Safety beyond the grave through Chainlink and NGRAVE

A dead man switch powered by the private key backup hardware of NGRAVE and Chainlink's decentralized oracle network

Disclaimer: *This article is a collaborative effort between Chainlink and NGRAVE. Chainlink is an open-source protocol that has been pioneering secure smart oracle technology. NGRAVE is a blockchain security provider offering a secure and user friendly end-to-end solution for the self-sovereign management of one's digital assets and cryptocurrencies.*

1. Intro & problem statement

A dead man's switch is a trigger designed to be activated if the human operator becomes incapacitated, such as through death. While this term was originally coined for physical switches on a vehicle or machine, it has since been used to describe other intangible uses like in computer software.

In the context of cryptocurrency, using a smart contract to execute a dead man's switch has been a popular subject of discussion because in many cases it's less expensive and faster than the legacy system of lawyers and wills. This kind of decentralized solution offers particular benefits around censorship resistance given the constant uptime and computational redundancy of decentralized blockchain networks. Furthermore, the highly automated aspect makes it possible to ensure that, in case of an untimely death, any and all digital assets are safely transferred to the assigned beneficiary without any friction.

Since cryptocurrency incorporates private/public key pairings to secure user's funds, the most logical part to pass on after death is the private key, or similarly the seed words of a hardware wallet. Many household solutions exist, such as making redundant copies and dividing these over many different people. However, all of these methods require trust that those third party guardians do not collude to steal your crypto.

To guarantee that a user's digital assets are safeguarded and will not be accessed before the owner dies, two things need to be secured:

- **the storage of the asset:** it should not be accessible by anyone whilst in custody.
- **the trigger of the dead man's switch:** the stored private key - or the access hereto - should only be released upon death, and even then, only in such a way that no third party other than the actual beneficiary can get access to this private key.

With this article we want to explain how a truly secure dead man's switch can be constructed for the NGRAVE ZERO hardware wallet using both a third party KYC provider and the decentralized oracle network of Chainlink. We demonstrate our proposed initial implementation and end with a short report on an improved future implementation using trusted execution environments. We are very open to having a discussion if you have any additional thoughts, so don't hesitate to reach out to us!

2 Components

In this section we give an overview of the different components of the proposed solution, as well as a description of their role in the framework. We start off with NGRAVE's[1] hardware wallet and cold backup, which allows for a backup seed or private key to be split up into two different parts which are meaningless if not combined. Then we describe how a third party KYC service is ideal for keeping the KYC of the beneficiary safe, as well as the information necessary to access part of the backup. Lastly we expand upon Chainlink[2], which is the market's leading oracle provider and is used to provide a trust-minimized check on an external event, which in this case is confirmation of the original owner's death.

2.1. NGRAVE: The ZERO hardware wallet and GRAPHENE cold backup

Hardware wallets are the safest way to store your digital assets. The NGRAVE ZERO is a true offline hardware wallet without any network capabilities, fully removing remote attack vectors. The device itself is military grade tamper proof and has an EAL7[3] certified secure OS, which brings an unparalleled level of security unseen in the blockchain space.

Figure 1: NGRAVE's ZERO & GRAPHENE.

[1] www.ngrave.io
[2] http://chain.link
[3] https://bit.ly/39AN1Nn

The ZERO is a touch-screen device with an intuitive and ergonomic user interface, enabling fast blockchain interactions through the use of QR codes that never contain data on the private keys. This can be done either through NGRAVE's own mobile app referred to as the NGRAVE "LIQUID", or any third party solution including crypto exchanges or software wallets.

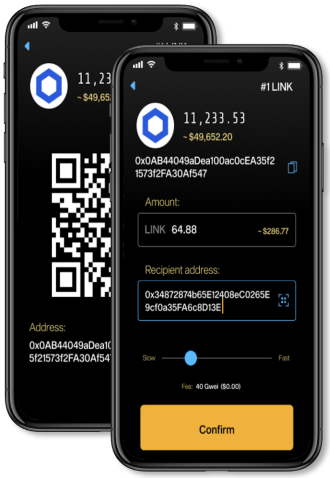

Figure 2: NGRAVE's mobile app, the LIQUID.

