out the

seedphrase which generated a specific 0x address. The 0x address is your PUBLIC KEY, or PUBLIC ADDRESS. It will always start with 0x. You can safely share it with others.*

https://preview.redd.it/j1swd8ych6q81.png?width=838&format;=png&auto;=webp&s;=b508266bf68de85af dc1b82d644472aeefb74708

\\\

BASICS: giev me my tendies

Now, you want to claim your price for scoring 69 (nice) points on the GCC. So, you go to the place where you made your test and want your tendie plushie. But how do you proof, that you are "Ken B Shawn"? Well, easy. The pseudonym generator can also create a password. So, you type in the password into the test verification device, and it confirms - yep, you are indeed "Ken B Shawn".

Now you can receive your tendie plushie.

https://preview.redd.it/5lz8t9kgh6q81.png?width=661&format;=png&auto;=webp&s;=2d839454e17f1ba14f 95c94b0d6cfcd4a1fc765d

Your seedphrase also generates a private key for each public key. Again, this is a deterministic process, so your seed phrase will always generate the same set of matching private keys. A private key is the "password" to prove you own the 0x address. A private key will NEVER start with "0x" and is longer than your public key (the 0x address).

You interact with a smart contract by creating a request, and signing it with your private key. This verifies your ownership, and will allow you to properly interact with the smart contract for $GCC, such as retrieving your tokens.

NEVER SHARE YOUR PRIVATE KEY. Losing/Sharing it, compromises your 0x address. Losing/sharing your seed phrase compromises ALL of your 0x addresses.

https://preview.redd.it/nxwn5jkih6q81.png?width=838&format;=png&auto;=webp&s;=0c0d75dc7832439ff2 a9f500bbcf3b6bdd34cc52

BASICS - that sounds complicated

Alternatively, you can also get yourself a robot, tell it your favourite color, birthday, and name, and it takes care of managing your passwords and tests. Nice.

You can use a programm to make requests with your private & public key, or use a "wallet/wallet provider" to save your seedphrase/private, which takes care of the proper interaction with smart contracts for you.

\\\

SO WHAT NOW?

So, Metamask, Trust Wallet and others are wallets. A wallet is just a small programm, which manages your private keys. You tell your wallet your seed phrase, it generates the proper public and private keys, and you can do stuff.

Your crypto is NOT in your wallet (like Metamask). Your crypto, tokens, coins, and NFTs are on the blockchain. Or, let's say, your crypto stuff is in your PRIVATE KEY, or in your SEED PHRASE

REMINDER: NEVER SHARE YOUR SEED PHRASE, RECOVERY PHRASE, MNEMONIC PHRASE, PRIVATE KEY, PRIVATE CODE, or a QR CODE generated by your wallet. (Unless you know what you are doing!)

So, metamask is a "decentralized" and, more important, **self-custodial wallet**. If you don't like

Metamask, ditch it, and go to a different wallet provider, put in your seed phrase, and off you go to the world of blockchain and web3. Metamask or any other people from the Metamask company can NOT prevent your access*, block you*, or steal your crypto.

Unless, you get scammed, by connecting to a weird site, interact with a weird contract, or if you get hacked and you have your seed phrase or private key lying around unencrypted and/or plain text.

^((Access can be blocked by geoblocking or ipblocking you from using a blockchain node - just use a different node, or spin up your own. In 99.9% you will never need to do this. Personally, I have my own node, hosted on a privary focused service, and interact with it via VPN. A node can, in theory, record your IP and metadata during access, thus nulling privacy if that is a concern.)********)*

KEEP YOUR SEED PHRASE OFFLINE IN PAPER/STEEL, LEARN AND MEMORIZE IT, OR SAVE PARTS OF IT IN DIFFERENT LOCATIONS. IN 999 of 1000 cases you won't need to export or use your private key.

There are wallets like Argent or Loopring Smart Wallet. These are SMART wallets.

In short: Your wallet, in this case, is a Smart Contract, and you are the only one who has acces and interaction rights with this smart contract. A smart contract is not as easy to transfer like using a raw seed phrase, but might be safer for some, as it contains safety and verification features.

Make sure that you trust the Smart Wallet, and know which rights and interactions the contract gives you. In MOST cases, a Smart Wallet is self-custodial. But, it does not need to be. Regardless, a Smart Wallet is MOST of the time a safe thing to prevent common scams and hacks as described above.

NEVER SHARE YOUR SEED PHRASE, PRIVATE KEY, QR CODE, or SCREENSHARE YOUR QR CODE. NO SUPPORT MEMBER WILL ASK YOU ABOUT THIS. MOST SUPPORT DOES NOT NEED TO BE IN DMs OR IN PRIVATE MESSAGES. NO, YOU DON'T NEED TO 'SYNC' YOUR WALLET, OR ACTIVATE IT WITH A SERVER, OR UPGRADE IT TO ALLOW WALLET CONNECTION. DON'T FALL FOR SCAMS, TIME IS NOT AN ISSUE, IF IN DOUBT, ASK IN A PRIVATE CHANNEL OR FORUM, AND WAIT FOR ANSWERS.

If it sounds too god, it probably is a scam. Interacting with a bad smart contract might expose you to security risks. Interacting with a bad site might lead to security risks.

A wallet will NEVER ask you twice for your seed phrase. Or need your seed phrase for verification. If it does, your wallet extension, software, or app might be compromised. Or you are on a fake site which fakes your wallet. AFAIK, scams regarding Smart Wallets are not here yet. Just to be safe: Never add a guardian or safe person, without veryfing.

IF YOU HAVE ANY QUESTIONS, ASK AWAY! There are no dumb questions! I can make it in crayons too.

TL;DR: DONT SKIP THIS POST! READ IT AND UNDERSTAND IT IF YOU PLAN TO USE THE BLOCKCHAIN.