

Hardware Wallet - Buzdea Matei

Introducere

Functionalitatea principala a unui Hardware Wallet este de a oferi o metoda sigura si independenta de gestionare a semnatuurilor criptografice, in special pentru tranzactii cu criptomonede. Acesta stocheaza in mod sigur cheile private ale utilizatorului.

Proiectul este dezvoltat cu ajutorul unui microcontroller care primeste o tranzactie prin bluetooth, afiseaza detaliile acesteia pe un LCD, iar dupa validarea manuala semneaza tranzactia cu cheia privata stocata local, returnand-o catre utilizator.

Ideea a pornit de la functionalitatea de baza a unui Hardware Wallet, dispozitiv care in ultimii ani a devenit din ce in ce mai popular odata cu necesitatea securitatii in tranzactiile digitale.

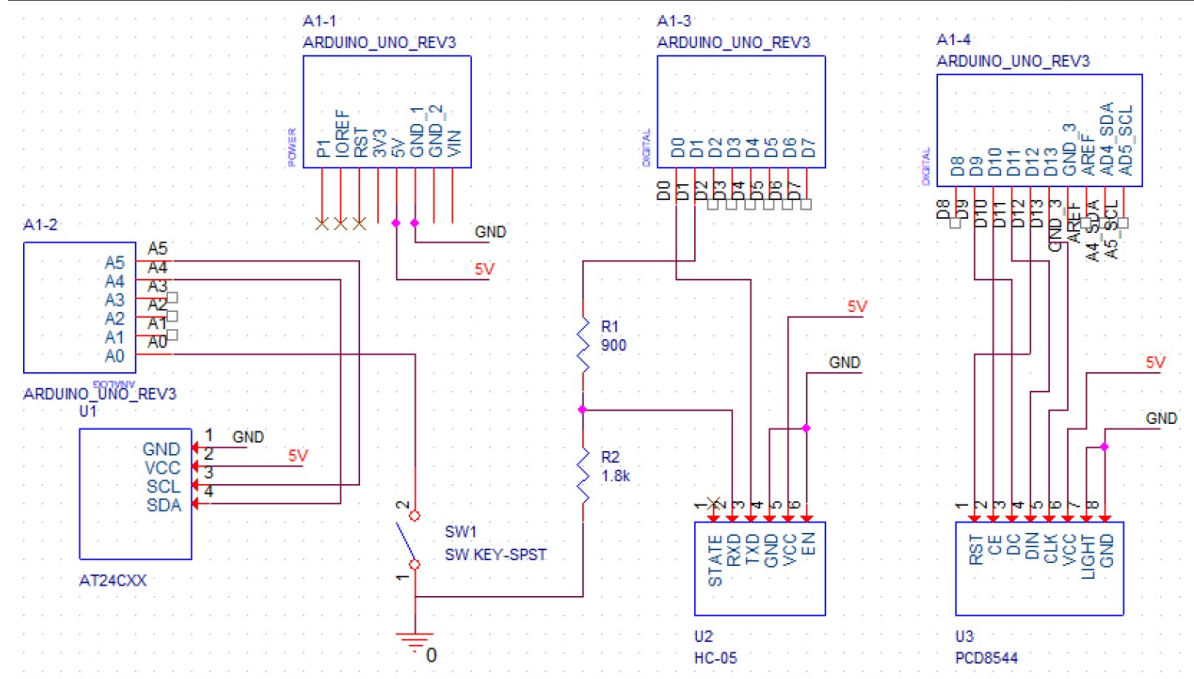
Descriere generală

Dispozitivul va functiona astfel:

- Utilizatorul se va conecta prin Bluetooth la Hardware Wallet
- Utilizatorul va genera o tranzactie, ale carei detalii le va trimite prin Bluetooth (folosind un script de interact drept demo)
- Detaliile tranzactiei vor fi afisate pe LCD timp de 10 secunde
- Pentru a accepta tranzactia, butonul va fi apasat indelung (> 1 secunda), iar device-ul va semna tranzactia si va trimite semnatura inapoi catre utilizator
- Pentru a refuza tranzactia utilizatorul va apasa butonul sub 1 secunda
- Optional, utilizatorul poate cere regenerarea cheii private, acesta primind inapoi noua cheie publica corespunzatoare

Hardware Design

Diagrama Hardware:



Lista componente:

- ATmega328p
- Modul bluetooth HC-05
- Modul LCD PCD8544
- External EEPROM AT24C256
- Buton
- Rezistori 1.8K
- Wires, breadboard

Conexiuni:

Toate componentele functioneaza pe 5V. Pentru modulul Bluetooth, care accepta 3.3V pe pinii RXD/TXD, semnalul dinspre Arduino-UNO:TX catre HC-05:RX trece printr-un divizor de tensiune 5V-3V3.

