A Secure End-to-End Solution for the Self-Sovereign Management of Digital Assets

v.0.9 2019 August 21st

Authors: Ruben Merre, Xavier Hendrickx, Edouard Vanham

Executive Summary

Problem: Security is paramount in the management of blockchain enabled crypto assets. Security breaches are continuously in the news and an increasing amount of already billions of dollars is lost or maliciously stolen on a yearly basis.

Cause: The single most important vulnerability in all these crypto hacks is [someone maliciously getting hold of] the private key: the secret access key to a blockchain wallet. If one can keep the private key invisible and out of reach of potential attackers, the private key cannot be stolen, as it is computationally infeasible to brute force it with today's available computing power[1]. However, existing solutions either generate the private key directly online or expose it to an online connection at some point in time. Furthermore, incumbent hardware wallets have several documented vulnerabilities concerning unwanted private key extraction.

Solution: NGRAVE brings to market a novel and breakthrough security solution that, for the first time, evaluates and implements security and usability from an end-to-end perspective. It effectively allows for an A – Z creation and management of one's private key(s) in a complete offline and user friendly manner. NGRAVE's innovation is an integrated three-part solution consisting of:

i) A new generation hardware wallet called the "NGRAVE ZERO", immune to online, remote attack vectors as the hardware device works entirely offline, a characteristic that in industry jargon is also referred to as "air-gapped". The device is capable of communicating in an offline manner through one-way QR codes. Moreover, the ZERO has been built from the ground up in

[1] FIPS 186-4: Digital Signature Standard (DSS) specifies the minimum required key sizes. 256bit for 2030 and beyond as defined by NIST. Available at https://www.keylength.com/en/4/.

close collaboration with world leading experts in chip manufacturing, applied industrial cryptography and hardware security to physically tamper proof the device, taking into account any known attack vectors of existing hardware wallet solutions, as well as novel security risks that have so far not been explicitly documented.

ii) An everlasting, encrypted (private or mnemonic phrase) key back-up solution made of two high-quality stainless steel plates, together called the "NGRAVE GRAPHENE". The innovation of this second product is at least two-fold. It is highly durable and resistant to severe conditions such as high heat situations (e.g. a house fire up to 1660°C / 3020°F), water spills and corrosion, shocks, and more. It is also the first recoverable back-up, meaning that the user can now securely recover a back-up of his back-up. This novelty provides an answer to the question: "what if I lose my key back-up"?

iii) A mobile app, referred to as the "NGRAVE LIQUID". The app can communicate with the hardware wallet via one-way QR codes. As such it can obtain an overview of all the public accounts created on the ZERO, and fetch the related real-time data directly from the blockchain. It can also receive transactions, and initiate transactions which the ZERO can sign in an air-gapped way, offline via QR codes. The mobile app never has any access to secret information such as the private key(s).

Result: NGRAVE's three-part solution is not only the most secure solution available, but also a very intuitive and user friendly, true one-stop shop end-to-end solution for crypto/digital asset owners' secure A – Z management of their private key(s) and hence, their crypto portfolios. Using NGRAVE's solution is one of the most effective ways for the user to protect him/herself from theft and/or loss of the digital assets in his or her possession.

1. Introduction

1.1. Security: One of the Biggest Hurdles towards Widespread Blockchain Adoption

Worldwide blockchain adoption is facing a big hurdle that is only growing in size. In 2018, an estimated $2.5B were maliciously stolen from crypto wallets. In 2019, the problem has only increased in size, with 2019's first two quarters already surpassing a whopping $4.3B[2] (or over $10M on a daily basis). It is clear that if you have cryptocurrencies, you and your portfolio are at risk.

1.2. NGRAVE's Genesis

The NGRAVE movement and solution came about from the NGRAVE founding team's own personal and professional experiences as cryptocurrency investors. There is no better illustration than the background story of NGRAVE's CTO Xavier Hendrickx. Hendrickx has been in the crypto space since early 2013. His conviction of blockchain technology's long term potential made him an early crypto investor. This resulted in him personally becoming a victim in several high-profile hacks, including the Mt. Gox hack in 2014. Even though these events meant considerable blows to his personal crypto portfolio, he kept an unwavering belief in blockchain technology's long-term potential. In parallel with his studies in Computer Science, Hendrickx passionately engaged in developing his own blockchain applications, including a set of automated cryptocurrency trading bots. The latter led to him being "talent-scouted" by a Belgo-American blockchain endeavor named Arkade City, where he became involved as a blockchain developer. In 2016, the project raised 76,000ETH in an ICO. The project rebranded to Swarm City and in 2017, it became one of the most impacted projects by what is today referred to in the industry as the "(Multi-sig) Parity hack". Swarm City lost 44,000ETH in the incident. Hendrickx was one of the first to quickly realize a security breach had occurred. He became involved with a white hat hack group formed to preventively hack other projects in order to protect them (all funds were returned). In just a few hours after the first Parity multi-sig related hacks, around $208M was rendered to safety by this white hat hack group[3][4][5]. Hendrickx' passion to

[2] Source: Q2 2019 Anti-Money Laundering Report, Ciphertrace July 2019, available at https://ciphertrace.com/q2-2019-cryptocurrency-anti-money-laundering-report/

[3] Additional information can be found here: "The Multi-Sig Hack: A Post-Mortem", Parity Technologies July 2017. Available at https://www.parity.io/the-multi-sig-hack-a-postmortem/.

[4] "White Hats Steal Ethereum To 'Save' Users After Hack", IT News.com July 2017. Available at https://www.itnews.com.au/news/ethereum-crypto-currency-in-new-million-dollar-hack-scare-468800.

[5] "How Coders Hacked Back To 'Rescue' $208M In Ethereum", Vice.com July 2017. Available at https://www.vice.com/en_us/article/d3djwj/ethereum-wallet-parity-knew-about-critical-flaw-that-let-user-devops199-lock-up-millions.

protect other crypto investors and blockchain believers from being stolen from or losing their keys became a search for like-minded individuals to set up a project going for ultimate security. When Hendrickx met future NGRAVE co-founders Ruben Merre (CEO) and Edouard Vanham (COO), the genesis of NGRAVE quickly came to realization. Today, the fight for security and convenience is one that the three co-founders passionately engage in, 24/7.

1.3. The "Private Key Paradox"

The root cause of the crypto security problem lies with what is called the private key. This is the secret access key to a blockchain wallet. Practically every crypto hack to this date involves stealing that private key[6]. At NGRAVE, this problem is referred to as the "private key paradox": on the one hand, the private key is the reason why a crypto wallet is so secure - if an attacker only knows the public information (i.e. the associated public address), it is statistically / computationally infeasible to brute force that private key. So the private key is one of the fundaments that makes crypto wallets so secure. However, on the other hand, he who gets his hands on the private key, directly has access to all the funds on the public key (i.e. address) associated with it.

Today's solutions have trouble in keeping the private key sufficiently secure. A good example are crypto exchanges, which generally safekeep the private keys themselves while giving the user a proxy (for example a password in combination with e.g. SMS authentication) to the account, but no actual insight in the private keys. This implies that the user never really owns the crypto on the exchange wallet as he never owns or knows the corresponding private keys. Having crypto exchanges hold the private keys for the user has repeatedly resulted in so-called exit scams or multi-million dollar exchange hacks. The main conclusion is that in order to fully protect your crypto wallet, you need to protect its private key.

1.4. Introducing NGRAVE: An A – Z Solution for Securely Creating, Storing, and Managing Your Private Keys

NGRAVE is a blockchain security company that has developed a complete end-to-end solution to protect your private key(s). The security framework discussed in this document elaborates on and illustrates the rationale for each and every step of managing a crypto wallet (i.e. the private key(s)), and how to render each step of the way crucially more secure than what existing alternatives provide.