While the ZERO supports mnemonic phrases (such as 24 word backup seeds), it also introduces a so-called "Perfect Key", a 64-character hexadecimal representation of your seed. This brings a whole new level of security. NGRAVE's seed backup, referred to as the GRAPHENE, is a cryptographic puzzle made of two fire-, water-, buried, & shock-proof stainless steel plates. It removes entirely the need for paper wallets and more traditional metal back-ups that, when found, reveal either the full key or part of it.

The GRAPHENE's top plate contains 64 columns each representing a respective hexadecimal (0-9, A-F) character of the seed. Hence 64 columns with each having 16 possible values. Character values of the top plate are scrambled differently for each user, making the top plate configuration as unique as an actual private key. The lower plate is blank

until the user punches indents into it using an embossing click pen and the unique top plate as an overlay. The real power here is in the fact that the bottom plate is useless without the top plate, and vice versa, since the unique characters of the top plate can only be identified if matched with indents of the bottom plate. Even if two people had the same bottom indents, their top plates will have different values associated with those indent locations. This introduces a whole new level of durability and security for user's backup seeds.

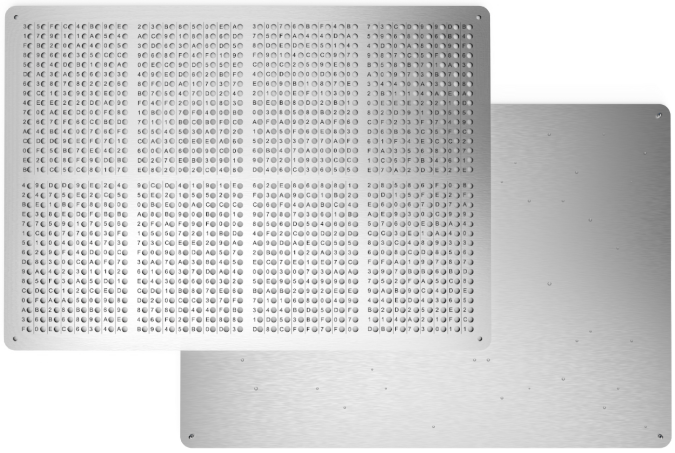

Figure 3: NGRAVE's GRAPHENE dual plate set-up.

Additionally, what makes the GRAPHENE stand out from competitors is its recoverability. When a user loses his top plate, NGRAVE is able to recover it. NGRAVE cannot recover the lower plate however - as it would then be able to reconstruct the seed. Nonetheless, there is a way to recover both if so desired by the user, and more peculiarly in the use case of beneficiary management for inheritance planning. The challenge is the following: *The beneficiary needs to know both the unique configuration of the top plate, and the location of the lower plate.* And that's where the dead man's switch comes in.

Learn more by visiting the NGRAVE website, Twitter, Facebook, LinkedIn, or Telegram.

2.2. KYC and beneficiary management

Know your customer, also referred to as know your client or simply KYC, is essentially the process of verifying the identity of users and clients. While KYC is widely used within the context of ensuring certain legal processes are followed, such as complying with anti-money laundering laws, KYC processes are also more generally employed by companies of all sizes for the purpose of ensuring their proposed customers, agents, consultants, or distributors are actually who they claim to be. In the context of this article, KYC is relied upon to know who the original owner of the key is, as well as who his assigned beneficiaries are. The KYC provider in the proposed solution will only have access to one piece of the information required to reconstruct the full private key / seed backup. There are many existing KYC providers that can perform this function, and the KYC process doesn't have to be as thorough as more rigourous anti-money laundering procedures. Also, this could allow for users to highlight their own preferred KYC provider.

2.3. Chainlink: Decentralized Oracle functionality

Smart contracts are highly reliable deterministic digital agreements running in the computation layer of a distributed ledger. To interact with data outside of the blockchain (for example an API) smart contracts use oracles. As blockchains and smart contracts are deterministic, oracles function as the messaging layer between off-chain and on-chain events.

