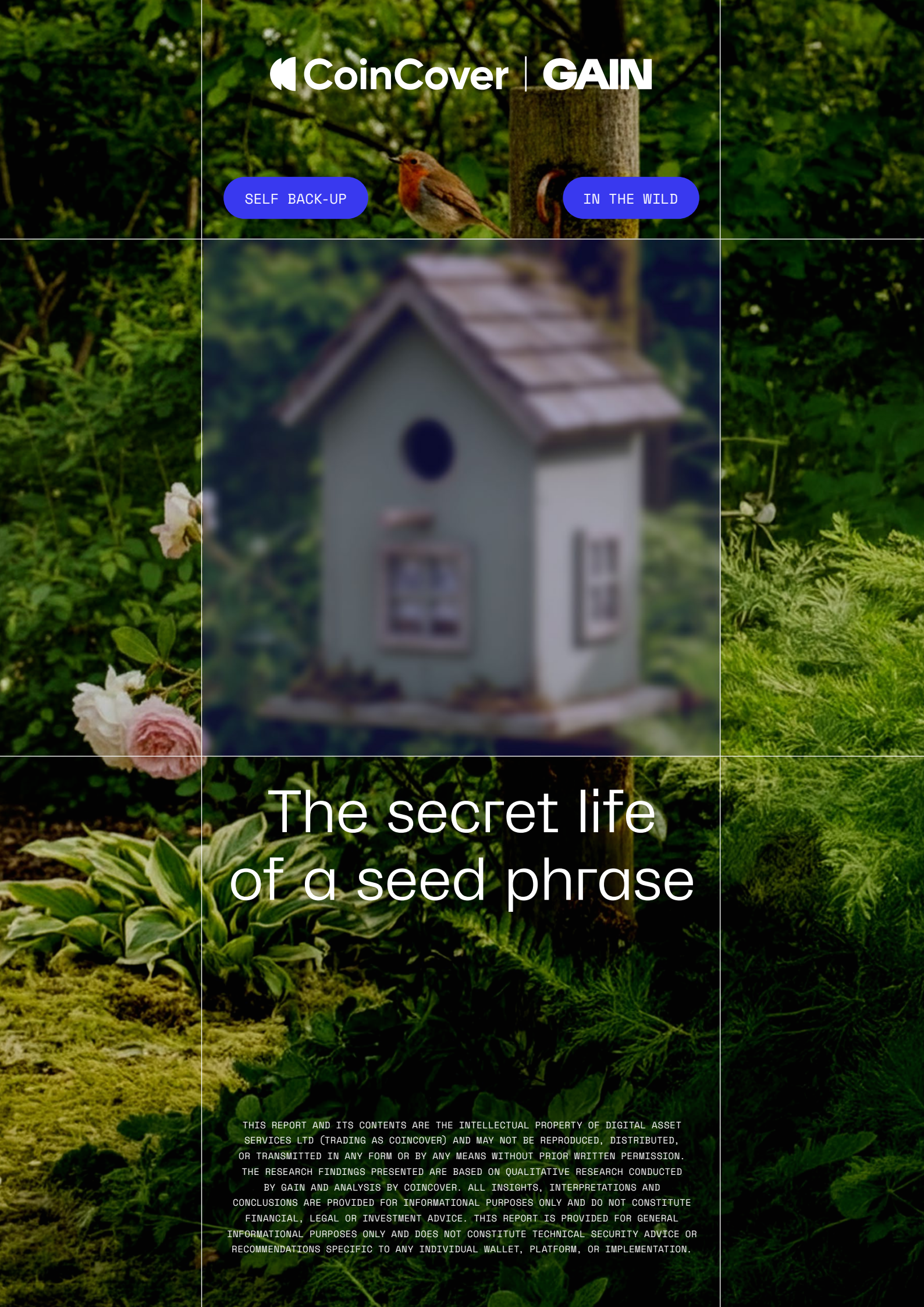


CoinCover | GAIN

SELF BACK-UP

IN THE WILD

The secret life of a seed phrase

Table of contents

Setting the scene 3

Why self-backup breaks in the real world 5

How users really store, hide and recover seed phrases 6

The life of a seed phrase 8

Attitudes to seed phrases 9

Levels of risk in seed phrase management 11

Examples of how people hide seed phrases 12

The absolutists 15

What “keeping them safe” looks like 17

Self-backup in the wild 19

Bridging user behaviour and recovery in crypto 21

OPENING STORY

Setting the scene

On a Friday night, a UK engineer with about £12,000 in various tokens sits at his kitchen table. He knows his seed phrase is his private key to his crypto wallet; he writes it carefully on paper, then copies it into a ‘normal’ notebook he hides behind cookbooks. He feels confident. He’s done the responsible thing.

