Insula

How does the blockchain keep my money secure?

One of the main selling points of ethereum and utility tokens is, of course, the security. Being told your funds are secured by technology is one thing, but how can you be satisfied with the security of the ethereum blockchain? Let us look at the infrastructure.

The Ethereum Address

Your Ethereum address, the same address where your ISLAs are stored, will be displayed in the format of "0x" at the start, followed by a string of letters and numbers. This is the typical format of a **hexadecimal** number.

Example Address

0xc3C180981b9A8daffa3f02113f5710505565429D

A hexadecimal number is simply a different number system. The number system we are familiar with (0-9) is the decimal system. Binary is another type (010101), Octal is another (0-7). Think of these number systems as dimensions or parallel number worlds. This means that your ethereum address is nothing more than a super long number, translated into hexadecimal format.

But how exactly does this secure my money?

The hexadecimal address we just mentioned is called your **public key**. It is the key that others will submit when they

want to identify and make payments to you. In fact, it only makes up half of your entire wallet. The other half is your **private key.**

Your private key is the reason you have sovereign ownership of your money.

Your private key is yours, forever. No one, under any circumstance whatsoever, will need to have access to your private key. When you want to switch to a new device, you will be asked to enter your private key. But to even access your own private key, you will need to enter a 12 seed key that was given to you when you first opened the account. You would have been asked to commit those 12 words to memory or to keep them in a secure location.

When money is sent to your public key, it communicates with your private key, and once the transaction is verified, the money is locked in. You and only you have the power to then use that money.

And to answer the question of how these keys are not hackable? Passwords and keys are usually obtainable through brute force, and the level of encryption of your public key, let alone your private key, will take a hacker several lifetimes to crack the code.

So, no risk of loss at all?

No risk! Well, not from our side at least. But If you keep your private key secure, then the risk is virtually obliterated!