---

[6] In some cases, it is sufficient to steal the proxy credentials, for example the login credentials of a user's crypto exchange account. However, the problem can again be reduced to the private key.

1.5. Designed and Developed in Close Collaboration with World Leading Experts

To truly build the best security solutions, NGRAVE has partnered up with two world- & industry leading players. To really address any existing but also non-previously identified technology and security loopholes, NGRAVE built its proprietary security solution(s) together with i) imec: the world leading R&D and innovation hub for nano-electronics, offering a vast expertise in chip manufacturing on nano-scale[7]; and ii) COSIC (KULeuven): a world leading applied cryptography research group renowned for inventing the security encryption protocols adopted by a.o. the US Government and the NSA[8]. In 2001 this group[9] invented AES256 (also known as the "Advanced Encryption Standard" or "Rijndael"), to this day the (so far uncompromised[10]) worldwide standard for data encryption. COSIC is also widely renowned for its involvement in the development of a multitude of cryptographic algorithms, many of which have served as crucial fundaments for blockchain technology protocols. An excerpt of them includes SHA2, SHA3, keccak, breakthroughs in Multi-Party Computation (MPC) and Fully Homomorphic Encryption (FHE), post-quantum cryptography, and more. At the time of writing, the COSIC group also has 2 applications running in the round 2 for the new NIST standard for (post) – quantum cryptography[11].

Imec and COSIC are core partners in the NGRAVE ecosystem and have been heavily involved since the very beginning of the project. At the time of writing, imec also fulfills the function of product development and industrialization partner for the NGRAVE solution, meaning that NGRAVE and imec are jointly finalizing the product design, development, and manufacturing phases.

---

[7] Imec (https://www.imec-int.com/en/home) is a global front runner in Chip manufacturing, Nanoelectronics, CMOS, Image sensors and vision systems, Silicon photonics, GaN, Sensor solutions for IoT, Wireless IoT Communication, Radar sensing systems, Solid state batteries, and data science. It has enormous expertise in building high-tech products that require incredible eye for detail. For example, imec taped out the industry's first atom-scale (3nm) test chip in 2018: https://www.imec-int.com/en/articles/imec-and-cadence-tape-out-industry-s-first-3nm-test-chip

[8] More info can be found at https://www.esat.kuleuven.be/cosic/.

[9] More specifically two professors of the team, named Vincent Rijmen and Johan Daemen (https://en.wikipedia.org/wiki/Advanced_Encryption_Standard).

[10] FIPS 186-4: Digital Signature Standard (DSS) specifies the minimum required key sizes. 256bit for 2030 and beyond as defined by NIST. Available at https://www.keylength.com/en/4/.

[11] The two running COSIC applications are LUOV and SABER, which can be found in the current NIST's Round 2 Submissions for the Post Quantum Cryptography Standard. (https://www.esat.kuleuven.be/cosic/nist-post-quantum-cryptography-round-2-submissions/).

1.6. A Thorough Underlying Security Framework

The NGRAVE team has developed a full security framework covering all the steps to securely manage a crypto wallet, end-to-end. The framework starts with 1) secure wallet generation, continues with 2) secure key safe-keeping, including creating and holding a back-up of your keys; 3) secure wallet management including consulting real-time account balances and history, receiving and signing transactions, and securely updating the relevant firmware; 4) recovery of the key back-up in case the back-up itself would be lost, 5) secure continuity in ownership of all digital assets, e.g. posthumously after the account holder passes away and his or her next of kin need to obtain access to their inheritance; and 6) secure trading.

This document aims to discuss all of these steps in more detail, providing a high level insight into how NGRAVE implements the underlying security requirements, and how existing hardware wallet alternatives and best-in-class crypto exchanges comparatively score on the framework.

1.7. An Upgrade in User Experience

The NGRAVE team has very consciously adopted a methodological, scientific approach where it defines and (in)validates hypotheses regarding specific customer needs, behaviors, and so on. The end user has been included in the ideation, design, and development process from the very beginning of the project and this type of co-creation is considered fundamental to building intuitive and easy to use NGRAVE product(s). This has led to crucial insights for customer-oriented decision making on for example choosing a fingerprint versus a facial recognition authorization factor.

1.8. A True End-to-End Solution: The "What If" Mindset

NGRAVE's end-to-end approach stems from a deliberate and continuous asking of the question "what if?". Just as with asking the "Why" question over and over in process optimization frameworks such as LEAN Six Sigma, where the root cause of a problem can be pinpointed by a technique called the "5 whys", where the question "Why" is repeatedly asked on each answer provided, NGRAVE applies the "what-if?" question rigorously in defining the next step in its product suite. What if I lose my NGRAVE ZERO hardware wallet? What if I lose my NGRAVE GRAPHENE backup solution? What if I cease to exist tomorrow? "What if" is a powerful question when building an A – Z solution. And it is paramount in NGRAVE's approach to problem solving.

2. The NGRAVE Product Suite 1.0

NGRAVE provides both hardware and software security products for securely storing and managing cryptocurrencies and cryptocurrency portfolios. The product suite 1.0 consists of the NGRAVE ZERO, the NGRAVE GRAPHENE, and the NGRAVE LIQUID.

2.1. The NGRAVE ZERO

The NGRAVE ZERO: the first 100% offline, physically tamper proofed and user friendly high-quality touch screen cryptocurrency hardware wallet.

- The ZERO is an offline hardware solution that is able to offline generate the secret access keys ("private keys") and the public keys (the addresses) of a blockchain wallet. This means that the device can for example create a bitcoin wallet without ever having to connect to the bitcoin blockchain to do so.
- The device supports traditional mnemonic phrases such as the 24 word recovery phrase commonly used by existing hardware wallets.
- A new "NGRAVE Perfect Key" is introduced: the 64 character hexadecimal equivalent of the 256 bit master seed. The underlying rationale is that this format allows for a more secure backup and a novel recovery method in case of losing both the hardware device *and* the backup.
- 100% offline means that the device has no network capabilities i.e. no Bluetooth, WiFi, 4G, NFC or other, nor is a USB connection required to generate the private key (or master seed) or to sign transactions. As such, the device is completely "air-gapped" and protected against any online / remote attack vectors. One can visualize an offline "wall" between the device and the internet.
- The device relies on one-way QR codes to securely communicate with the NGRAVE mobile app. QR code technology is used to sync accounts created on the hardware device to the app. For signing signatures, QR code technology is used as well. Crucial is that the secret keys are generated offline and never exposed to an online connection afterwards. This makes the ZERO device incredibly secure as it effectively removes all online attack vectors.
- The device has been built from scratch together with world leading experts to be multi-layered tamper proof against physical attacks as well.

