Self Custody Risk Analysis

Author: Eric Schuh

Email: eric@legreq.com

Github: @eric-schuh

Introduction

As the world moves more and more towards digital lives being a norm, the need to securely and reliably store digital assets in a privacy respecting way becomes paramount for the people of the world to trust the digital systems that are being put in place. Moreover there is a need for the technical implementers of these new technologies to enable individuals to handle their digital assets in such a way that does not prove unreasonably burdensome to the individual as this will be one of the main deciding factors in whether a given individual interacts with systems that issue and consume digital assets securely. Through the last two decades of the internet's evolution it has become abundantly clear that given a choice between doing more work to ensure privacy and security and convenience in the use of a system most users choose convenience–to the point that many will stop using a system if the privacy and security aspects of the system prove to be above their accepted level of burden. One of the main challenges of this is that each individual has subtly different requirements for what they consider to be "too burdensome," and these requirements change for the same individual depending on what assets they are securing and/or the context they are in.

Background

Traditionally in the cryptocurrency space backup and recovery of your digital assets has primarily been done through the storage of seed phrases [1]. To many that are in the cryptography space this has become almost second nature, to the point that when talking to many in the space they will act like keeping a string of 24 words and punching them into a steel plate before securing it in some location is something that everyone should be familiar with. The issue is that for most of the world's people you may as well be telling them to become an astronaut. In the world of usernames, passwords, and for many software like LastPass, the idea of needing to keep this string of 24 words around seems insane.

In more recent times, there has been extensive work by groups like Blockchain Commons trying to develop better formulations for systems for self custody of cryptocurrencies, as seen in their SmartCustody scenario [2]. However, this still focuses mostly on the custody of monetary assets and likely has to high of a burden for many users and use cases, such as in the use cases for digital assets like an Over Age Credential or other similarly low-risk items. That is to say that while a user may accept a large degree of setup and maintenance burden to secure their life savings, they likely won't if what they are trying to secure is their local grocery store loyalty card.

Proposal

There are two main pieces of work that need to be done to get to the point where a piece of software could be created that would provide the framework for walking a user through the selection process of a self custody configuration that both addresses their individual security and privacy needs while also meeting the level of burden they are willing to accept at a given point in time, for a given context. These are: 1. Identification of recovery, backup and security strategies that are acceptable to use for different types of users. 1. As part of a contract with Digital Contract Design, Legendary Requirements has started a project to analyze various recovery strategies which was the driver for much of this paper [3]. 2. The development of a threat and risk model framework.

Item 1 above is needed to define the ways in which a user would be able to construct their system. Whether this is using Blockchain Common's Smart Custody strategy of setting up multiple "Signatory" devices that are in physically different locations, using a seed phrase stored on a titanium plate, utilizing your social network and distributing seed shards that can be pulled back together to recover, making use of a functionary/fiduciary service that holds shards of keys, etc. There are almost an endless number of ways in which you could theoretically construct a system, each with its own surface of burden and risks that it is weak to. So, the first step here is defining a structure so that these things can be defined, and maybe as importantly, updated in the future to account for better or new strategies of self-custody.

If Item 1 deals with physical construction of the system, Item 2 represents one of the key inputs that will inform the level of burden a user is willing to accept when deciding how to construct their particular self custody solution. The threats and risks a user cares about largely depend on what assets the user is storing and can change drastically for the same user in different contexts. That is why for the purposes of this software it is important to define a structure which any organization or entity could modify and update to represent the risks and threats they care about for their particular use case.

Combining these two items into a system where a given user can select the recovery strategies they are willing or able to use alongside the threat model that, to them, best represents the risks they care about, it should be possible to have an program that is able to recommend the best way to construct the particular user's system. This would, in theory, provide a framework for the organizations that wish to build a business around these digital asset systems with a tool that will make it easier for their users to interact with their system in a reliable and non-burdensome way.

References

[1] Ledger Seed Phrase Recovery

[2] SmartCustody

[3] Wallet Recovery