Title: Crypto Wallets and Decentralized Apps - An Overview
Author: disoriented_llama
Created 2022-05-25 12:05:45 UTC
Permalink: /r/TheGloryHodl/comments/uxfvls/crypto_wallets_and_decentralized_apps_an_overview/
Url: /r/Superstonk/comments/ux9gch/crypto_wallets_and_decentralized_apps_an_overview/

Linked Post Content:
Peace and love Apes. Very exciting times for everyone with the release of the long-sought after GME Wallet. I've seen a lot of ape-ing into it which I think is beautiful in some regards but also dangerous. And so, I wanted to write up some DD on wallets to make sure everyone is staying well informed and safe.

One of the greatest hurdles in Crypto has been the complexity and mystery of wallets, so it is natural many have not taken the time to really understand the fundamentals... Which I think are important for any major decision in our life, especially cryptographic assets.

I'm going to format this as follows:
\- ELI5 metaphor of what different wallets mean/do
\- ELISEC graphics for the visual learners out there (read from bottom to top)
\- Longer reading towards the end if you feel inclined

\~\~ Please lmk of any corrections or additions to text or graphics and I will gladly fix it \~\~

# Explain Like I'm 5

When we go outside to play `(use web3)`, we will need to be wearing pants `(a hot wallet)`. Pants help keep our legs and privates safe `(seed phrase/private keys)`, and generally make us socially acceptable.

Some occasions `(decentralized web apps)` call for blue pants `(meta mask)`, some call for green pants `(GME wallet)`. Some occasions give us options to wear many different kinds of pants based on our preference, because they set a relaxed dress code `(programmed many wallet options into their site)`.

BUT just wearing pants can be a risk. What if they get torn `(hacked)`, or soiled `(phished)`.. Someone at the function might be able to see our legs and privates `(keys)`! So another layer of protection is wearing draws/panties `(hardware/cold wallet)`. No one is allowed to see our draws except us, or if granted express permission `(manually approving transactions on device)` . And they help keep our legs and privates super secure `(writing down our private seedphrase on paper, in safe keeping)`

If we change pants, for example from blue to green `(migrating wallets)`, only the outside changes.. but inside we have the same legs and privates `(seed phrase/private keys)`.

# Explain Like I'm SEC

[Cold vs Hot wallets](https://preview.redd.it/cx213hmvdj191.png?width=1500&format;=png&auto;=webp&s;=df1b737978ec2f0ed49b45e06635068906521aae)

There are two basic types of wallets:
Cold (hardware) and Hot (software/web). Both are digital locations on a blockchain that allow us to hold cryptographic assets. We are given access to the location in the form of a **private key** (10-20 word seed phrase) and **public address** (0x.....)

Cold wallets provide the best security. They are not connected to the internet, and when a transaction happens (for example sending funds) we must manually press a button on the hardware to confirm it. Cold wallets generate their seedphrase (aka private key) offline, which means it will never touch the internet or be stored in a database. It is only shown once, and can never be retrieved by anyone after the fact.

Hot wallets provide convenience and accessibility, but compromise security. They are great for small everyday transactions, but since they are/were connected to the internet, they present a security risk for large assets. There have been plenty of hacks and hot wallets being stolen, as searchable online. As opposed to a cold wallet, transactions are approved on the device or browser. If the Hot wallet is non-custodial chances are the seedphrase is also not stored somewhere in a server, but still has the possibility of being found. An attacker can they migrate the wallet without knowledge or verification of the owner.

Companies with software/hot wallets spend a LOT of energy on security to prevent such things, but hackers will try everything. **Loopring** sets itself apart from other software wallets in that it uses *Social Guardians* instead of *seed phrases*. This, along with whitelisting addresses (meaning we can only send out so much $$ in any given transaction to pre-specified wallets) makes it more difficult to dump the funds if it were to get hacked. As it will need to essentially be signed by multiple other wallets. This is also a push in the direction of wallet recovery in general.

As you can imagine, having thousands of dollars in a wallet with it's most critical security key being written down on a piece of paper has turned out bad for many many users. Social Guardians is a new tech to allow more ways to recover lost/inaccessible wallets *(1 of many reasons I am so bullish on LRC)*

[Levels of Security](https://preview.redd.it/3cexu9y3hj191.png?width=1500&format;=png&auto;=webp&s;=77fb744c16bdc7abaf7d1ffe7211e1050db64658)

No matter which type of wallet we choose, we need to connect them to websites to start getting the benefits of web3.0. This means we give the website permissions to take a look at our public key and if applicable transact with it.