Protocoale:

- HC-05: UART
- PCD8544: SPI
- AT24C256: I2C

Software Design

Cod sursa: <https://github.com/MateiBuzdea/Hardware-Wallet>

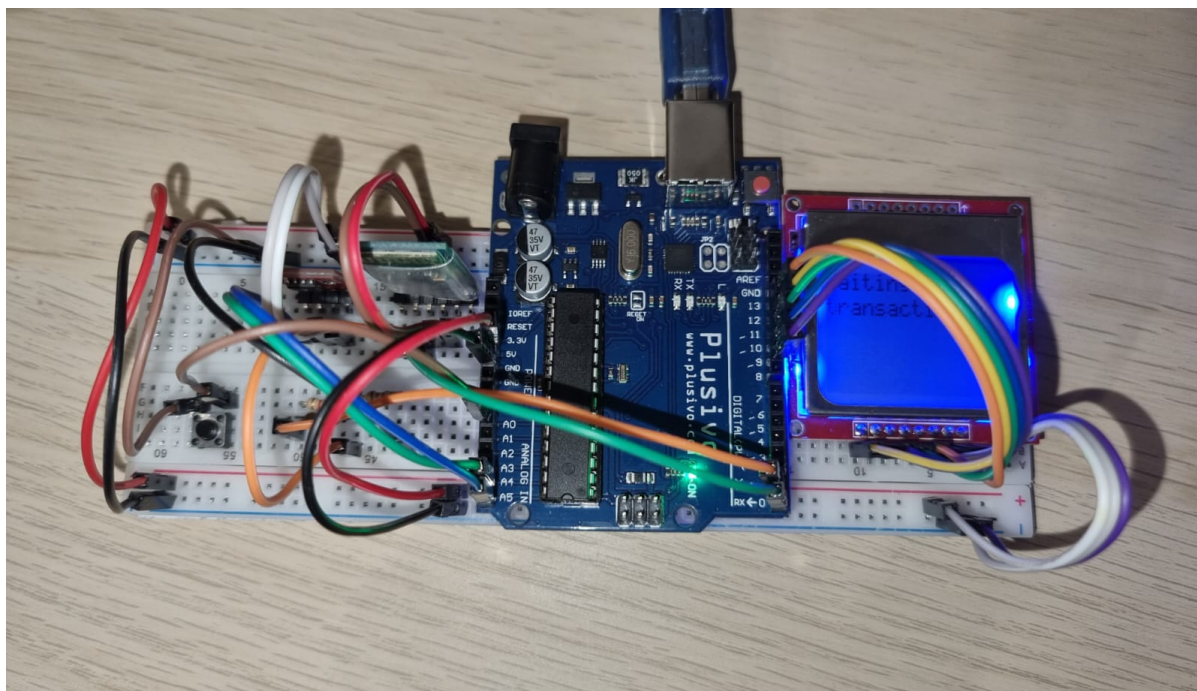
Resurse third-party:

- [AVR Nokia 5110](#)
- [Micro ECC](#)
- [AVR Crypto lib](#)

Pentru a interactiona cu Wallet-ul, se va folosi ``interact/sign.py``.

Rezultate Obținute

Dispozitivul functioneaza in parametri normali.



Concluzii

Download

O arhivă (sau mai multe dacă este cazul) cu fișierele obținute în urma realizării proiectului: surse, scheme, etc. Un fișier README, un ChangeLog, un script de compilare și copiere automată pe uC crează întotdeauna o impresie bună 😊.

Fișierele se încarcă pe wiki folosind facilitatea **Add Images or other files**. Namespace-ul în care se încarcă fișierele este de tipul **:pm:prj20??:c?** sau **:pm:prj20??:c?:nume_student** (dacă este cazul).

Exemplu: Dumitru Alin, 331CC → **:pm:prj2009:cc:dumitru_alin**.

Jurnal

Puteți avea și o secțiune de jurnal în care să poată urmări asistentul de proiect progresul proiectului.

Bibliografie/Resurse

Listă cu documente, datasheet-uri, resurse Internet folosite, eventual grupate pe **Resurse Software** și **Resurse Hardware**.

[Export to PDF](#)

From:

<http://ocw.cs.pub.ro/courses/> - **CS Open CourseWare**

Permanent link:

<http://ocw.cs.pub.ro/courses/pm/prj2025/fstancu/matei.buzdea>



Last update: **2025/05/25 21:58**