Asset management & Authentication using RFID & Blockchain

Advisor: Dr. Justin Foreman
Student: J'son Brim

Project Purpose:

- To help businesses manage merchandise while also proving the authenticity of their merchandise, due to oversaturation of 1:1 copies created by authenticators.

- Further add security to anything that uses RFID.

- To explore the feasibility to incorporating checksums paired with RFID, and the digital signatures created using blockchain.
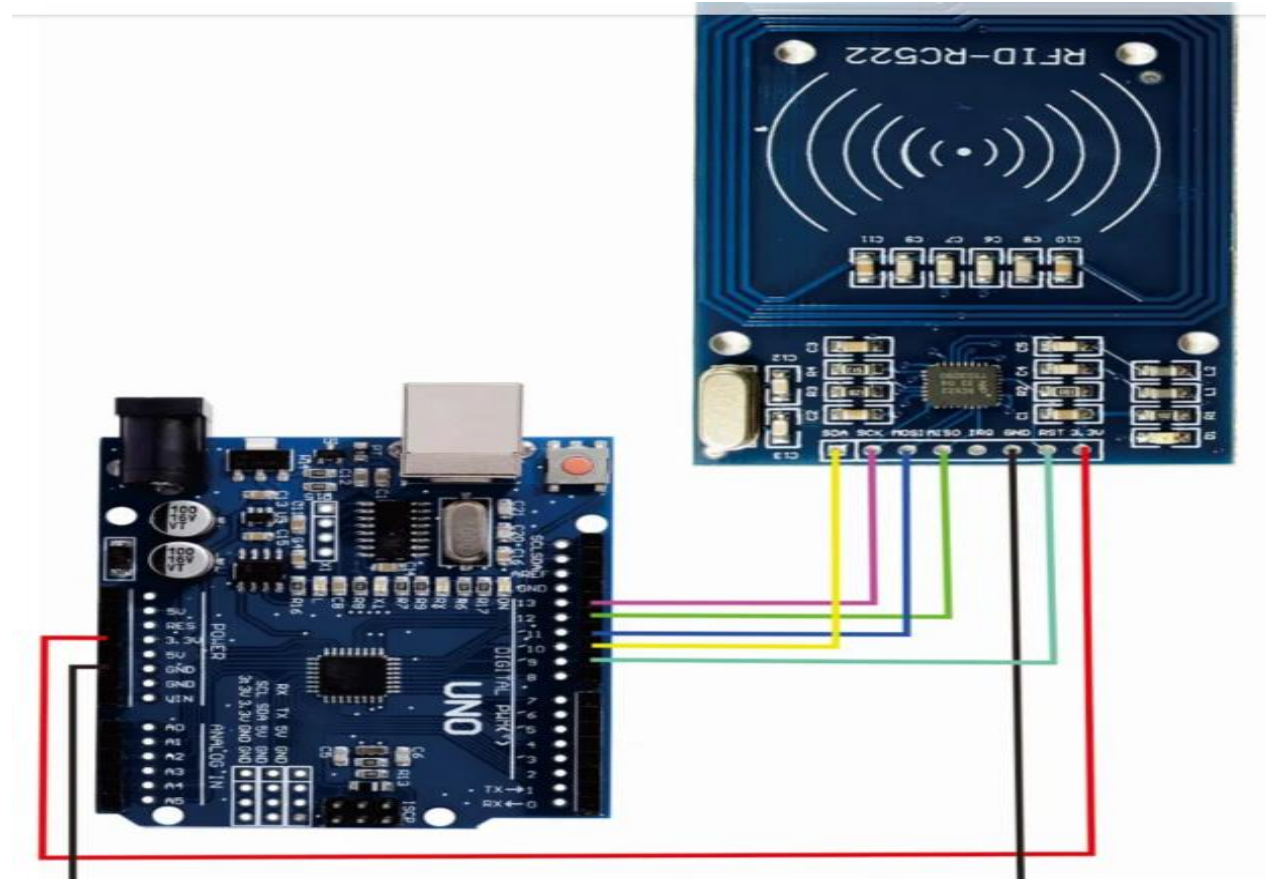
Arduino Uno R3 & MFRC 522 scanner equipment