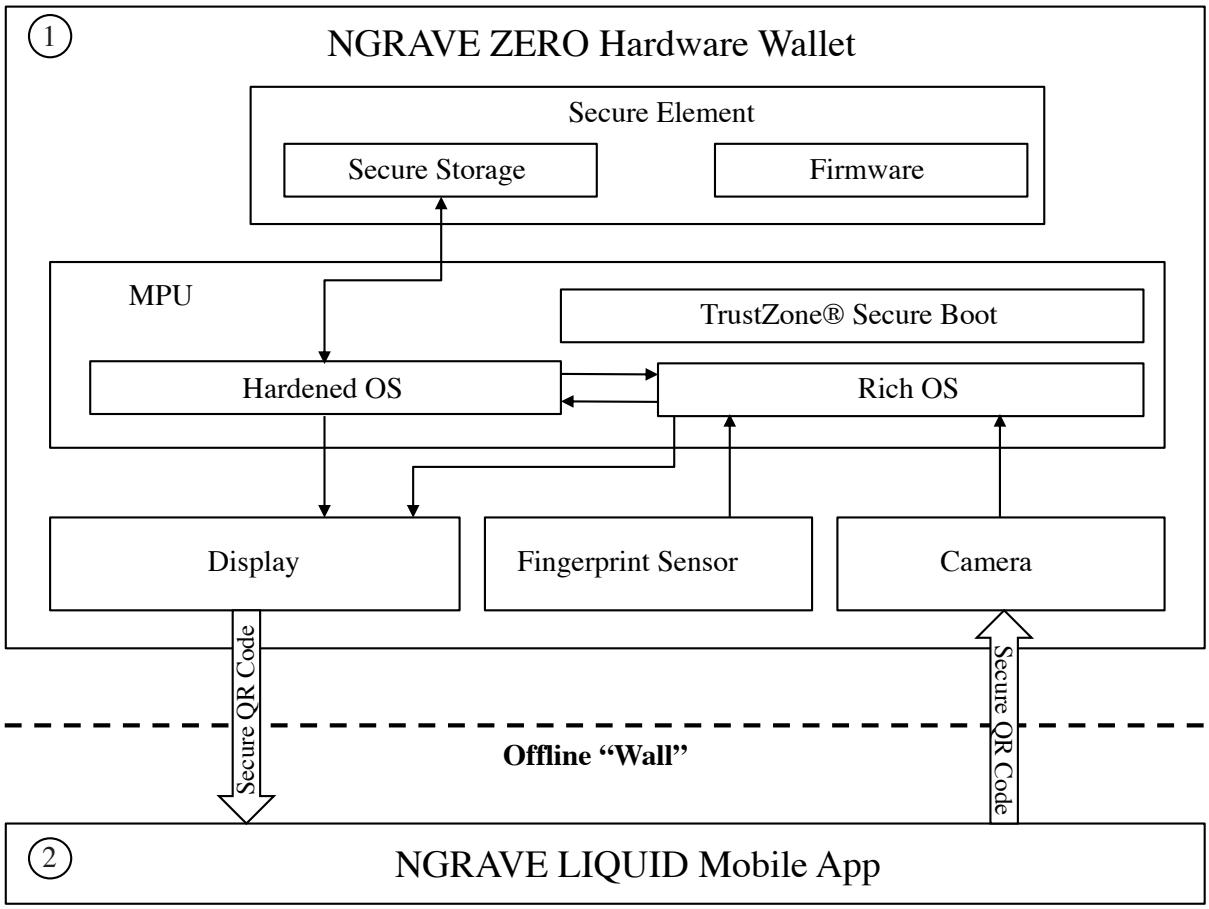

Figure 1: Schematic of (1) NGRAVE ZERO hardware wallet and its interaction with the (2) LIQUID mobile app

2.2. The NGRAVE GRAPHENE

The NGRAVE GRAPHENE: an everlasting backup solution in the form of a cryptographic puzzle, serving as a backup for the secret cryptographic keys created by the ZERO.

- The GRAPHENE consists of two stainless steel plates that replace the need for a paper wallet, the latter being a simple piece of paper currently used by over 90% of cryptocurrency owners to write down their private key or seed phrase. Both plates are resistant to high heat temperatures up to 1660°C (3020°F), water- and corrosion damage, shocks, and more.
- The GRAPHENE allows for engraving the hexadecimal 64 character equivalent of a 24 mnemonic phrase (or 256 bit) master seed. This format allows fully splitting up the key in two parts, as well as for an ingenious recovery mechanism in case the user loses the backup.
- The embossing process takes place by putting both plates exactly on top of each other, and punching holes through the upper plate in the lower plate with an automated click-embossing pen.

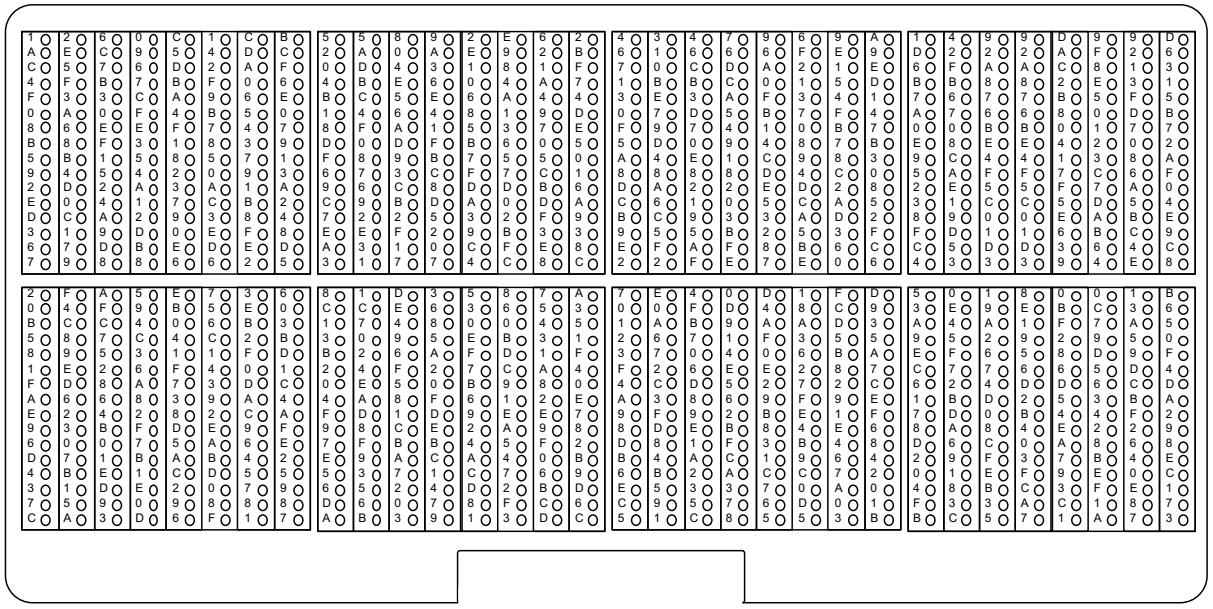

Figure 2: NGRAVE GRAPHENE upper embossing plate with 2x32 columns and 16 holes per character position to allow for hexadecimal master seed notation. Dimensions: 148 x 210 x 1mm (5.8 x 8.3 x 0.5")

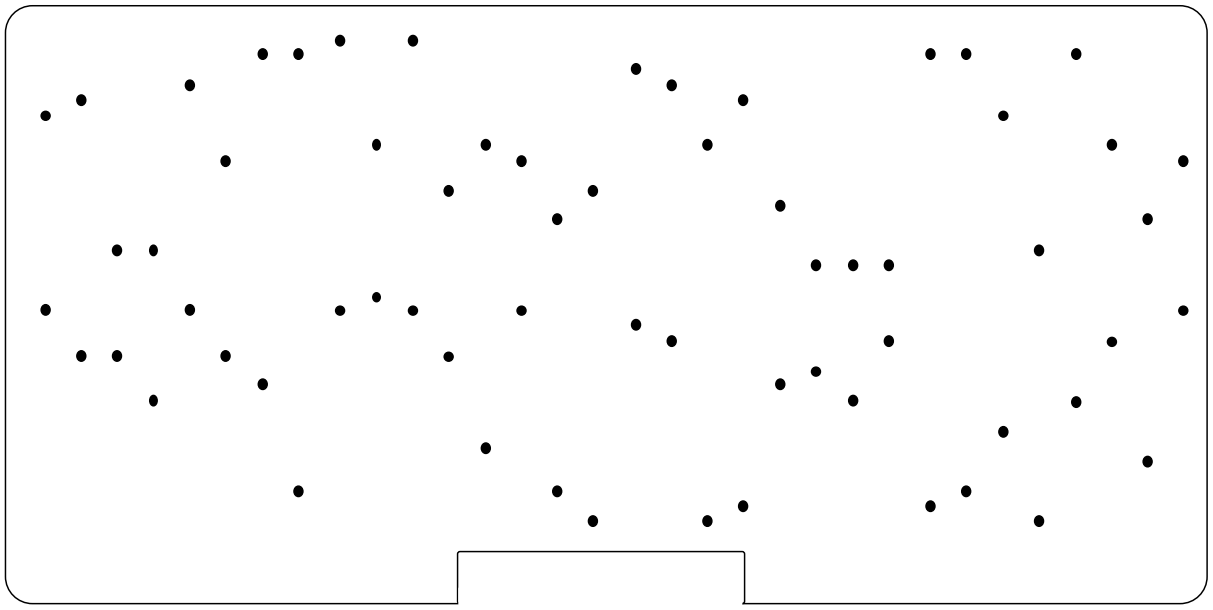

Figure 3: NGRAVE GRAPHENE lower embossing plate post-embossing process, leaving 64 holes that cannot be deciphered without the GRAPHENE upper plate configuration.

