Keeping Track of Seeds: Pain Points & A Potentially Groundbreaking Solution

Securely storing crypto seeds is a pain point for crypto users. With Kirobo, many problems can be safely resolved.

[James Howells](http://www.wired.co.uk/article/bitcoin-lost-newport-landfill) could have been a very rich man. In fact, he technically still is. Only he can’t access his money. That’s because his crypto seed, saved on a hard drive accidentally thrown out during a routine cleanup, is buried under roughly 20,000 tons worth of waste. His funds, $750,000 worth of Bitcoin, are lost forever. And guess what? James isn’t alone.

It has been just under a decade since the world was first introduced to the possibility of investing and transacting using cryptocurrency and blockchains. [In this time](https://www.forbes.com/sites/forbestechcouncil/2018/03/14/the-future-of-crypto-in-2018-ripple-and-tron/#325fcf081a18), decentralized exchanges have risen, more and more companies are launching ICOs and individuals are looking to crypto coins and tokens as a highly lucrative, more secure form of financial planning.

# Seeds are the key to your crypto fortune

The chain of crypto custody is secured by [a seed](https://medium.com/%40peterryszkiewicz/secure-cryptocurrency-seeds-fdd99f39df7e), a combination of words or characters used to access your funds stored in cryptocurrency wallets. Each seed is typically long and 100 percent unique, making it very difficult to guess or hack. They are used to generate they keys to sign transactions and access the funds stored in digital wallets at a later date.

Yet, between the risky “[Be Your Own Bank](https://techcrunch.com/2018/02/01/the-sad-state-of-crypto-custody/)” promise inherent in holding cryptocurrency and the struggle to find the right hardware or digital wallet to suit your crypto needs, people have become exceedingly paranoid, stashing their seeds, their singular and unique crypto wallet passcodes, only to forget where they put them, lose them, have them stolen from under their noses or destroyed altogether. Today, [100 billion dollars](https://medium.com/%40alin_82339/the-world-needs-to-catch-up-with-cryptocurrency-ee99191fc853) of cryptocurrency, or 17 percent of the entire crypto market, is lost. Gone, never to be retrieved, because the chain of crypto custody depends solely on seeds – and human preoccupation with safely storing said seeds has led to a preponderance of seed loss.

# Lose your seed; lose your funds

While seeds are the “key” to securing your crypto assets, managing these secret passcodes are at the root of nearly all crypto challenges you most likely have - or will encounter. Lose your seed, fail to pass it on to the right people, or leave it in the wrong hands - and your digital funds will be lost forever.

Even though 24-year-old graduate student Chao Lu of China was capable of remembering all [67,980 digits of pi](http://www.bbc.com/future/story/20150401-whats-the-most-we-can-remember), the average person can only commit a far shorter string of characters to memory. Most people struggle to remember even the most commonly used phone numbers! Since seeds can be long – up to 12-24 words - remembering them in the long-term proves to be extremely difficult, if not impossible, forcing seed holders to resort to other storage methods, such as writing seeds down on paper, saving them on hard drives or in the cloud.

It is your responsibility as crypto wallet users, to hold onto your seed, store it in a safe place and remember where you put it. If you can’t find your seed, or if it was destroyed in a natural (or other kind of) disaster, you won’t be able to call a help-desk, request a new seed or access your cryptocurrency via any other means. This is because seeds are not your standard account password. They are far more secure. There is no restoring or resetting passwords if the need arises. Without a backup of your seed, your funds are gone, perhaps still in existence but beyond the reach of any single being forever. Take the example of [M.,](https://www.wired.com/story/i-forgot-my-pin-an-epic-tale-of-losing-dollar30000-in-bitcoin/) who feared that keeping his Bitcoin keys on a web-based wallet was opening himself to risk of theft. He opted to move them to “a more secure place,” a Trezor hardware wallet, a glorified memory stick, only to lose the PIN granting him access to the Trezor. Stashed in his daughter’s room for safekeeping (without her knowledge - bad move), it was thrown away during a routine house cleaning. $30,000 worth of Bitcoin lost forever. All because M. was scared his seed would be stolen.

In truth, seeds are prone to hacking and theft. With crypto holders turning to a wide variety of methods for storing their seed details for future use, your actual seed can be stolen with relative ease. And once your seed is stolen, it’s only a matter of time before your cryptocurrency is taken as well. This, of course, without any way to track or nab those responsible, thanks to the anonymous nature of the crypto market - an asset for all other transactional activities, but a huge problem when it comes to malicious activity. It is also worthwhile to note that online seed generators are also at risk of being compromised. If this is the case, any future seed generated would be immediately accessible to malicious attackers – and your crypto funds could be easily plundered. This happened to a group of IOTA users this past January, when their wallets were emptied of nearly [$4 million](https://cryptovest.com/news/4m-iota-stolen-from-wallets-which-used-online-seed-generation-websites/) in digital coins, after successfully hacking into an online seed generator and pilfering its secured seeds. This is far from the only incident of real-life robbery of cryptocurrency. [Instances of extortion](https://www.nytimes.com/2018/02/18/technology/virtual-currency-extortion.html) by crypto-robbers happen around the world, from Thailand, to Ukraine, to New York and in between.

And that’s without taking into account any potential technical malfunctions, errors or failures. If a digital connection fails to be made, a bug accidentally triggers some sort of flaw, or some other process does not complete as programmed, inputting the right seed will not grant you access to your crypto funds, even if it’s staring you straight in the face. In one case, a series of bugs led a user to accidentally take control over and lock up over [$300 million worth](https://www.theguardian.com/technology/2017/nov/08/cryptocurrency-300m-dollars-stolen-bug-ether) of crypto funds stored using a digital wallet service. And though he tried to return the money, he ultimately wound up destroying them altogether, through no direct fault of his own. And without a help-desk, there was no way for the crypto’s rightful owners to access their money via any other means.

Malicious and accidental behavior aside, what is perhaps the saddest, most painful problem with seeds is the human paranoia they breed. People are so money hungry, so worried about losing their funds, stashing them away so deep, not even their closest friends or relatives know of their existence – or how to access them. This is particularly unfortunate in the event of the crypto holder’s untimely death. Unless you include your seed in your will, your crypto funds will be inaccessible when you die. There is no third party capable of transferring ownership based on a legal will, unless that third-party was given your seed. Something human paranoia simply will not allow you to do, lest these people attempt to access your crypto funds, before it’s time, lose the seed, or have it stolen from them. You don’t want your money to be lost in crypto space when you’re gone, but you also don’t want to lose it while you’re still alive. Quite an unfortunate conundrum.

# Kirobo - A potentially revolutionary solution for your seed

All is not lost – yet. Kirobo has developed a blockchain solution to tackle as many problems with seeds as possible to prevent loss of crypto, regardless of the cause. Kirobo’s SmartWallet technology allows users to set rules regarding asset holdings and distribution, using backup wallets, daily rule setting and multi-signature division, enabling you to access and transact in crypto like never before.