Since blockchain-based smart contracts get their security from an extreme redundancy of computation from independent nodes, and because smart contracts are deterministic in that they use inputs to compute outputs based on pre-defined logic, it is no surprise that using one single oracle to trigger this smart contract is a single point of failure, as this oracle essentially functions as a trusted third party. Downtime or

malicious acting of the oracle could result in the smart contract malfunctioning, which introduces a major security vulnerability. This obstacle is generally called the “oracle problem”.

To solve this, Chainlink applies the concept of decentralization to oracles, by forming a network of independent oracles that provide a wide range of data and connections. Users can customize, among others, the number of oracles, types and number of data sources, and aggregation techniques used to combine said data.

For this implementation, Chainlink was chosen as it is quickly establishing itself as the leading oracle provider. The high customizability offers the chance to get the highest level of security when it comes to connecting off-chain data to the smart contract used by the dead man’s switch. Thanks to Chainlink’s solution, the proposed framework now has an end-to-end security of the very highest level.

Chainlink is a decentralized oracle network that enables smart contracts to securely access off-chain data feeds, web APIs, and traditional bank payments. Chainlink is consistently selected as one of the top blockchain technologies by leading independent research firms such as Gartner. It is well known for providing highly secure and reliable oracles to large enterprises (Google, Oracle and SWIFT) and leading smart contract development teams. Learn more by visiting the Chainlink website, Twitter or Telegram. If you’re a developer, visit the developer documentation or join the technical discussion on Discord.

Learn more by visiting the Chainlink website, Twitter or Telegram. If you’re a developer, visit the developer documentation or join the technical discussion on Discord.