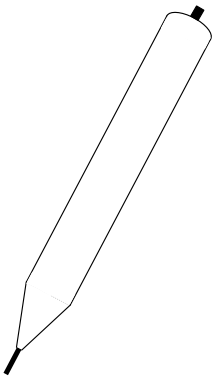

Figure 4: NGRAVE GRAPHENE embossing pen. The pen comes with a click-mechanism that automates the physical power exertion required to "punch" a hole in the lower GRAPHENE plate without damaging the upper one.

2.3. The NGRAVE LIQUID

The NGRAVE LIQUID is NGRAVE's proprietary mobile application for fetching data from and for doing the last-mile communication with the blockchain. The risk of exposing the private keys through the use of the app is fully eliminated as the sensitive data never leaves the ZERO hardware device in the first place. The ZERO can communicate with the app, the app subsequently communicates with the blockchain. Important is that the ZERO never exposes any secret information to the app, and that any communication takes place exclusively through one-way QR codes.

3. The NGRAVE Security Framework

	NGRAVE	Incumbent hardware wallets	Best-in-class exchanges
OVERALL SECURITY	●	◕	◑
END-TO-END SECURITY	●	◔	◔
1. Secure Wallet Generation	●	◕	◑
2. Secure Key Backup	●	◔	◔
3. Secure (same crypto) Wallet Management	●	◕	◑
4. Secure Key Backup Recovery	●	○	◕
5. Secure Posthumous Continuity	●	○	◕
6. Secure (crypto to other crypto) Trading	N/A	N/A	◕

Table 1: NGRAVE's high-level security framework including a comparison to incumbent hardware wallets and best-in-class exchanges. The higher the Harvey ball fill degree, the higher the competitive ranking on relevant sub-criteria. To keep the document concise, new tables will not be named.

NGRAVE has developed its own thorough security framework to which it believes every hardware wallet or broader crypto security solution should assess itself. Based on this framework, NGRAVE's own tear-down reports of multiple crypto hardware wallets and bank security tokens, as well as other relevant available information, NGRAVE decided to build a hardware wallet from the ground up. This may seem like a trivial decision, but it is a crucial one to make. For example, several stripped smartphones turned hardware wallet have been proven to have severe security issues[12].

[12] Two examples include Ellipal and Bitfi, both stripped down Android smartphones. Ellipal has been extensively analyzed and hacked by the Ledger Donjon team (more info available at https://ledger-donjon.github.io/Ellipal-Security/). Deeper analysis on the Bitfi wallet can be found here: https://cybergibbons.com/category/security-2/bitfi/. Some Bitfi attack examples include i) the cold boot attack: the private keys persist in memory for days, allowing their recovery over USB in a few minutes, and ii) the "evil maid" attack: the device can be easily rooted and backdoored over USB in a few minutes, allowing an attacker to receive the user's private keys.

3.1. Secure Wallet Generation

NGRAVE takes current key generation processes several steps further, with the main goal of excluding any possible security loopholes that still exist in today's incumbent solutions. NGRAVE focuses on two important required outcomes here: 1) only the user is allowed to see and know the key, and 2) the key needs to be strong, i.e. statistically unique, unbreakable, and unpredictable for anyone who is not the user. To accomplish this, NGRAVE starts from a fully offline wallet generation process. Whereas this offline character removes any remote attack vectors, the device itself has been built from the ground up to make it physically tamper proof as well. This is important, as there are several recorded cases of so-called "supply chain attacks" where the hardware device is intercepted before it reaches the end customer, and the device is pre-programmed with the attacker's public key[13]. In combination with this offline character, a best-in-class TRNG[14] chip is the basis for the wallet generation process to create a truly statistically unique, unbreakable and unpredictable key. Biometric data (fingerprint of the user) is included in the key generation input process as a salt, together with light sensor measurements. The use of light sensory methods is a proven way of further optimizing and increasing entropy (i.e. randomness)[15]. Finally, a user interaction step has been added as a last step to render any malicious tampering or hacking attacks useless. This last step also assures the user that he and only he has ever had access to and knowledge of the key, and that even the manufacturer – in this case NGRAVE – has no way of knowing what the key is or might be as the difficulty to brute force it becomes too high.

3.1.1: Tamper Resistant

	NGRAVE	Incumbent hardware wallets	Best-in-class exchanges
1.1. Level 1 - Tamper resistant	●	◕	N/A
1.1.1. Outer casing	●	◑	N/A
1.1.2. Inner casing and PCB (incl. Electronic circuitry)	●	◑	N/A
1.1.3. Secure element	●	●	N/A
1.1.4. Firmware	●	●	N/A
1.1.5. Side channel attack resistant	●	◕	N/A

The first level of the NGRAVE multi-layered anti-tampering framework is tamper resistance. This preventive layer is developed to make it extremely difficult to tamper with the different architectural layers of the device. This section will only superficially

[13] An example of such a supply chain attack can be found here: https://saleemrashid.com/2018/03/20/breaking-ledger-security-model/

[14] True Random Number Generation

15 Harvesting Entropy for Random Number Generation for Internet of Things Constrained Devices Using On-board Sensors, Pawlowski, M. P., Jara, A., & Ogorzalek, M. (2015). Available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4634515/

touch upon the specific implementation on each level by NGRAVE, to maintain information asymmetry with any potential attackers.

In making the ZERO device tamper resistant, NGRAVE has focused on making not only a strong metal outer device casing tightly sealed to a tamper proofed screen, but also on implementing precautions at the inner component level. Examples here include a secure element and microcontroller unit with anti-tampering features. On the firmware level, relevant precautions have been added. Finally, side channel attacks are known for their ingenious nature of bypassing the need to brute force private keys. NGRAVE has thoroughly considered related attack vectors and made the device accordingly resistant. For example, the metal casing allows for shielding radio frequencies that could otherwise be picked up by an attacker to pin down and reduce the range of potential private keys.

Incumbent hardware wallets foresee only a minimum of anti-tampering. Either the solutions consider supply chain attacks as out of scope (e.g. Trezor[16]), or they rely primarily on the protection provided by the secure element (e.g. Ledger[17] [18]). There are however multiple proven vulnerabilities due to the lack of such anti-tampering measures[19]. NGRAVE has learned from these documented attacks and has incorporated mitigation at design to protect the device against both known and other identified potential direct tampering attempts. For exchanges this anti-tampering discussion is obviously not applicable.

[16] Trezor considers tamper proofing against supply chain attacks out of scope, as they state on their own blog. To seal up the device they rely primarily on ultrasonic welding and industrial grade glue for the anti-tamper hologram seal on the packaging. They point out that a passphrase is sufficient. Trezor does not have a secure element. More info available at https://blog.trezor.io/our-response-to-ledgers-mitbitcoinexpo-findings-194f1b0a97d4.

[17] Ledger states on its blog that it fully relies on its secure element and therefore does not need other anti-tampering measures such as anti-tamper stickers. More info available at https://support.ledger.com/hc/en-us/articles/360002481534.