RFID tags

Buck Converter

Arduino Uno R3

MFRC 552 scanner
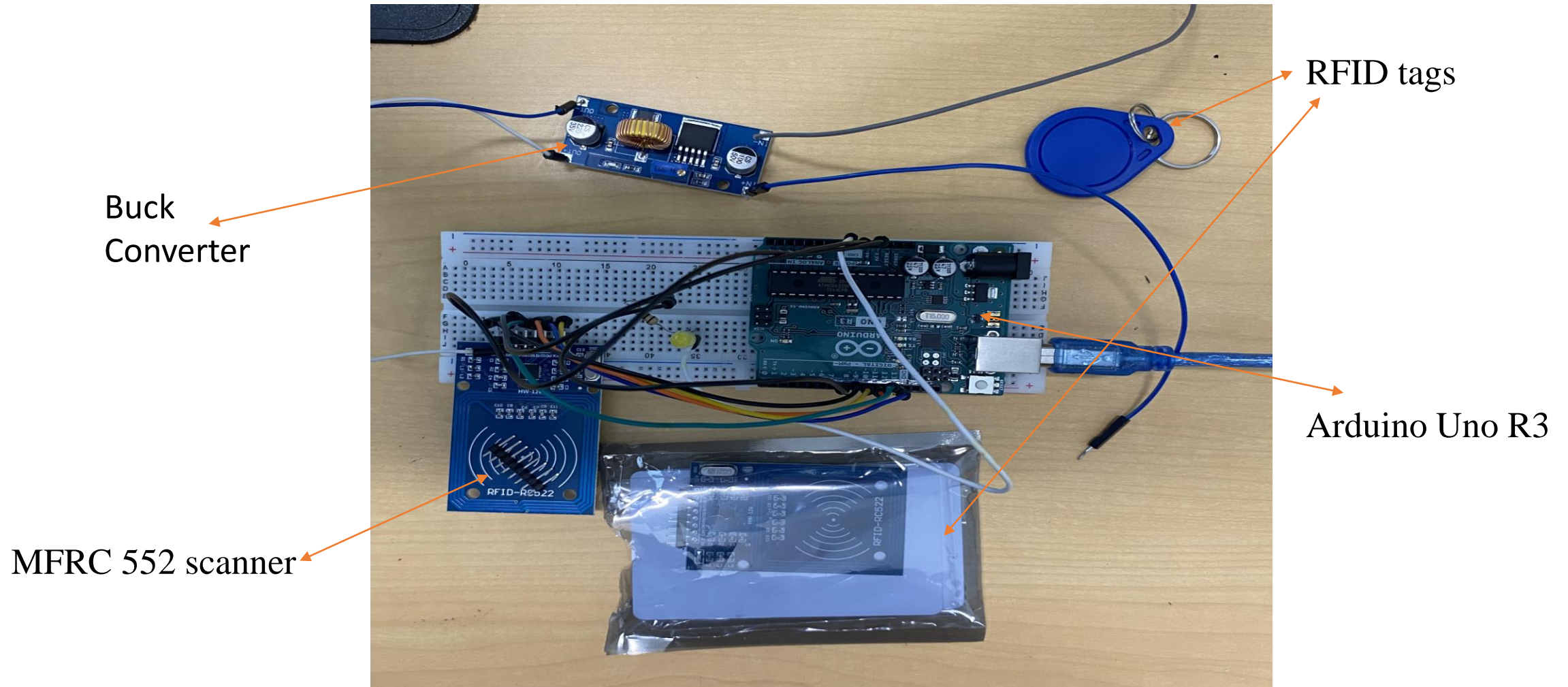
Arduino, MFRC 522 schematic

Arduino Uno R3/MFRC scanner schematic

RFID (Radio Frequency Identification)

- RFID essentially is the communication of 3 systems, a reader, antenna, and tag. This system uses the antenna to emit radio waves to communicate between the tag and the reader.