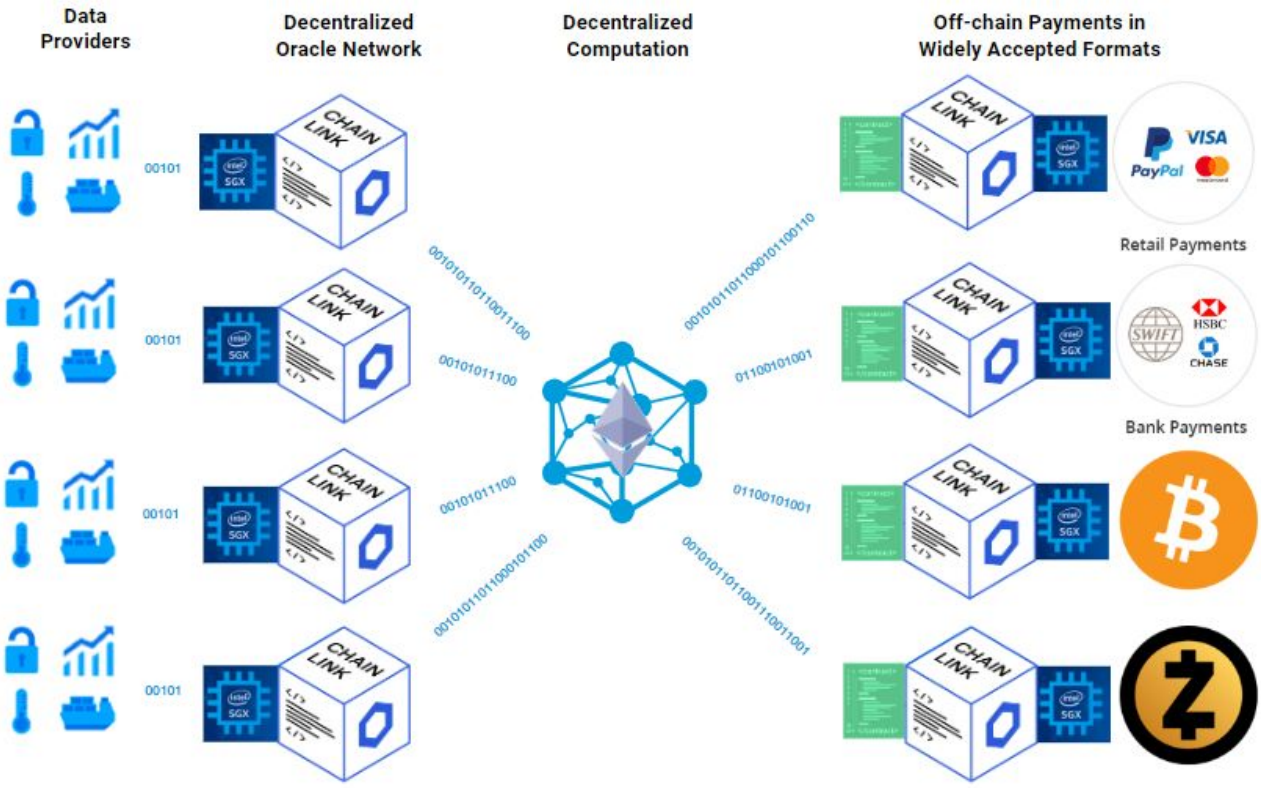

Figure 4: A visualization of Chainlink’s decentralized oracle network.

3. Implementation

Abbreviations used: OO = Original Owner; LP = Lower Plate; TP = Top Plate; B = Beneficiar(y)(ies)

Step 1 - Engrave & store the GRAPHENE plates

1.1 The OO[4] generates an NGRAVE "perfect key", being the hexadecimal version of the 24 word mnemonic:

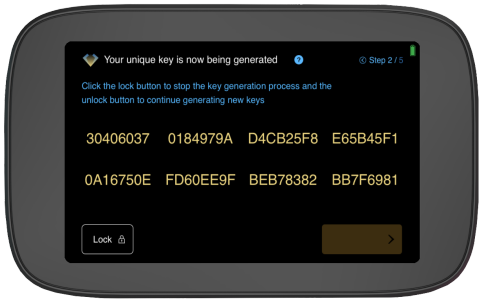

Figure 5: NGRAVE's ZERO hexadecimal seed.

1.2 The OO makes a backup of this seed on the NGRAVE GRAPHENE, by means of a punch pen that makes holes in the LP[5] through the overlay holes in the TP[6]. This eventually will reveal the key visually if both plates are placed on top of each other, as shown in figure 3.

1.3 It is recommended that the OO keeps both plates in a separate physical location, as both plates are required to figure out the key.

1.4 Inside the GRAPHENE product package, the OO will receive a unique recovery ID with which he can request NGRAVE to send him a new TP with an identical configuration.

Step 2 - Using a third party KYC provider and Chainlink for LP recovery

2.1 + 2.2 To assign a B[7], both OO and B need to do KYC via a third party KYC provider and link B to OO. OO's data will include a message with the location of the LP. An alternative here is that OO just provides B with a second, identical LP. However, this is the more risky alternative, especially if the OO gives the TP recovery ID (see further) to B. B would then be able to fully reconstruct the seed, regardless of the OO being out of the picture.

2.3 When B wants to get access to the LP location, B will have to prompt the third party KYC provider, ideally with a death certificate.

2.4 In any case, the KYC provider will then prompt Chainlink's oracle function to confirm with a relevant obituary.

2.5 This provider can, when validated by Chainlink, release all info, including the LP location message, to B.

Step 3 - Using NGRAVE for TP recovery

Step 3.1 Whereas the LP recovery will be managed through the third party KYC provider and Chainlink, the TP recovery will be done by NGRAVE. NGRAVE will always attach a unique recovery ID to a GRAPHENE shipment.

Step 3.2 This recovery ID can be used by the OO to recover his TP in case of loss.

Step 3.3 In the use case of posthumous recovery, the OO can provide the TP recovery ID to his B, for whom it will be useless as long as they don't have the LP configuration.

Step 3.4 The B can ask NGRAVE to recover the TP with the recovery ID.