We can use Cold wallets, with Hot wallet interfaces for maximum security and convenience. For example I have a Trezor hardware wallet that is unplugged. It is connected to MM (using my cold wallet 0x..... address) and I can use that to interact with decentralized apps (dApps) on the web. When I transact, although I am using a hot wallet addon, I still need to physically press a button on my hardware to approve anything. This is how we know it is working and secure. Tedious but secure.

Loopring is technically considered a hot wallet, although features like guardians, the fact it is counterfactual and non-custodial (our phone is the secret phrase, and no one at LRC has access to the data) makes it more like a warm wallet. Social guardians can also be cold wallets that we own and whitelisted for even more security.

Only having a hot wallet as our main bank is not advised in the general crypto community. In the future, fees on L1 and L2 will be much cheaper, and it is generally advised to only send funds to purely hot wallets for the sake of transacting, but not long term hodling.

note It is also not needed or recommended to keep all our assets in a single wallet. Cold or Hot. I have 2 Cold addresses, and 4 Hot addresses on ETH mainnet (using Ethereum blockchain).. Not to mention 4 other coins that require their own wallets/nodes. They are basically free, and having things split up actually improves security.

[examples of dApps](https://preview.redd.it/9n71qprfij191.png?width=1500&format;=png&auto;=webp&s;=10a04141db5f0e0612f9884ed77cf59559a50fd3)

As the ecosystem of web3 protocols grows from finance, banking, exchanges, to games, social media, news.. We will get more comfortable with connecting our wallets to websites. It proves that we own whatever asset are in the wallet (even if it is not being sold/bought. For example a season pass held in the form of an NFT in our wallet can let us in a certain part of a journalist's website). It also gives a way to authenticate who we are, in a semi-anonymous way

#

# Longer reading

Wallets are a critical piece of the crypto puzzle. Thankfully developers (simplified as devs) chose a very practical name for this component.. because a wallet is exactly what you think it is, a place to hold our monies. Digital monies that is, in cryptographic format.

When we use a credit card, or our driver's licensee, or even cash.. we tend to reach into our wallet for these things. Wallets help keep some of our functional gadgets in order and safe. If you ever lost a wallet you know how much of a pain it is to freeze accounts and get everything back. Sometimes it takes weeks, and things like cash and consumables might never make it back. The same way we hold physical wallets as important and highly protected, we should consider crypto wallets.

However with crypto wallets, there is much more at stake to lose. Not even just having it stolen but literally losing access to it. If I lost my bank card, I call my bank and they freeze that number, and ship me a new one. Easy… This however is a fundamental difference: in crypto, **there is no customer support**. The very nature of *'decentralized'* means there is no central agency in control of our funds.

So what does that mean exactly... Why is there a push for decentralization when it seems highly risky? Well as Spiderman taught us, **with great power comes great responsibility**. When there is no customer service, we become our own. When there is no central bank, we become our own… when their is no central authority, *we develop our own autonomy and power*. And that's the ethos

No customer service also means no one can tell us how to spend our money, no withdraw limits, no transfer restrictions etc. So we get certain features as a trade off. Let's get back to wallets. There are basically two types of wallets we should know about as discussed above: a HOT wallet, and a COLD wallet.

Hot and cold are just terms for security. In a hot wallet, our funds are stored on a mobile/browser app. Basically they are stored in a secure way, but on a program or addon that has connection to the internet. A cold wallet stores funds in a device that is not connected to the internet, like a usb drive.

Meta Mask is the most popular form of hot wallet. It is a addon for our web browser that gives us access to a wallet for storage and many DeFi websites. We can send crypto purchased on coinbase for example to our metamask wallet, and then use that to connect and utilize sites like Bancor.

The problem is that because the wallet has direct access to the internet (although again, encrypted and secure via the companies procedures) there is the possibility it can be hacked. Obviously MM's main focus is making their app un-hackable and secure, but this is in general considered an open ended risk. Programmers are smart, and scammers are vast.. so this problem is on going for hot wallets.

A cold wallet on the otherhand is not connected to the internet. It is basically a hyper secure usb stick that we plug in ONLY when we need to transact. Which means there is an air barrier so to speak. *Hackers cannot find something that is not connected to the internet*. Although, someone could confiscate our physical device and attempt a break in, but this is allot less likely… unless your a high profile criminal, then be cautious.