- My project consists of an Arduino uno r3(RFID reader), MFRC 522 (antenna), and my RFID tags.

Arduino RFID system:

- Depicts a portion of the Arduino code used to run the RFID system

- Output results which show the RFID number associated with tags

- Physical representation of system, when the correct tag is scanned the led light turns on


```
sketch_apr5a.ino
    1    #include <MFRC522.h>
    2    #include <MFRC522Extended.h>
    3    #include <deprecated.h>
    4    #include <require_cpp11.h>
    5
    6    #include "SPI.h"
    7
    8    #include "MFRC522.h"
    9
   10    #define SS_PIN 10
   11
   12    #define RST_PIN 9
   13
   14    #define LED_PIN 8
   15
   16
   17
```

Output   Serial Monitor ✕

Message (Enter to send message to 'Arduino Uno' on 'COM3')

```
14:47:30.840 -> 13:22:0B:0E
14:47:34.785 -> 13:22:0B:0E
```
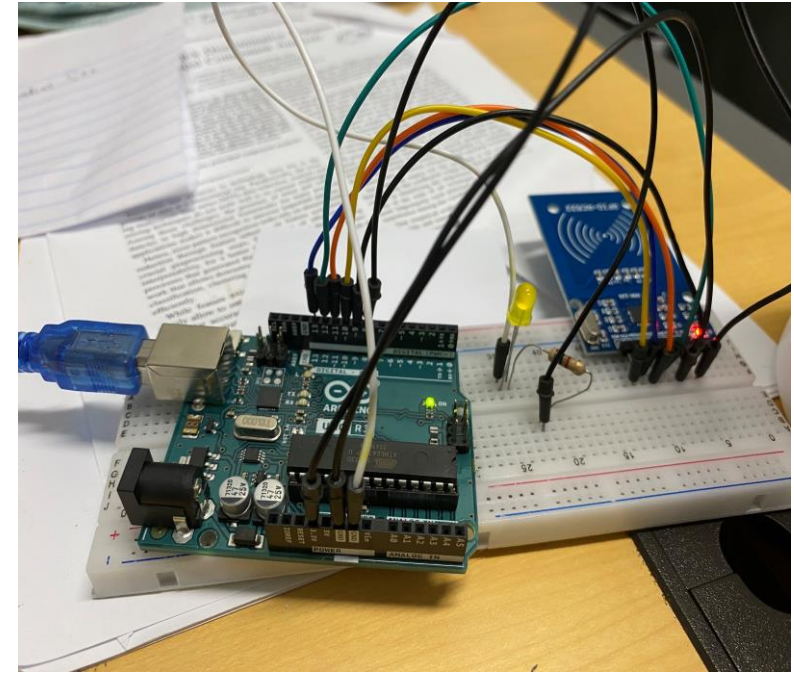
Output   Serial Monitor ✕

Message (Enter to send message to 'Arduino Uno' on 'COM3')

```
15:34:11.759 -> Tap card key: 13:22:0B:0E
15:34:14.294 -> Tap card key: C3:83:05:0E
15:34:18.695 -> Tap card key: 03:DA:72:9A
```

Buck Converter

- A buck converter or a dc chopper is an electronic system that allows for the manipulation of voltage, in this case it behaves as a step down for the voltage supplied to the MFRC 522 scanner.