Note that the B could get a LP from the OO directly, as the OO can order several LPs, keeping one or more himself and having one at his beneficiary, who still needs the TP anyway. It is in any case recommended for the OO to have at least two LPs

[4] Original Owner
[5] Lower Plate of the NGRAVE GRAPHENE
[6] Top Plate of the NGRAVE GRAPHENE
[7] Beneficiary

in case he would lose one of them, as there is no recovery option for the LP from NGRAVE's perspective (otherwise NGRAVE could reconstruct the full key by itself). However, as it is typically the TP recovery code that will be shared with B already, this would introduce an (undesired) risk.

The OO could order two TPs with identical configuration, which would require the B to just validate the obituary part at the KYC provider to obtain the lower plate.

Instead of the location of the LP, the KYC provider could keep a visual version of it, which might be less prone to error or change compared to the location of the LP.

NGRAVE doesn't keep a direct link between the TP configuration and the recovery ID, instead it combines the latter with a dedicated NGRAVE key. The two "codes" together result in the TP configuration. This adds additional security for NGRAVE's part.

Upon user request, NGRAVE can also keep specific KYC data so that it can ultimately link one or more TP configurations to the OO himself.

In the "most paranoid" version of a potential implementation, the OO could also opt for NGRAVE not keeping anything on the TP. That way, there is no recovery option and the OO is the only one with information on his plates and key.