A company like Trezor is regarded as top of the line cold (aka hardware) wallet, and an OG in the space. There is a small screen that asks for confirmation any time crypto is sent out of the wallet, which has to physically be pressed while the device is plugged in (and the associated trezor program is running)

The first step in making a cold or hot wallet will be writing down our **seedphrase**. This is a string of 10-20 randomly generated words that is **THE most important part of owning crypto**.

No one will know this set of words besides us. Once it is generated and shown to us, no one will ever be able to make it appear again, as it was made by a computer that does not store it. This seedphrase we have to take very seriously. Most wallets will even take us through a verification process in which we type parts of the seedphrase back in, to confirm we wrote it down correctly.

And yes… we have to literally write it down on paper! Why you may ask.. in an advanced computer world do we need use the ancient tools of pen and paper. Well imagine this scenario:

Instead of writing the seedphrase down physically we just take a screenshot and save the image on our phone’s library. Easy right? Why waste paper? **Absolutely wrong**. What if we lose our phone, or go on a site that seems legit, or even one we trust gets hacked and someone gets access to our photo library? An attacker could grab that photo and our seedphrase, and recover our entire wallet without our permission or knowledge.

But my phone is super secure you might say.. What if it those photos were backed up to a cloud storage and it slipped our mind, then the cloud gets hacked. We just never know. For the best security, *and this should be considered the immutable standard*.. **we do not want our seedphrase to ever be in digital form**. Not even typed in to print (someone could read deleted files from a hard drive no problem).

People who want to go the extra mile, even store this piece of paper in an indestructible metal tube, or a safe. It is the one single access point to our wallet. Take it very seriously.

With the seedphrase secured and written down manually we can basically forget about it. Our regular transactions will use whats called our **public key**. This is another randomly generated line of code that represents public access to read our wallet and looks like this '0xh9daDHhjha77ad7dabh...' It is also what others can use to send us assets. **Essentially the public key is like our home address or our blog website**, it’s how others can find us. (for bonus points we can assign an ENS address to a public key, which acts like a web domain that points all traffic to it, instead of writing a giant line of code every time).

Now newer protocols like **Loopring** (an OG protocol actually, but some features are new/still in development) have changed the game a bit as mentioned above. They invented **Social Guardians** which brings a new level of security to a software wallet (our phones). They also introduce Layer 2, which basically means we sign a contract (that's why we pay a fee to create one, as opposed to L1 wallets being made for free) that makes a wallet for us inside of their protocol.

It has already been shown elsewhere that although our funds are in a specific layer 2 protocol, we are able to withdraw them if the relayers went haywire at anytime, or there was a bad actor in the organization. This means that LRC does not have access to our funds even though by signing into a layer 2 contract we are 'rolled up' in their protocol. At this time, there is no *general* L2 Rollup protocol, similar to how Ethereum is a general layer 1.

The **Gamestop wallet** is very much like the LRC wallet.. Heck, LRC helped them build it! However *GME decided to use seedphrases instead of social guardians*. They also allow us to connect cold wallets to the back end (provide a 0x... address and seedphrase from offline) for an additional layer of security. Personally I prefer this over Social Guardians at the moment, although I know that tech will make big waves in the future. Both of these wallets will allow access to the NFT marketplace (as well as MM), and you only need one or the other. If we want to make more, that is totally fine. Since the GME wallet is also non-custodial there is literally no advantage to the company by having one. It is only an easy tool provided to satisfy customers who want a complete in-house experience of the marketplaces. If every ape abandoned their current wallet and migrated to gme, literally no benefit to the company (other than perhaps addon downloads and wallet statistics if they use it for marketing to investors).

I would not advise migrating wallets into GME, when we can **easily make new ones** for very cheap (using L2 LRC as activation btw) when gas is low. Migrating is even considered risky from programmer perspectives, and I have heard a few.. Unless we have a gigantic amount of funds in one wallet and do not want to pay transfer fees, but that goes against two principles.. never keep large amounts of assets in a hot wallet, and only use hot wallets for small transactions or trades, not long term storage.

I am sure there are plenty of questions, and I am leaning on the community to help me with that. I have a super busy work-week ahead and hope the graphics really help drive the points home. There are TONS of writings online about all of this, as what I have said here is in no way novel (except maybe the pants metaphor).

I would also advise to test things out. Play around, get familiar with what works and how things work, and why they work. Develop a curiosity for the technology and we will naturally figure everything out. Use some money you don't mind losing. Send some stupid transfers, test test test (and look online before asking every single question in a reddit post please lol)

Really hope this helps everyone. Thanks for the time, and as usual..
Keep Shining out there !
■■■■

\-Helios