[18] Ledger's CTO confirms that the attestation (software and physical) step is sufficient to buy the solution from eBay. Source: https://twitter.com/BTChip/status/949679898012078082.

[19] Examples available at https://saleemrashid.com/2018/03/20/breaking-ledger-security-model/.

3.1.2: Tamper Evident

	NGRAVE	Incumbent hardware wallets	Best-in-class exchanges
1.2. Level 2 - Tamper evident	●	◕	N/A
1.2.1. Physical tamper evidence	●	◑	N/A
1.2.2. Cryptographic attestation process on firmware level	●	●	N/A

On a second level, the ZERO is tamper evident, meaning that even in the event someone successfully breaks open the device, this will be noticeable to the end user. Physical / visual examples include that the device cannot be opened without breaking it. For example, an attempt to remove the screen will cause it to break. Also, the casing is made out of a single metal housing piece, where it is again highly infeasible to open the device without leaving a trace.

When setting up the device for the first time, there also is a "cryptographic attestation" process where the ZERO has to cryptographically sign a challenge received by NGRAVE's servers with a secret key to prove it was originally shipped by NGRAVE. If anything goes wrong or is "hacked" in this step, the device will show up as compromised during initialization by the user. Incumbent hardware wallets typically have the cryptographic attestation process, and/or tamper evident stickers, as already mentioned in section 3.1.1.

3.1.3: Tamper Responsive

	NGRAVE	Incumbent hardware wallets	Best-in-class exchanges
1.3. Level 3 - Tamper responsive	●	○	N/A
1.3.1. Wipe device based on any tampering attempt	●	○	N/A

To make the NGRAVE ZERO even more resilient, it has also been made tamper responsive. This third level ensures that if someone tries to open up the device or attempts to tamper with it, the device will notice this and will wipe itself. This tamper responsiveness is implemented in different layers in the device and a.o. follows the principles of bank security tokens. NGRAVE keeps the exact applied methods and precautions undisclosed to ensure information asymmetry keeps the device and the end user maximally protected. Noteworthy is that incumbent hardware wallets do not engage in tamper responsive protection.

3.1.4: Tamper Resolution

	NGRAVE	Incumbent hardware wallets	Best-in-class exchanges
1.4. Tampering-resolution: post device tampering, the tampering is rendered useless	●	○	○
1.4.1. Offline key generation interaction by the user, making it truly his personal key	●	○	○

Finally, the user can ensure that any tampering that might have occurred is cancelled out by an important interaction step in the key generation process itself. This is a rather unique step that is not implemented in any of the existing hardware wallets. It can be compared to the user modifying a certain number of bits (or characters) in the secret key he receives, thereby introducing a certain level of additional difficulty to break the key for a party that might know the outcome of the key generation process prior to that point. The implementation is somewhat more complex as the user is human and therefore psychologically predictable. NGRAVE developed an interaction process that eliminates this psychological factor and that makes the resulting key very hard to brute force for an attacker that already knew the prior key value. It is a powerful step that provides very high assurance and a last protection layer against any tampering steps earlier in the process. This step prevents being vulnerable to backdoors. And overall, it is one of the characteristics that make NGRAVE stand out as a more secure solution.

The combination of all these anti-tampering layers allows for an unparalleled level of device security. NGRAVE continuously incorporates learnings from existing wallets, adds best industry practices, and the result (as a whole) is yet unseen. Each part on its own is not necessarily ground-breaking, but established security practice. Put together, the solution is however novel and highly secure.

3.1.5: Truly (Statistically) Random and Unpredictable, Unique, Unbreakable Key

	NGRAVE	Incumbent hardware wallets	Best-in-class exchanges
1.5. Truly (statistically) random & unpredictable, unique, unbreakable key	●	◕	◕
1.5.1. Advanced TRNG (True Random Number Generation) chip as a source of entropy	●	●	◕
1.5.2. Additional entropy: biometric data	●	N/A	N/A
1.5.3. Additional entropy: light technology	●	N/A	N/A

NGRAVE uses one of the strongest key generator chips available, certified for TRNG (True Random Number Generation), and CC EAL5+ certified which is on par with or better than the competition or any government or bank deployment. This is a powerful process that allows for unpredictably deriving a totally random secret key, which will

serve as the basis for the user's crypto wallet. NGRAVE has further enhanced and optimized the key generation protocol by including biometric data (fingerprint) and additional environmental data (light sensor), the latter a proven method to increase the quality of entropy[20].

The above process ensures that the NGRAVE key generation process will generate a statistically unique value in the 256-bit range, which sounds easy in theory, but complex in practice. NGRAVE is able to generate a key of which the user has the strongest statistical guarantee that no one else will ever have the same key, and so that there is no collision risk (= the fact that someone else would generate the same key and hence wallet access). The actual statistical risk is 1 out of 115,792,089,237,316,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000 ,000,000,000,000 or 1 out of 10^{78}or 1 out of 2^{256}, which is a number comparable to the total number of atoms in the universe. Again, the existing TRNG chips are in principle good enough for this.

The uniqueness of the key shows the number of values a supercomputer would have to try to break the key. It is statistically near-impossible to brute force the key. It is statistically unbreakable with today's available computational methods.

3.1.6: Offline Key Generation

	NGRAVE	Incumbent hardware wallets	Best-in-class exchanges
1.6. Offline generated	●	◕	○
1.6.1. No USB	●	○	N/A
1.6.2. No connection to connected device	●	○	○
1.6.3. No connection to Bluetooth	●	○	○
1.6.4. No connection to wifi	●	●	○
1.6.5. No connection to 4G	●	●	○
1.6.6. Completely air-gapped	●	○	○

The NGRAVE hardware wallet is a standalone network-disabled device that does the entire wallet generation process offline: no USB connection nor any network connection is relied upon at any point. The key can never be found by a hacker as the key never touches the internet, rendering the attack surface near-zero, unlike for example online generated keys. This is a differentiator compared to existing USB- or Bluetooth based hardware wallets. In the case of online wallets or exchange accounts, the entire generation process occurs fully online, putting the key generation and hence the key itself at significant risk.

[20] Harvesting Entropy for Random Number Generation for Internet of Things Constrained Devices Using On-board Sensors, Pawlowski, M. P., Jara, A., & Ogorzalek, M. (2015). Available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4634515/

3.1.7: User's Eyes Only Principle

	NGRAVE	Incumbent hardware wallets	Best-in-class exchanges
1.7. User's eyes only principle	●	○	○
1.7.1. Key is not just provided as a fact, but user takes part in the generation process	●	○	○

To take the key generation process one step further, NGRAVE involves the user himself to ensure that not even a third party (not even NGRAVE) has a way of knowing what the key is or could be. This is crucial. Imagine the key would be generated offline with all the previous steps in mind, and the user would simply receive the key as a fact. Who is to say that the company that made the process doesn't just keep a database of all keys it ever distributed, fooling the user in believing nobody can know his key. The user's eyes only principle means that i) the key is generated in a way that he and only he can see it (see section 1.6.), AND that the user is able to modify the key (see section 1.5) in a certain way so that he can rest assured that even NGRAVE has no feasible computational way of knowing what key the user actually generated.

3.2. Secure key safekeeping

NGRAVE solves one of the significant drawbacks currently associated with crypto wallets: making and storing a backup of a secret key. Incumbents either provide a paper wallet solution[21] or a single-point-of-failure steel solution to back-up the private key or master seed. Even if the solution is very durable, if it is found by an attacker, the key can be stolen. NGRAVE has invented a cryptographic puzzle solution consisting of two everlasting durable and resilient stainless steel plates that can be stored separate from each other. Crucial is that both plates are agnostic, meaning that if someone finds one of these plates, he has no information whatsoever on the actual private key or master seed and still needs to brute force the full key.

