A cold wallet can only be an air-gapped wallet

Uncompromised Security

Brussels 19th of May 2023 - Ruben Merre, NGRAVE's CEO & Co-founder

In 2017 and with ETH still in its early days, my co-founder Xavier's previous blockchain project was hacked for 44,000 Ether. A deadly blow to any project. And yet, out of this event, there were two silver linings. First off, it incited a joint effort from Xavier and other developers to set up one of the biggest rescue missions in crypto history, ultimately saving 500 other crypto projects for a cumulative 208M dollars. This event also started a discussion between Xavier, Edouard (NGRAVE's third co-founder) and I, on **"where would we store all our crypto and other digital assets and be able to sleep at night".** That question very quickly led us to one conclusion: the solution did not yet exist and we would have to build it ourselves.

Fast forward to April 2018, we started our NGRAVE journey guided by three fundamental principles and an extreme passion for protecting people. In the fast-paced crypto space, starting on such a long-term endeavor, combining the intricacies of three challenging niches - hardware, maximum security, and crypto - you only embark with a clear mission: **"Empower people to safeguard their wealth so they can live the life they want"**. Here are NGRAVE's three leading principles to achieve that mission:

1. No compromise on users' security.
2. User friendly, intuitive tap and swipe experience.
3. End-to-end security from key generation to seed recovery.

Security does not start nor end with your cold wallet. Security is systemic; it includes managing potential attacks in the supply chain, securely generating keys, seed backup, and a smart recovery process that doesn't expose the user to any third party risk. **At NGRAVE we hold a firm conviction that you should be, at all times, the sole owner of your keys and your crypto.** Our role is to support and protect you in the ownership of your assets. All of what we do is to empower you to "Start Truly Owning What Is Yours".

Highlighting and demonstrating our core values is crucial for NGRAVE. To support our stance, we present four key points that outline our self-custody solution.

1. **Truly air-gapped, AKA 100% offline**

   It is important to highlight a very important distinction between our ZERO cold wallet and most cold wallets on the market: the principle of true air-gapping. As you now may understand in light of recent discussions, **a USB-, Bluetooth-, WiFi-, 4G- or NFC-enabled device comes with the huge risk of being vulnerable to any kind of remote**

attacks. Users are thus vulnerable to hackers but also need to trust that the manufacturer of their device will not exploit this channel.

Hence, the first step should always be to sever that type of connectivity to reduce the risk as much as possible. ZERO is 100% air-gapped and only communicates with the outside world through verifiable QR-codes. It cannot connect to your phone or computer over Bluetooth, Wifi, 4G, NFC nor USB. This means that with ZERO, users create keys, manage accounts and wallets, and sign transactions on a device that is not connected to any network.

2. **Verifiable QR code communication**

Interactions between NGRAVE ZERO and our NGRAVE LIQUID app are enabled through QR-code interactions. Upcoming integrations with Trust Wallet and Metamask will work the same way. Your phone has a camera and a screen, and so does your ZERO, which allows for a smooth experience.

Once you set up your wallet on ZERO, you can scan a QR code on its screen to sync the accounts with the LIQUID app. **Your private keys and seed are never exposed, only the public addresses are shared with LIQUID**. From then on, if the user wants to sign a transaction, you just open the app, fill in the transaction details, show a QR code to your ZERO, sign the transaction request on the device and show a signed QR code back to the LIQUID app to broadcast the transaction to the blockchain.

At every step of the process, you can check the information that is contained in every QR code to ensure that NGRAVE is not sharing information or doing anything else than what we are claiming to do. This allows users to verify exactly what they are signing. When your other cold wallets connect to a computer or phone via USB or other communication technologies, you are basically interacting with a black box, not necessarily knowing what you are actually signing. Putting it all together, QR-codes allow for security through transparency.