Six months later, he has no idea where his notebook is. He can't remember whether he left his notebook in his hotel room on his last work trip. That's when he realises that there is no way back in. That £12,000 is irrecoverable.

This opening vignette is just an illustration, but it is built from patterns seen across the research undertaken by CoinCover in collaboration with GAIN: paper backups, hidden household storage, travel-related complexity, and memory-dependent recovery.

SELF BACK-UP

A homemade, hidden, offline security ritual users build around themselves.

EXECUTIVE STATEMENT

Why self-backup breaks in the real world

In crypto, the seed phrase sits at the centre of self-custody. Users understand the slogans, they understand the stakes, and they know that this set of words is the ultimate point of control over their assets.

And yet, when you look closely at how seed phrases are handled, a clear mismatch emerges between what wallet users understand about the importance of seed phrases, and how they are protected in practice.

This research captures the very moment a seed phrase leaves the screen. The moment it stops being a feature and becomes a responsibility, entering the wild, where it is shaped not by systems, but by the people who carry it.

Self-backup in the wild reflects how wallet users care intensely about their crypto, but build personal, invisible architectures around their seed phrases that nobody else can see, test or – ultimately – rescue.

THE RESEARCH

How users really store, hide and recover seed phrases

In December 2025, leading research specialists GAIN were commissioned by CoinCover to understand the life of a seed phrase.

The study focused on wallet users in the UK and US.

During eight 60 minute one to one sessions, participants from the US and the UK, with four participants representing each market, were asked to walk through the full lifecycle of their seed phrase: from the moment it was generated and initially recorded, through to how and where it was stored, hidden, or distributed across locations, and ultimately how they would attempt to recover access if something went wrong.

THE RESULTS

What happens after the seed phrase leaves the screen

THE CONTEXT

The life of a seed phrase

It starts with a phrase.

Typically twelve or twenty-four words, generated in seconds, often written down without much ceremony. But to all self-custodied crypto holders, it is the master secret, the thing that matters most, the line between ownership and loss.

It starts as a simple list of words but quickly becomes something that feels permanent. In the way wallet users talk about it, you can hear the shift from information to responsibility, like something you carry with you indefinitely.

The seed phrase is a string of 24 or 12 random words. You should **never share** your seed phrase. It controls the entire wallet and should never be left exposed or unattended.

USER BEHAVIOURS

Attitudes to seed phrases

01

Learning the hard way

One participant describes getting into Bitcoin early by playing online games and “earning little bits for free”, then repeatedly losing access because they didn’t keep seed phrases or understand wallet hygiene when they were younger.

When asked how they store their seed today, they say they’ve written it down on paper and keep this physical copy at home; they explicitly rejected the idea of screenshots because if someone hacks the phone, they could find the image and take over the wallet.

When imagining losing the seed phrase, their previous response has simply been “start another wallet,” but they note this was only tolerable when the balances were small.

02

Knowing the risk and doing it anyway

One participant knows that storing phrases in unencrypted computer notes is not secure, but justifies it on convenience grounds, and layers on other measures like decoy phrases and Evernote encryption. The resulting system is complex, undocumented and completely reliant on their memory.

Source: GAIN qualitative study

One participant knowingly chooses a less secure method out of pragmatism, opting for something familiar they can recall under pressure, because recovery depends on memory as much as storage.

03

Trying to outsmart the system

One participant describes a colleague who resets his seed phrases every weekend, wiping and re-initialising hardware wallets and moving funds regularly to avoid any long-term exposure.

They understand the intent behind the measures but also sees the risk of “mistakes and misplaced seed phrases with this level of frequent changes.” It’s a good example of how trying to remove risk entirely can actually create more of it.

04

Copies, copies everywhere

Another participant makes copies of parts of their seed phrase and hides each part in a different location in their house.

A multi-copy, multi-location paper system offers redundancy but is still entirely dependent on them remembering where everything is and never mis-labelling a copy.

But copies can drift out of sync. Locations can blur together. A label that made perfect sense at the time can become ambiguous later. And under pressure — when something has actually gone wrong — recalling that entire mental map, without a single error, has now become part of the recovery process.