3.2.1. Only the owner should have access to and/or own the key

	NGRAVE	Incumbent hardware wallets	Best-in-class exchanges
2.1. Only owner owns the key	●	◕	○

A very crucial part in crypto security is who actually owns the keys. At first glance, this seems a simple and logical idea, yet all crypto exchanges today are the ones who own the user's private keys. The user merely receive a password and an optional two factor authentication code. He receives the account addresses from and to which he can send cryptocurrencies. At no point is he the real and sole owner of the private keys. He merely receives a proxy account. The exchanges have all the private keys. This is one of the biggest downsides of centralized exchanges. Small ones can do (and several of them have done) an exit scam and leave with all their users' funds overnight. Larger ones can get hacked, good examples include the recent 2019 7,000BTC Binance hack, and Cryptopia going bankrupt post-hacking incidents. The exit scam of 246,000 users large Irish exchange Bitsane in 2019 is a good example of a recent exit scam at the time of writing. Decentralized exchanges can provide an answer to this and could be an interesting growth catalyst for hardware wallet demand[22]. Unlike with exchanges, NGRAVE generates the secret key following the principles in section 3.1, thus the user is the only one who sees the key and therefore truly the only owner. Even NGRAVE has absolutely no computationally feasible way of knowing the user's secret key. This is a crucial starting point from which the user can set up a key backup. The GRAPHENE keeps following the principle of the owner being the only one to know the key.

[21] For example, Ledger and Trezor hardware wallets come with a paper sheet to write down the 12/18/24 word mnemonic phrase to recover the secret key in case of loss of the hardware wallet.
[22] See section 3.6. Secure Trading

3.2.2: Key split principle

	NGRAVE	Incumbent hardware wallets	Best-in-class exchanges
2.2. No single point of failure	●	○	◔
2.2.1. Split-key principle: key is split in two parts that can be kept separately	●	○	◔

NGRAVE introduces the "NGRAVE Perfect Key": the 64 character hexadecimal equivalent of the 256 bit (or 24 word mnemonic) master seed. The underlying rationale is that this format allows for a more secure backup. The NGRAVE GRAPHENE is a key back-up solution that splits the 64 hexadecimal perfect key onto two everlasting stainless steel plates.

- The upper plate consists of 2 rows of each 32 columns, with each row split in 4 boxes of eight columns. Every column represents one character of the secret key for in total 64 positions. Each character can have one out of 16 values (0 - 9 and A - F (hexademical format)). For each column, the values are randomly scrambled. Therefore, each upper plate is as unique as there are private keys (i.e. there are 10^{78} possible upper plate configurations). Next to each value there is a hole in the plate, so there are 1024 (or 2^{10}) holes in the upper plate.
- The lower plate is a clean stainless steel metal plate.
- The user can "punch" holes in the lower plate by placing the upper plate exactly on top of it, and wielding the automated NGRAVE embossing click-pen. The user doesn't have to exert any physical power, he simply needs to click the embossing pen which then exercises the exact required physical power to make a hole in the lower plate at the right position for each value of the secret key.
- Eventually, the upper plate will still be completely clean, i.e. it remains untouched after the embossing process. The lower plate will have holes. In this way, the key is actually split in two parts, instead of one. The fact that the solution is split in two parts overcomes the single-point-of-failure problem current solutions have and where, when the storage medium is found, the attacker has all the information he needs. Splitting the mnemonic version (the 12 - 18 - 24 words version) isn't best practice, as the user would lose half the security. This is why the NGRAVE back-up relies on the hexadecimal version.

3.2.3: Agnostic parts (One part = no part)

	NGRAVE	Incumbent hardware wallets	Best-in-class exchanges
2.3. Agnostic parts (one part = no part)	●	○	◔
2.3.1. One recovered part provides zero information on the full key	●	○	◔

The GRAPHENE solution has the peculiar characteristic that if someone finds one of the GRAPHENE plates, he has as much information as someone who has no part at all, as each plate by itself is useless for deriving the key without its counterpart. An attacker that finds only one of both plates still needs to brute force the entire key. This is something that would not be possible when a 24 word phrase would be split in two. Finally, each plate has a vast amount of unique possible configurations, with both the number of unique upper plate configurations AND the number of unique lower plate configurations each at 10^{78}.

3.2.4: (Quasi)-indestructible / "everlasting"

	NGRAVE	Incumbent hardware wallets	Best-in-class exchanges
2.4. Quasi - indestructible	●	○	○
2.4.1. Water- & corrosion -proof key backup	●	○	○
2.4.2. Fire-proof key backup	●	○	○
2.4.3. Buried-proof key backup	●	○	○
2.4.4. Shock-proof key backup	●	○	○

Whereas a traditional "paper wallet" might already be destroyed after a simple, small, water spill, the GRAPHENE plates are made of highly resilient, quasi-indestructible material: stainles steel. These plates are heat resistant up to 1660°C (3020°F). They are water-, corrosion-, shock-, and buried proof.

3.3. Secure (same crypto) wallet management

NGRAVE offers a fully air-gapped, 100% offline hardware wallet that comes with secure access management. Together with the app and tailored QR-code technology, it has effectively created a method through which accounts can be synced, account balances and past transactions can be consulted in real time, incoming transactions can be requested and received, and outgoing transactions can be initiated and securely signed. Private keys are never exposed to a connected device or an online connection and are kept on the ZERO at all times (with an optional GRAPHENE backup). Existing hardware wallets generally rely on USB or Bluetooth for e.g. syncing accounts or signing transactions. Whereas these solutions are considered secure, there does remain an inherent associated risk, albeit small. An extreme example is the Stuxnet virus that is widely believed to be responsible for causing substantial damage to Iran's nuclear program[23]. This virus spread unnoticed via infected USB flash drives, effectively circumventing "air-gapped" USBs. It remained dormant inside most computers, but when the conditions were fulfilled, it introduced an infected rootkit onto the relevant PLC and Step7 software. Finally, exchanges are inherently online, resulting in a multitude of risks as already discussed thoroughly throughout this document.

3.3.1. Secure Wallet Access

	NGRAVE	Incumbent hardware wallets	Best-in-class exchanges
3.1. Secure wallet access	●	◕	◑
3.1.1. Access real-time account data without private key exposure	●	◕	N/A
3.1.2. Two-factor authentication	●	◕	◕
3.1.3. Hardware wallet scrambled PIN-pad	●	●	N/A
3.1.4. Hardware wallet biometric access	●	○	N/A
3.1.5. Only the user has ownership of the account(s)	●	◕	○

Whereas existing hardware wallets rely mostly on the PIN code, NGRAVE introduces two-factor authentication access management for its hardware wallet, consisting of a fingerprint reading and a PIN-code validation that triggers a wiping of the device in case of multiple subsequent error attempts. The PIN has to be a number of minimum 4 and maximum 8 characters. All input values are scrambled on the screen to prevent vulnerabilities from side channel attacks targeting the PIN code.

[23] Stuxnet reportedly ruined almost one fifth of Iran's nuclear centrifuges. Source: "The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought", Business Insider 2013 (available at: https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11?r=US&IR=T).

Exchanges and other online solutions are improving when it comes to multi-factor authentication but keep having considerable attack surface. Also, as they own the private keys, these are exposed. Also, the user does not have real ownership of his accounts and is merely an account proxy.