Justification:

- Due to the rating of the MFRC 522 scanner being 2.5v-3.3v, I didn't want to operate this device at its maximum voltage rating due to potential degradation effects.
- A buck converter was preferred over a voltage due to a better efficiency of heat dissipated, while it also freed up more space to be used on my breadboard.
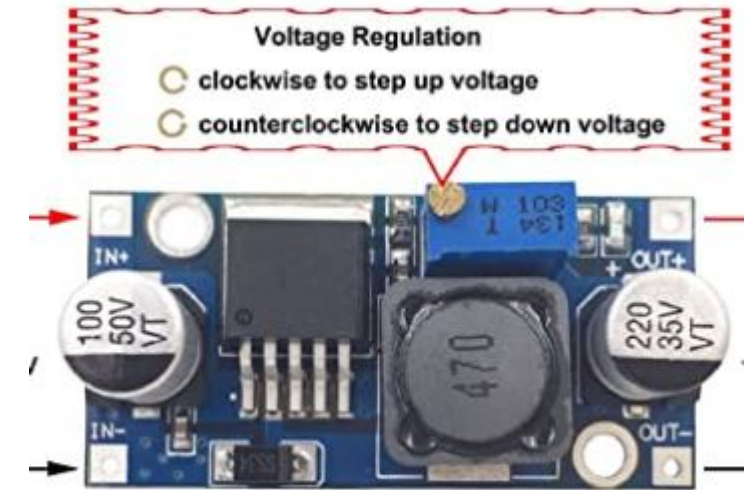
Buck converter implementation:
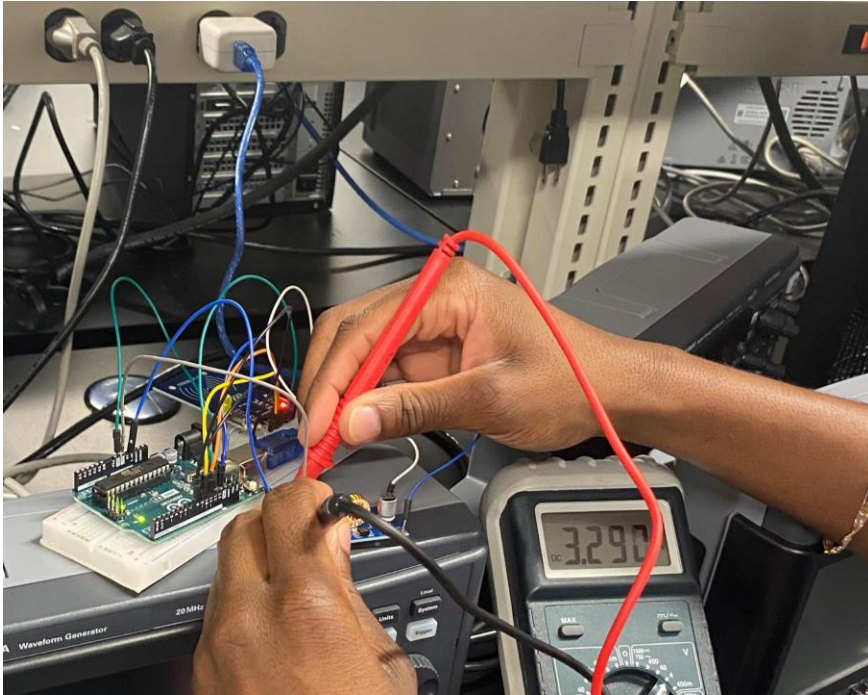
Input voltage
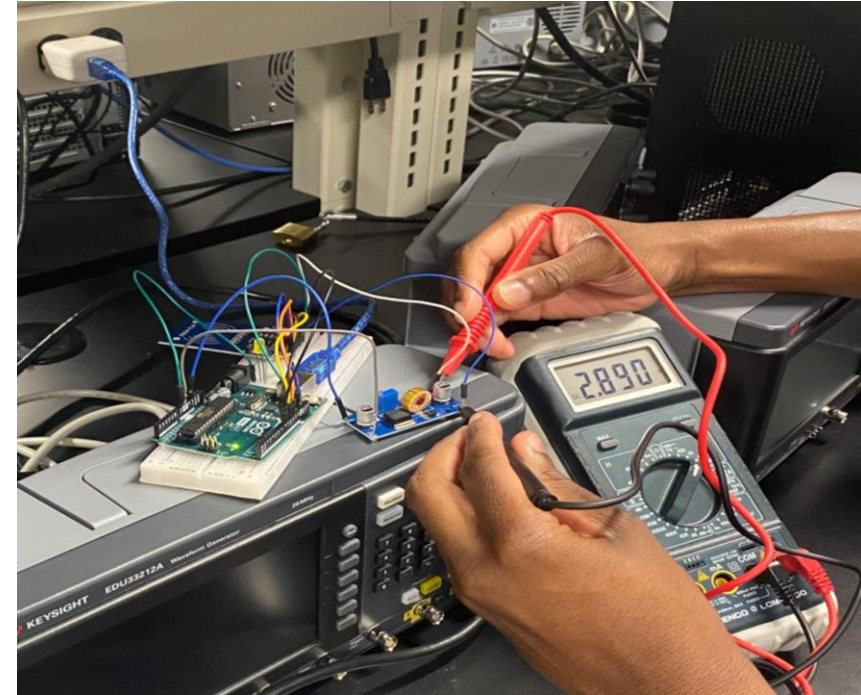
Output voltage