Source: GAIN qualitative study

THE TRADE-OFFS

Levels of risk in seed phrase management

Users may be highly risk-seeking in markets but extremely risk-averse when it comes to backing up their seed phrase.

“High risk, high convenience” users

One participant describes themselves as “9 out of 10” for overall risk tolerance and behaves like it. They keep seed phrases in unencrypted notes, mix in decoy phrases, and rely on cloud tools like Evernote because they value quick access over strict security. They know it isn’t secure, but accept that trade-off for convenience.

“Selective caution” users

Another participant rates around 7–8/10 on risk in general but draws a much lower-risk line around their crypto. They stick to paper copies of their seed phrase, avoid screenshots, and experiment briefly with more formal storage solutions before deciding they are “too complicated” for day-to-day use.

“Control at all costs” users

A third participant is comfortable taking big investment risks (8–9/10) and uses hardware wallets, decoy phrases and multi-location storage, but dismisses third-party recovery solutions out of hand, stating that no system is 100% secure, even those provided by institutions.

Source: GAIN qualitative study, with interpretation by CoinCover

THE TACTICS

Examples of how people hide seed phrases

When wallet users talk about protecting their seed phrase, the conversation quickly stops being about storage and starts sounding more like a side quest.

GAIN study finding:

One participant, a hardware wallet user, describes making multiple physical copies of the seed phrase and dotting them around so that if one location is lost or destroyed, others still exist.

What starts as sensible redundancy quickly turns into a highly personal scavenger hunt. That participant described backup locations such as a home safe, a parent's house, a friend or cousin's house, and sealed paperwork stored among tax documents.

Published guides on seed phrase storage on bitseedsafe.com and unchained.com show just how inventive these hiding strategies can become.

THE TACTICS

Under the floorboards.

Rolled up inside a curtain rod.

Hidden inside an old clock or behind the battery cover of a wall clock.

Slipped inside obsolete electronics such as old VHS players, radios or other unused devices.

Hidden inside sports equipment such as tennis racket handles or bike handlebars.

Sealed above false ceiling panels or behind decorative tiles.

Buried in a garden shed, potted plant or other outdoor hiding place.

THE TACTICS

At its most inventive, the seed phrase starts to disappear into ordinary life: hidden in objects that look mundane, buried among household clutter, disguised inside filing systems, or folded into places nobody else would think to inspect.

From the user's point of view, this feels smart. From the outside, it looks like the world's least user-friendly treasure map. From the inside, the system becomes more distributed, more personalised and, ultimately, far more dependent on memory than it first appears.

THE OUTLIERS

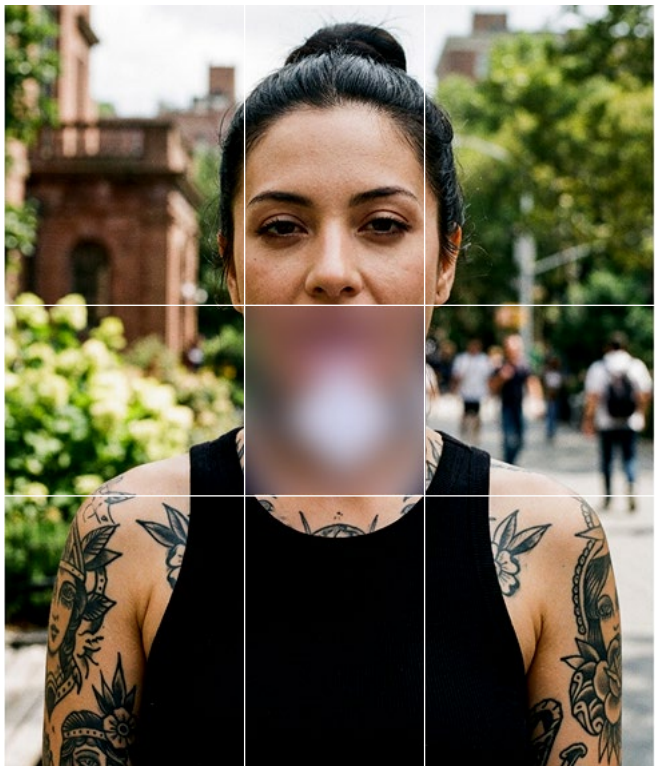
The absolutists

At the far edge of self-backup methods things start to get… intense.