3.3.2: Consult Account

	NGRAVE	Incumbent hardware wallets	Best-in-class exchanges
3.2. Secure public accounts export / syncing without secret cryptographic key exposure	●	◕	◑
3.2.1. Secure accounts export without USB	●	○	N/A
3.2.2. Secure accounts export without connection to connected device	●	○	◔
3.2.3. Secure accounts export without Bluetooth	●	○	◔
3.2.4. Secure accounts export without wifi	●	●	◔
3.2.5. Secure accounts export without 4G	●	●	◔
3.2.6. Completely airgapped secure accounts export	●	○	○

The NGRAVE ZERO hardware wallet interacts with the LIQUID app through QR codes. The user can set up his accounts offline on the ZERO by selecting the coins he wants in his portfolio. He can add more accounts whenever he wants (for example more accounts of the same cryptocurrency, active new ones that are already supported by the ZERO, or include new ones when there is a firmware update including the support of new coins). The user can securely sync these offline generated accounts to the mobile app by exporting them via one or more QR codes generated by the ZERO. Private keys remain offline, so the user remains the sole proprietor of the accounts. Based on the public data the app fetches from the blockchain, the user can then access the real-time status of his account balances and transaction history. As mentioned in the introduction of section 3.3, incumbent USB or Bluetooth solutions still have proven vulnerabilities, and the experience remains inherently online.

3.3.3: Receive transactions

	NGRAVE	Incumbent hardware wallets	Best-in-class exchanges
3.3. Secure receive transactions without secret key exposure	●	◕	◑
3.3.1. No secret cryptographic key exposure	●	◕	◑

If the user wants to receive transactions, he or she has to share his/her public address / public key with the party that should do the transaction. As he or she only shares this public information – no private key – there is no statistical risk.

3.3.4: Secure transaction signing

	NGRAVE	Incumbent hardware wallets	Best-in-class exchanges
3.4. Secure signing of transactions	●	◕	◑
3.4.1. Secure transaction signing without USB	●	○	●
3.4.2. Secure transaction signing without connection to connected device	●	○	○
3.4.3. Secure transaction signing without Bluetooth	●	○	●
3.4.4. Secure transaction signing without wifi	●	●	◑
3.4.5. Secure transaction signing without 4G	●	●	◑
3.4.6. Completely airgapped secure transaction signing	●	○	○

To sign and execute an outgoing transaction, the user initiates the transaction on the mobile app where he inputs the from- and to-account, the amount of crypto to send, and an optional gas limit. This unsigned transaction object is then encoded into a QR code. The user scans this QR code with the NGRAVE ZERO's built-in camera. The NGRAVE ZERO decodes and displays the transaction data on its screen so that the user can verify what the QR code contains. This is a crucial verification step as the mobile app is online and therefore a potential surface for attack. By correctly verifying the QR code content however, a mobile hack is infeasible as the user will not sign a non-valid transaction that he does not want to make. By fingerprint and PIN-code two-factor authorization, the user can unlock the relevant private key to cryptographically sign the transaction. The ZERO then encodes the transaction signature into a QR code. Due to the cryptographic nature, this QR code contains no information that can lead back to the private key. Hence, the secret key remains fully offline and protected. The user can then scan the QR code on the NGRAVE ZERO with his mobile app. The app now has a valid transaction signature it can send to the blockchain. The blockchain will not accept any other signatures than the valid one, so no fake or corrupt transactions can take place without the user's consent.

3.3.5. Secure firmware updates

	NGRAVE	Incumbent hardware wallets	Best-in-class exchanges
3.5. Secure firmware updates	●	◕	N/A
3.5.1. Verification of Trusted Origin for firmware updates	●	●	N/A
3.5.2. Physical disabling of firmware manipulation via chip	●	●	N/A
3.5.3. Secure and encrypted bootloader code	●	●	N/A
3.5.4. Unsafe update detection and warning	●	●	N/A
3.5.5. Chip Access prevention via tamper-resistance	●	◕	N/A

Firmware updates are being transmitted over USB. The ZERO will boot in a separate, empty partition specifically for the purpose of receiving the new firmware. The new firmware will have been cryptographically signed by NGRAVE's secret keys. A new boot will load the Integrity Verifier, contained in the ARM®TrustZone® module. The purpose of this module will be to check at boot time and regularly that the NGRAVE software stack side of the platform is free from unintended modifications or alien tasks running. For firmware updates, the new firmware will be verified as it is received on the isolated partition. This way there is total separation between the update process while connected over USB (receiving the new package) and any software actually running the device. The same Integrity Verifier used to verify the new firmware package will also run at every boot and regularly thereafter to verify that solely the intended software is running unmodified, no alien tasks are running and the platform has not been tampered with otherwise, thus solving both security concerns of authenticity and integrity.

To prevent any possibility of flashing the chip directly with malicious firmware, any debugger access has been disabled. Even if the chip were exposed, there would be no way to modify the currently loaded firmware. Since the bootloader will be responsible for verification of the firmware, it has to be impossible to modify the bootloader. This security is achieved by locking that part of the chip from write access, encrypting its contents and employing the basic hardware and firmware authenticity protections provided by the MPU's TrustZone® module. Any attempt to access the chip in any other way will trigger the tamper responsive mechanisms in place to wipe the stored secrets.

3.4. Secure Key Recovery

An important part where most crypto security solutions are lacking is the possibility to securely recover the key, not only from the backup, but also in the event of losing the backup itself. NGRAVE introduces a solution that resolves these drawbacks.

3.4.1. Possibility to Recover Part of the Key for the User

	NGRAVE	Incumbent hardware wallets	Best-in-class exchanges
4. Secure key recovery	●	○	◕
4.1. Possibility to recover part of the key for the user	●	○	◕

NGRAVE is able to recover one of the two NGRAVE GRAPHENE backup plates, more precisely the upper plate. As this is the most expensive of the two plates, it is recommended that the user purchases two or more lower plates that he can store safely. This is a minimum cost increase on the user's side, as he now has two physical lower plates for which he can always recover the upper plate.

The cryptographic puzzle "key split" principle as explained in section 3.2 ensures that if anyone finds any of the two plates but not both, there is no way of divining the actual private key or master seed protected by them.

How the recovery works: when a customer orders an NGRAVE GRAPHENE (or the bundle with the hardware wallet), he has 3 options:

1) Default option: NGRAVE adds an order number to the package it sends to the user, and the user can at a later time recover the upper plate configuration either by typing in the order number on a dedicated NGRAVE server, or directly via a blockchain interface, the latter being the more decentralized option;

2) Personalized option: the user can provide additional KYC data, based on which he can identify himself with the NGRAVE team when he wants to recover his upper plate. He can call NGRAVE customer support who keeps offline records of which order numbers and hence which upper plate configuration(s) are linked to a specific customer;

3) Right to be forgotten option: the user can also ask to be forgotten, i.e. that NGRAVE does not store the order number. This entails that the user cannot ask NGRAVE for a recovery of the upper plate.

3.4.2. No (statistical risk of) malicious 3rd party recovery

	NGRAVE	Incumbent hardware wallets	Best-in-class exchanges
4. Secure key recovery	●	○	◕
4.1. Possibility to recover part of the key for the user	●	○	◕

NGRAVE has designed the key back-up recovery such that no 3rd party, not even NGRAVE, can guess or compute the value of the key, as long as the two parts are not both available. Hence, it is always required to have access to the lower plate, which in principle (and recommended) is kept away physically from its upper counterpart. Unless the user would make pictures of it and store these somewhere online, physical acces to the lower plate is required to reconstruct the key.

As such, even if the whole database of upper plate configurations would be hacked, the user's keys would not be at risk. Moreover, if a hacker would simply delete all data, there will always be a back-up server. Also, if the implementation occurs directly on the blockchain, the data is in principle immutable. Note that a similar solution invented by any of the existing alternatives currently does not exist.

3.5. Continuity

3.5.1: Posthumous continuity: wallet credentials can be disclosed to the owner's next of kin

	NGRAVE	Incumbent hardware wallets	Best-in-class exchanges
5. Continuity	●	○	◕
5.1. Posthumous continuity: wallet credentials can be disclosed to next of kin	●	○	◕

Without elaborating too much on this yet, it is possible to disclose the locations of the upper and lower plate to separate heirs. For example, the respective locations of the plates could be stipulated in a will, managed either by a traditional notary, a blockchain notary system (e.g. upon death certificate, the blockchain can release the locations), or otherwise. It could also be automated, for example by sending notifications to the user if he or she has been inactive on the app for a specific period of time and reminder notifications are also not responded to. These events could then trigger additional smart contract logic communicating the location of the plates. Posthumous recovery will be covered more in-depth in later versions of the white paper.