I checked my input and output voltage using the multimeter show above. Then I used the potentiometer to manipulate the voltage as shown, to achieve the goal of stepping the voltage down to more appropriate levels.

Blockchain

Blockchain is known as distributed ledger technology, it promotes transparency between entities and is a peer-to-peer network. Some examples of blockchain are Bitcoin, Ethereum, and Corda.

In my project I'm using blockchain technology to create a blockchain using each RFID tags assigned to each individual piece of merchandise, in order to hash each RFID tag to get a unique digital signature that associated with that specific RFID tag.

Blockchain in C++

- Here is my C++ code created using replit. A string is created for each individual RFID, and a blockchain is created in which each block created by the tags are dependent upon each other. If I change one of the tags the digital signatures for all of them chang. simultaneously.

```cpp
#include <functional>
#include <iostream>
#include <string>

using namespace std;

// To demonstrate String Hashing
void stringHashing() {

    // Get the string
    // to get its hash value
    string genblock = "RFID 13:22:0B:0E";
    string block2 = "RFID C3:83:05:0E";
    string block3 = "RFID 03:DA:72:9A";
    string block4 = "RFID 33 A7 Z9 77";

    // Instantiation of Object
    hash<string> mystdhash;
```

```cpp
    // Using operator() to get hash value
    cout << "genesis block hash values: " << mystdhash(genblock) << endl;
    cout << "Block 2 hash values: " << mystdhash(block2 + genblock) << endl;
    cout << "Block 3 hash values: " << mystdhash(block3 + block2 + genblock)
        << endl;
    cout << "Block 4 hash values: "
        << mystdhash(block4 + block3 + block2 + genblock) << endl;
}

// Driver Code
int main() {

    stringHashing();

    return 0;
}
```

Blockchain results

As demonstrated running the code assigns digital signatures and creates a blockchain.

```
> sh -c make -s
> ./main
genesis block hash values: 15235158836414755889
Block 2 hash values: 237779085523494110
Block 3 hash values: 15051671018298995404
Block 4 hash values: 691248080303023788541
```

Original block chain

```
> sh -c make -s
> ./main
genesis block hash values: 8419464429105928147
Block 2 hash values: 9857312407641241988
Block 3 hash values: 6910770385305733161
Block 4 hash values: 7280250203685766577
```

Tampered block chain

Changing any number in the RFID tag results in a change in all the outputs/digital signatures.

The aspect of pairing an RFID tag with a digital signature created by a blockchain further increases the security of any item allowing them to become uncopiable.

CECSTR

Future work

- Investigate approaches to making the hashing of objects autonomous.

- Exploring the feasibility of further increasing the security by adding checksums to the digital signatures.

Conclusion

- After implementation of both blockchain and RFID to assign unique RFID tag numbers and digital signatures to specific items. I found that the use of these two systems have other implementations that can further endeavors outside of retail.