GAIN study finding:

One participant, a highly security-focused hardware-wallet user recalls how they have seen people go as far as tattooing the seed phrase on their body (or an encoded version) in “discreet” places like behind the ear or on the sole of the foot; spreading the phrase across multiple tattoos, with a few words per body part or per person in a trusted group; and even “prison wallet”-style swallowing or bodily hiding of written phrases or metal slivers as an ultra-paranoid smuggling tactic.

Beyond the GAIN study, crypto communities and public discussions on seed phrase storage often push into more elaborate and unconventional territory. These ideas range from encoding phrases into tattoos to splitting them across multiple tattoos, individuals, or physical artifacts to reduce single points of failure. Some concepts even resemble treasure hunt-style setups, where fragments are hidden across different locations and can only be reassembled through a predefined process, blending security with obscurity and, at times, theatricality.



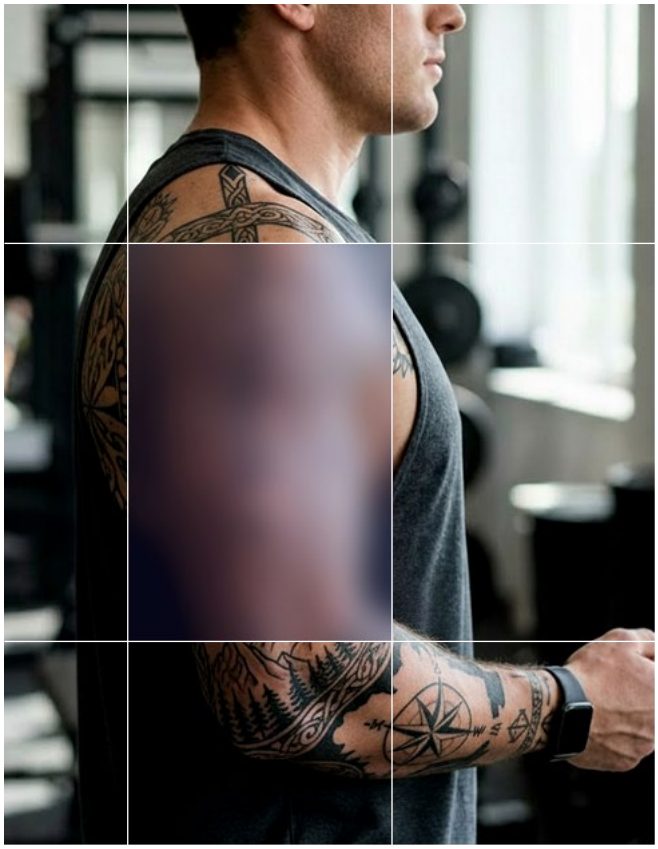
THE OUTLIERS

Body and tattoo tricks

This can involve tattooing the words, or an encoded version, in discreet locations such as behind the ear or on the sole of the foot. Some go further by converting the phrase into small symbols that only the owner can interpret, or by dividing it across multiple tattoos, placing a few words on each limb or even distributing segments among trusted friends and family members.

There are stories of people joking about “prison wallet” hiding tactics or swallowing metal slivers with etched words as a last-resort smuggling play.

It all sounds cinematic, but how exactly do you “rotate” a phrase that lives inside your skin?



Scavenger hunts and world-spread puzzles

Some approaches extend this idea even further, turning seed phrase storage into something resembling a global escape room.

A single word might be hidden in each of several locations around the world, with a map of coordinates secured for heirs, or the phrase could be divided across multiple cities so that each journey adds another word to a new hiding place.

In the most baroque versions, a treasure map is tattooed or encoded on someone else, while the actual phrase waits in a separate secret location. These are fun as puzzle-game concepts, but every new clue, city and co-conspirator multiplies the odds that you never quite put the puzzle back together.

If the seed phrase is everything, these methods try to turn it into legend: part spy movie, part treasure hunt, part body art.

But once the seed phrase lives on the body or is scattered across a world map, the risks become physical and logistical: visibility, coercion, health, border crossings, the reliability of other people and of your future self.

You can’t rotate it easily. You can’t quietly update it after a compromise. You can’t separate it from the stories you’ve told. This is the point where self-backup stops feeling like a security system and starts feeling like a mythology the user has to keep performing.

THE BEHAVIOURS

What “keeping them safe” looks like

As the weight of the seed phrase sinks in, the backup “system” begins to grow. One copy becomes two. One location becomes several. Not in a formal way, but gradually, shaped by habit and perceived threat.

GAIN study finding – baseline practice

Most participants in the GAIN qualitative study described writing their seed phrase on paper and hiding it in one or more locations known only to them, such as under a mattress, inside a particular drawer or among personal documents at home.

