Crypto Will

Decentralized testaments on the blockchain

Abstract

During the early ages of crypto-currencies, more and more people started to join the network. Every person has the inevitable outcome of death. In the age of fiat-currencies it’s possible for others to manage your funds. With crypto-currencies, assuming that only the person in question has the private key, no one would be able to recover said person’s funds. The person has to do it – post-mortem.

In this white-paper, we take a look into the CryptoWill-program, which is capable of storing both physical and digital assets and goods.

Table of Contents

The cryptographic workings

There are 3 roles in the CryptoWill network:

- Will author (makes a will for his successors)
- Successors (i.e children)
- Will keepers (nodes in the network keeping the wills in the form of cold-storage)

When the process begins, the will author will create a list of items, both physical and digital, and writes them down in his will. Each item can be assigned to a successor, like the family.

Each successor gets his own password for decrypting their part of the will. This is happening using symmetric encryption (i.e aes256). In essence, when you leave your will to your mother and sister, the sister can view the part of the will directed to her, but not the mother's, unless the mother discloses the information with the sister.

As a final result, a **master key** is created**.** This is a public-private keypair, where the public key is stored & signed with the will on the cold-storage network. The master key allows the creator to make changes to the will. Because the public key is stored with the will, all one needs to edit one's will, is the master key. The master key serves as a digital signature method to prove ownership, in case that's needed, and also serves as a seed to derive any other keys from (like the passwords for the successors) or a third-party data-storage network (like Siacoin).

The encrypted result is being uploaded to a decentralized cold-storage network, along with some WillCoins, representing a finite amount of time of storage. Note that no one has to pay for the storage for a long time, this makes the will-creation process prepaid, and unattended for years to come.

For the creator of the will, it's important to share the passwords with each successor, as upon death, they can access the will's contents.

Will Creation & Upload

Upon will creation, the file is being encrypted and sent to a fixed amount of random, independent nodes. Let's make that *n = 10.* The nodes all get a full copy of the file. Note that we don't have to trust the nodes won't grab your private keys, since the contents are unreadable for them.

Along with the will, a smart contract is created and deployed on the block-chain, serving 3 purposes: **Proof-of-Life, External Proof-of-Storage** and **Rewards**. More on that later.

The will author will be presented with an interface where a few options can be selected, for instance:

- Respond after 7 days
- Respond after a month
- Respond after a year

What will be selected will determine the deadline for when the creator has to ping and perform a Proof-of-Life. When the creator fails to respond, death, or an otherwise inability to respond is assumed (i.e kidnapping), and the nodes storing the will, upload it to a third-party storage network, so successors can inherit the money.

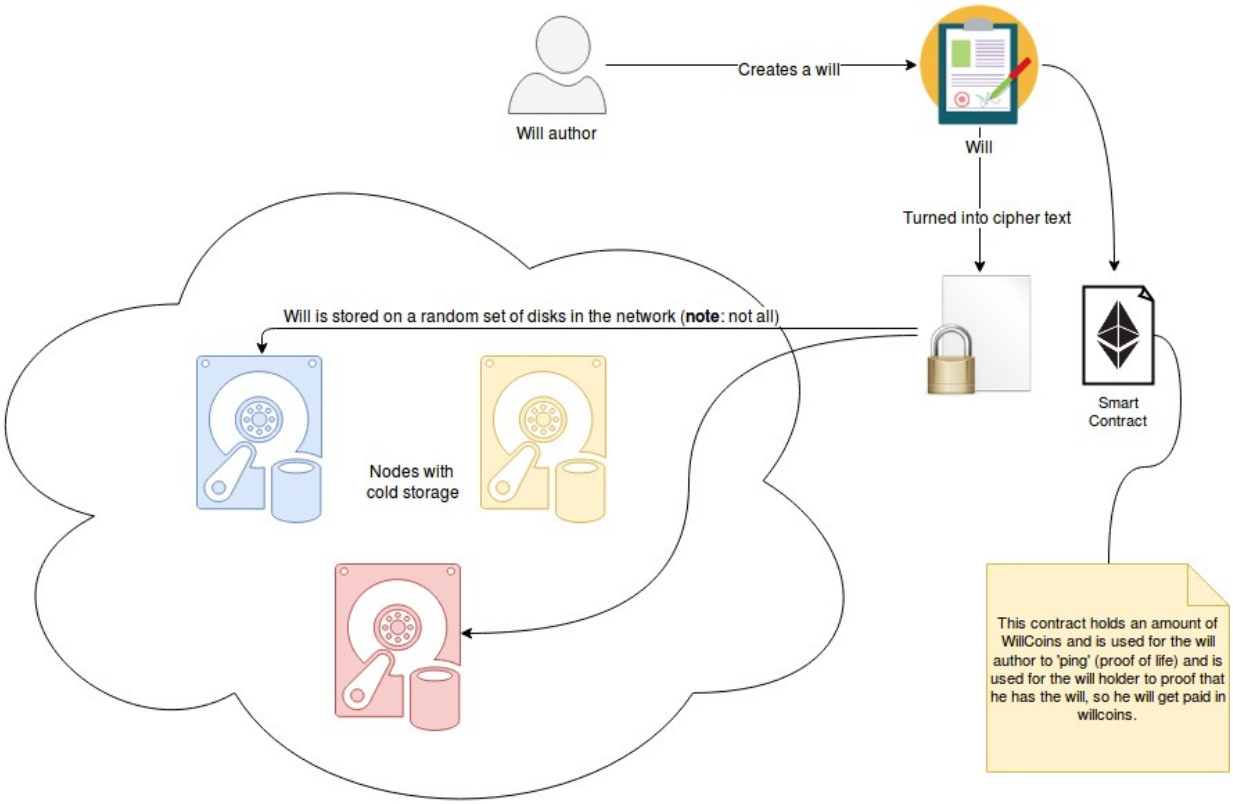

Illustration 1: Creating a will

Cold-Storage Network Validation

Cold-Storage is one of the key elements in the CryptoWill network. It’s purpose is to store wills in such a way that it is guaranteed to be kept for as long as necessary.