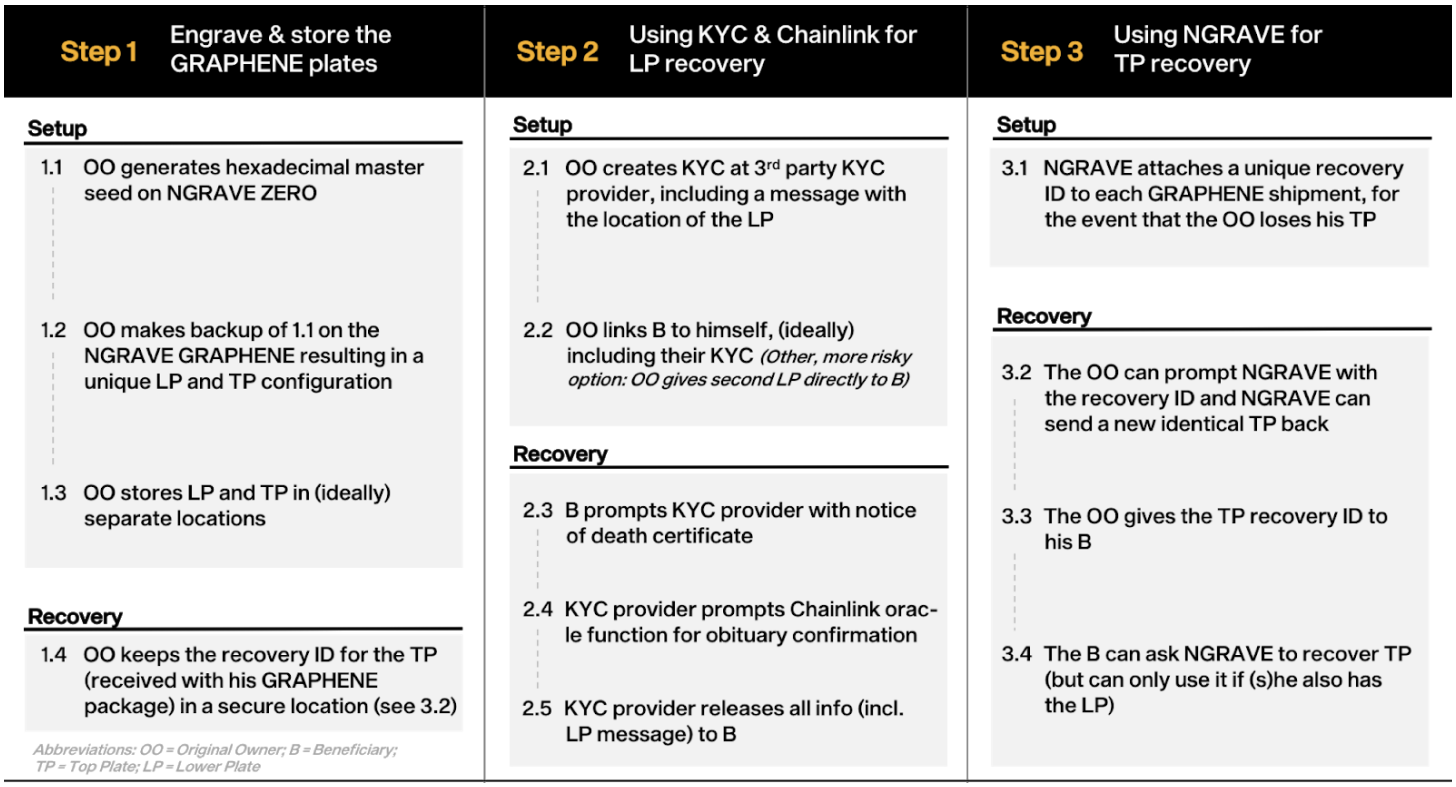

Figure 6: Overview of the dead man switch.

4. Future implementation

While the aforementioned implementation is built up from a vision of extreme security and reliability with as few compromises as possible, some extensions can be considered in the medium to long term.

4.1 Full smart contract

A 100% smart contract based solution was considered, but has its own security issues. Smart contracts are inherently online and this opens up another potential attack surface. However, once smart contracts transcend beyond their current nascent stage, this avenue of investigation could be reopened and perused.

4.2 Trusted Execution Environments

A trusted execution environment or TEE is a secure part of a CPU. It is an isolated part of the chip that runs completely parallel with the operating system, providing security and privacy from everything outside the trusted execution environment. As this enclave is completely isolated, it is protected from apps running in a main operating system, as shown in figure 6. An example of aTEE is Intel Software Guard Extensions (Intel SGX).

The trusted execution environment functions as a black box environment. A user can encrypt messages going into the TEE using the TEEs public key, meaning the message can only be decrypted inside the TEE with the TEEs private key. Likewise, the TEE could send an encrypted message out that only the user knows how to decrypt. This allows for private and secure computations.

Optionally, Chainlink oracles can run on computers or servers that have CPUs which offer TEEs - thereby extending the level of security available to smart contracts.

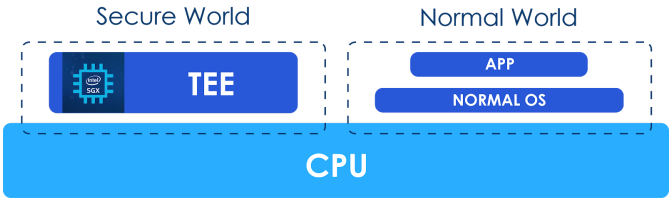

Figure 7: Architecture of a trusted execution environment.

If you want to have a smart contract trigger a transaction, the oracle has to access the private key, and with a Trusted Execution Environment you have a stronger assurance on the hardware level that the chainlink node operator does not have access to this key.

5. Conclusion

In this article we proposed a dead man switch powered by the private key backup hardware of NGRAVE, a third party KYC provider, and Chainlink's decentralized oracle network. Using the GRAPHENE's double plate system, the back-up key can be stored in a divided fashion with one part recoverable through NGRAVE, and the other through a KYC provider waiting to be triggered by Chainlink's decentralized oracle network upon passing of the original owner. This combination would serve as a highly reliable, trust-minimized dead man switch for recovering digital assets stored on the hardware wallet.

Contact us: support@chain.link
Join the discussion on Discord

The Chainlink network provides reliable tamper-proof inputs and outputs for complex smart contracts on any blockchain.

Chainlink

Contact us: safe@ngrave.io
Subscribe on www.ngrave.io

NGRAVE

NGRAVE is a blockchain security provider offering a secure and user friendly end-to-end solution for the self-sovereign management of individuals' and business' digital assets and cryptocurrencies.