The Blockchain Lawnmower! A Tokenization Tutorial

Author	josh
Date	2020-01-31 18:48:39

Overview

Several years ago during my early journey into the Bitcoin space, I heard Andreas Antonopoulos discuss the idea of tokenization on Joe Rogan's podcast. He was imagining a future in which we no longer trade car titles or mortgage deeds through government agencies. Instead, we would represent those assets as tokens on a blockchain.

I was inspired by this discussion, and a friend from our local blockchain meetup that encouraged me to pursue this concept further. So I built a prototype of a "tokenized" lawnmower in order to teach this concept!

To understand what a tokenized future might look like, we need to discuss a few technical components. Let's learn about the concept of non-fungible tokens, digital signatures, and then take a look at how this lawnmower prototype works!

Token Types, Proof-of-Keys, and a Prototype

Non-Fungible Tokens

First, in order to understand tokenizing real-world assets, we must understand the different types of digital tokens. There are "fungible" and "non-fungible" token types. Normal cryptocurrencies such as Bitcoin, Ethereum, etc. are generally considered "fungible" - this means that no one coin has different value than another. This is similar to US dollar bills - each dollar bill in your wallet is functionally no different than another. Each dollar bill represents an interchangeable one dollar in value.

But tokens that represent *specific* assets are called "non-fungible". The popular "Crypto Kitties" tokens are an example of this. Each token represents a *unique* asset - the crypto kitty. Applying this to real-world tokenization, a non-fungible token can be used to represent a unique asset like a home or a car. Each car is unique, each home is unique - and therefore the tokens must be distinguishable from one another in this manner.

Digital Signatures

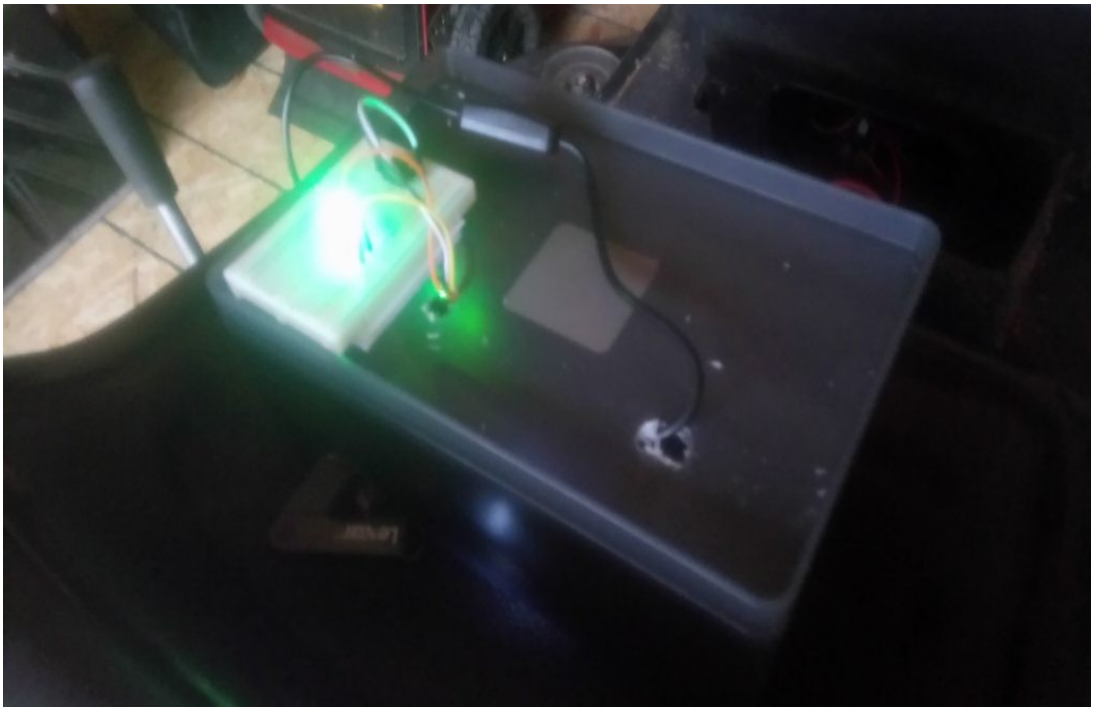
Next, we'll need to understand digital signatures to build our future world of tokenization. If you've used a cryptocurrency like Bitcoin before, you know that coins are sent to and from various *addresses.* Addresses are derived using what's called *public key cryptography.* A random "private key" is generated. Next, an elliptic curve algorithm is used to derive a "public key". Finally, some further hashing and encoding is done to create the final address.

This process is one way - you cannot go back from the public key to the private key. However, the magic of public key cryptography is the ability to prove that one owns the private key for a particular public key by "signing" a message. Anyone with the signature, message, and public key can verify that this person owns the private key *without that key having to be revealed.*

This is a critical part of our tokenized future - users can prove they own an asset at a public key (address) by signing with their private key. However, they never have to trade or reveal that secret key at all!

A Prototype - The Blockchain Lawnmower

Based on these concepts, I built a prototype "tokenized asset" using a Raspberry Pi, a USB drive, and my trusty lawn tractor!



Here's how this prototype works:

> First, I created a non-fungible token to represent the tractor on the Bitcoin Cash blockchain, using the SLP standard
> The Raspberry Pi serves as a "starter module", which fetches the current owning address from the blockchain and stores it for offline use
> The "starter module" sends a message to the user's crypto wallet - in this case, a USB drive with the private key and some Python code on it. The message is based on the asset ID, address, and timestamp
> The wallet (USB key) signs the message using the private key
> The starter module verifies the signature is valid - meaning the wallet holder is the rightful owner of the mower
> The mower can then be started using a push-button

The Blockchain Mower and a Tokenized World

This mower represents a proof-of-concept for a tokenized future. I don't think it's likely we'll need to trade mower titles on the blockchain in the future, but it certainly shows the idea! We could some day see car titles, mortgage deeds, and more traded on blockchains instead of through government agencies. And instead of trading keys, we'll simply use our own private crypto wallets to unlock and start our assets. With non-fungible tokens, digital signatures, and a bit of electronics know-how, we can show what this ecosystem might look like!