3. **The Perfect Key**

Users and cold wallets often forget that true security entails a strong key. After all, if your key is easy to guess, the strongest fortress can’t protect it. When we started working on ZERO, we realized there are many risks in how key generation processes available in the market work. Most hardware wallets today show the key on-screen, and the user has no choice other than to accept it. One of the obvious risks here is that the manufacturer keeps a database of all the keys they ever made. In the light of recent events, this may not be far from the truth.

Moreover, relying entirely on the built-in key generation chip - known as a TRNG- or True Random Number Generation chip - is dangerous as these have been proven to have backdoors. **To counter both threats, ZERO only partly relies on the internal chip's entropy and combines it with external sources of randomness, including biometric data of the user and ambient light, the latter proven as a source of high entropy.** Finally, the user can interact with the key generation process and truly make the key their own, ensuring they are the only one knowing the actual key. In a nutshell:

1. ZERO's TRNG chip generates a first key.
2. Non-chip entropy is added:
    a. Randomness of the user's biometrics, measured by the fingerprint sensor.
    b. Randomness of the ambient light, measured by a built-in light sensor.
3. The user can adapt the key in a gamified way.

This ultimately ensures that only the user sees and knows the final key. No need to trust NGRAVE, nor the chip manufacturer or any other third party.

ZERO is also the only financial product to integrate an EAL7-certified OS to protect your Perfect Key. To prevent physical attacks, ZERO is tamper-proof and will erase any confidential information when sensing a physical attack, powered by its four layers of anti-tampering.

4. End-to-end security & smart recovery

End-to-end security needs to be regarded from a systemic point of view. Your safety encompasses much more than just your hardware wallet. **At NGRAVE, your security starts from the moment you place your order and overarches everything up until smart recovery of your seed if you would lose it.** So when we looked at paper wallets, we understood we had to go beyond. If you can't answer simple questions like "What if you spill water on the backup that holds your wealth?", then you know further innovation is crucial.

This is the reason why we invented our encrypted key backup GRAPHENE. Made of highly durable stainless steel, it resists temperatures way beyond those of a house fire, as well as other extreme circumstances including water floods, corrosion, shocks, and basically anything else.

However, the true power of GRAPHENE lies in its design: it consists of two unique plates, enabling a layer of encryption allowing users to store and safeguard each plate separately and each plate on its own contains no information on your key. Only when both plates are together, the Perfect Key reveals itself. This removes the single point of failure of a paper wallet.

This configuration allows for a unique recovery process. Every upper plate holds a unique recovery ID that users can provide to NGRAVE to reconstruct that plate and send it to the user. There is no risk of NGRAVE retrieving the key as the upper plate alone contains no information about it. For lower plate recovery, most of our users get a second lower plate upon purchase. Alternatively, in the future, it will be possible to assign the lower plate configuration to guardians selected by the user.

NGRAVE builds easy-to-use and secure solutions to allow crypto investors to manage their digital assets as independently as they wish. NGRAVE goes carefully through all the “What if” scenarios to mitigate as much as possible any points of failure and potential attack vectors.

###

Ruben Merre, CEO and Co-founder of NGRAVE, is available for an interview.

About NGRAVE

Founded in 2018, NGRAVE is a digital asset security provider offering user-friendly maximum security solutions for blockchain and crypto use cases. Its flagship product — crypto hardware wallet “NGRAVE ZERO” — is the world’s only financial product with a secure firmware that features the highest security certification: EAL7. NGRAVE is partnered with the world’s top tier in nano- and chip technology, cryptography and hardware security, and counts among its advisors several blockchain pioneers such as Jean-Jacques Quisquater, famous cryptography professor and second reference of the Bitcoin paper.

Resources

- Beyond Mnemonic Phrases: The Path to the NGRAVE Perfect Key
- Are Cryptocurrency Hardware Wallets Safe
- What If NGRAVE Goes Out Of Business?
- NGRAVE’s GRAPHENE is an encrypted and everlasting backup for your private keys

Contact

Email: press@ngrave.io