EXTERNAL SOURCES

Escalation to creative hiding

Users in the thread describe hiding a full seed phrase on a metal or paper backup inside a concealed wall or bathroom vault that is only accessible via hidden mechanical or remote triggers, ideally in a private room rather than a guest bathroom. Others suggest “hidden in plain sight” approaches such as encoding seed words into poems, pictures, or other everyday objects, so only someone who knows the decoding method can reconstruct the phrase.

Source: BitcoinTalk

Decoys and “spycraft” schemes

Beyond the behaviours observed in the study, external sources describe users layering in decoy phrases, safety deposit boxes, password-protected files and home-made ciphers, as well as more complex steganographic approaches such as invisible or UV-reactive ink, coded notes in books, and other personalised encodings. These techniques can increase perceived security but also introduce significant cognitive and operational risk, because successful recovery depends on one person remembering the exact scheme years later.

Source: ChangeHero

Literary, games and “playful” encodings

Industry commentary and community discussions also reference bookshelf codes, annotated dictionaries or Bibles, game saves, puzzles and other playful encodings of seed phrases. While these approaches may feel engaging or discreet, they share the same structural weakness: they are highly idiosyncratic, hard for others to interpret and rarely tested under stress.

Source: Bitseedsafe

Taken together, the GAIN study and external evidence point to the same conclusion: there is no common standard for self-backup. Most systems are personal, improvised and only lightly documented, which means recoverability ultimately depends on a single individual being present, available and able to reconstruct their own logic at exactly the moment something has gone wrong.

THE CONCLUSION

Self-backup in the wild

As this report has shown, people understand that their seed phrase is everything – "typically a string of 24 or 12 random words" that functions as the ultimate key to their assets – and they know losing it can mean losing everything.

They talk about it in serious, almost reverent terms, insisting that you "don't share your seed phrase… you don't leave it laying around."

At the same time, when asked how they actually back it up, the answers spill into a tangle of improvised rituals: phrases written in multiple notebooks "only I know about," words split across different pieces of paper "hidden around the house," decoy phrases created "just in case someone finds the real one," or seed words stored in obscure digital files and password managers that only make sense to the person who created them.

Across both the GAIN study and external storage guidance, self-backup emerges as a mesh of paper, memory, ad-hoc concealment and half-remembered logic that is highly individualised and rarely stress-tested.

This is what self-backup looks like in the wild.

CONCLUDING REMARKS

What starts as careful protection becomes more difficult to navigate over time.

CLOSING THE GAP

Bridging user behaviour and recovery in crypto

The seed phrase is not misunderstood.

Across the research, wallet users are clear about what it is. They describe it as the thing that controls everything. The line between having access and losing it completely. There is no confusion about the stakes.

However, this understanding does not translate into robust backup behaviour. Instead, most participants described systems built around paper notes, hidden locations, decoys, and memory-dependent routines.

For wallet providers, this disorder has direct commercial consequences. Informal and untested in-house self-backup practices increase the likelihood of access loss, create future support pressure, erode trust in the wallet brand, and reinforce the perception that self-backup remains too fragile for ordinary users.

The findings suggest that users optimise first for familiarity, privacy and personal control, rather than for resilience over time. In practice, what feels sovereign and secure at setup can quickly become difficult to manage, explain or recover from later.

An integrated, non-custodial recovery mechanism that preserves user control can reduce reliance on fragile self-backup practices and improve recoverability.

CoinCover | GAIN

About the authors

Research design and qualitative fieldwork by GAIN. Report framing, analysis and industry context by CoinCover, supported by published external sources on seed phrase storage and backup practice.

About CoinCover

Founded in 2018, CoinCover is the gold standard in digital asset disaster recovery, trusted by over 100 wallets, platforms and institutions worldwide.

Contact CoinCover →

About Gain

GAIN is a leading user research and insight consultancy that helps organisations understand how real people think, decide and behave around complex products and services. They design and run in-depth qualitative studies, turning raw conversations and behaviour into clear, actionable recommendations for product, design and strategy teams.

Contact Gain →

Methodology

This report is based on qualitative one-to-one interviews with self-custodied wallet users in the UK and US, exploring how they generate, store, hide and attempt to recover their seed phrases.

Findings illustrate behavioural patterns rather than providing a statistically representative view of all crypto users, and are supplemented by a review of external published sources on seed phrase storage and backup practices.