3.5.2. No third party risk

	NGRAVE	Incumbent hardware wallets	Best-in-class exchanges
5. Continuity	●	○	◕
5.2. No third party risk	●	○	◕

It is again crucial that there should not be any third party risk, which is why a physical notary would be advised against in the most decentralized case. The blockchain can provide solutions here. Again, posthumous recovery will be covered more in-depth in later versions of the white paper.

3.6. Secure (crypto to other crypto) trading

	NGRAVE	Incumbent hardware wallets	Best-in-class exchanges
6. Secure (crypto to other crypto) trading	N/A	N/A	◕

The advent of decentralized exchanges allow users to interact directly with market orders, without the need to trust a central host to manage their keys. Hardware wallets can play a crucial role in security and ease-of-use, and NGRAVE is uniquely positioned with its use of QR codes and their ease of implementation. It is NGRAVE's clear intention to develop safe and user friendly integrations for a variety of decentralized

exchanges and for a wide range of crypto protocols. This will be elaborated more in a later version of this white paper

4. User Experience

	NGRAVE	Incumbent hardware wallets	Best-in-class exchanges
OVERALL USER EXPERIENCE	●	◑	●
1. Screen	●	◔	●
1.1.1. Screen size	4 inch colour high pixel density	< 2inch low pixel density	Full desktop / mobile
1.2.1. Touch screen	Yes	No	N/A
2. Ease of use	●	◑	●
2.1. Set-up	●	◑	●
2.1.1. Create wallet instantly, no additional connection required	YES	No	YES
2.1.2. Total time to set up / initialize	< 5 min	10 - 20 min	< 5 min
2.2. Ease of use in general	●	◕	●
2.2.1.. No need to set up connection to start using	YES	No	N/A
2.2.2. Offline experience, so no need to feel unsafe (if online connection established, experience is inherently online and perceived less safe)	YES	No	No
2.1.3. Easy visual toggling through accounts	YES	Easy on mobile, less so on device	YES
2.1.4. Strong mobile app experience	●	●	●

Customer centricity is a fundamental pillar of NGRAVE's product philosophy. Every device interaction has been designed and developed in co-creation with the end user and has been methodologically tested and validated in deep dive one-on-one interviews and larger scale quantitative validation sessions.

The result for the NGRAVE ZERO is a pocket-size high pixel density 4 inch diagonal capacitive touch screen device that provides increased convenience compared to incumbent's smaller device screens. Moreover, device set-up and overall management requires considerably less time and takes place completely offline, removing the perception for the user of interacting with a connected medium and therefore an online attack vector.

The NGRAVE GRAPHENE is an intuitive, very understandable and easy to use backup and (backup) recovery mechanism. It does not require relatively complex (and often expensive) governance structures such as the inclusion of 3rd party multi-factor schemes for key recovery. It is also deliberately non-electronic, as electronics degrade over time, which would therefore be a risk. The NGRAVE GRAPHENE is simple by principle, yet extremely powerful in its application.

5. Conclusion – Summary of Key Takeaways

Security is a real issue and hurdle for gaining widespread blockchain adoption. In 2018, $2.5B were stolen from crypto wallets. The first half of 2019 netted $4.3B. The root cause lies with the management and safekeeping of the private key, the access key to a blockchain wallet. The private key makes the security of a crypto wallet statistically unbreakable. However, this security ends as soon as the key is lost or exposed to a third party. This makes the private key also the Achilles heel of a blockchain wallet. NGRAVE refers to this contradictory characteristic as the "Private Key Paradox".

NGRAVE brings to market a novel and breakthrough three-part security solution that, for the first time, evaluates and implements security and usability from an end-to-end perspective. It effectively allows for an A – Z creation and management of one's private key(s) in a complete offline and user friendly manner, thereby never exposing the private keys and providing a valid resolution to the "Private Key Paradox".

NGRAVE's innovation consists of a secure hardware wallet called the NGRAVE ZERO, a secure key backup solution called the NGRAVE GRAPHENE, and a mobile app called the NGRAVE LIQUID. NGRAVE has designed and developed its security system from the ground up and in close collaboration with world leading experts to not only eliminate vulnerabilities of existing hardware wallet solutions, but also to protect the user from new and not yet publicly documented security risks. NGRAVE removes the risk for remote attacks by completely "air-gapping" the hardware device, meaning that the device does not have any network capabilities nor does it need a USB connection to sync accounts or sign transactions. The NGRAVE ZERO communicates with the LIQUID app solely via one-way QR codes. NGRAVE also introduces a multi-layered anti-tampering framework to protect the device from any remaining physical attack vectors.

Several novelties are introduced in the various stages of the customer journey, triggered by NGRAVE's unique "What-if" approach. One example is the upgraded key generation process, introducing a user interaction step to counter tampering attempts and potential weaknesses in the integrity of the secret key. Another is the "key split" principle and recoverable nature of the NGRAVE GRAPHENE backup plates.

NGRAVE has actively been seeking and including user feedback as from the early stages of the project. Using NGRAVE's solution is one of the most effective ways for the user to protect him/herself from theft and/or loss of the digital assets in his or her possession.

References

Damien Giri, Jean-Jacques Quisquater. 2018. "Cryptographic Key Length Recommendation". Available at https://www.keylength.com/en/4/.

Ciphertrace. 2019. "Q2 2019 Anti-Money Laundering Report". Available at https://ciphertrace.com/q2-2019-cryptocurrency-anti-money-laundering-report/.

Parity Technologies. 2017. "The Multi-Sig Hack: A Post-Mortem". Available at https://www.parity.io/the-multi-sig-hack-a-postmortem/.

Juha Saarinen, IT News.com. 2017. "White Hats Steal Ethereum To 'Save' Users After Hack". Available at https://www.itnews.com.au/news/ethereum-crypto-currency-in-new-million-dollar-hack-scare-468800.

Jordan Pearson, Vice.com. 2017. "How Coders Hacked Back To 'Rescue' $208M In Ethereum". Available at https://www.vice.com/en_us/article/d3djwj/ethereum-wallet-parity-knew-about-critical-flaw-that-let-user-devops199-lock-up-millions.

Hanne Degans, Imec Press Release. 2018. "Imec And Cadence Tape Out Industry's First 3nm Test Chip". Available at https://www.imec-int.com/en/articles/imec-and-cadence-tape-out-industry-s-first-3nm-test-chip.

Ledger Donjon. 2019. "Security Analysis Of Ellipal (Hardware) Wallet". Available at https://ledger-donjon.github.io/Ellipal-Security/).

Cybergibbons. 2019. "Bitfi Archive". Available at https://cybergibbons.com/category/security-2/bitfi/.

Saleem Rashid. 2018. "Breaking The Ledger Security Model". Available at https://saleemrashid.com/2018/03/20/breaking-ledger-security-model/

M.P. Pawlowski, A. Jara, & M. Ogorzalek. 2015. "Harvesting Entropy for Random Number Generation for Internet of Things Constrained Devices Using On-board Sensors". Available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4634515/

SatoshiLabs. 2019. "Our Response To Ledger's #MITBitcoinExpo Findings". Available at https://blog.trezor.io/our-response-to-ledgers-mitbitcoinexpo-findings-194f1b0a97d4.

Ledger. 2019. "Check If Device Is Genuine". Available at https://support.ledger.com/hc/en-us/articles/360002481534.

Nicolas Bacca. 2018. Twitter Discussion On Cryptographic Attestation. Available at https://twitter.com/BTChip/status/949679898012078082.

Michael B. Kelly, Business Insider. 2013. "The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought". Available at: https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11?r=US&IR=T.