

BAB II

TINJAUAN PUSTAKA

Pembuatan *cryptocurrency cold wallet* menggunakan *microcontroller* seperti Raspberry Pi Pico 2 masih jarang dieksplorasi. Walaupun begitu, penelitian ini akan tetap dilakukan dengan mengkaji beberapa penelitian yang terkait dan masih relevan sebelumnya. Kajian ini akan berfungsi sebagai landasan dan acuan untuk menganalisis serta mengevaluasi topik penelitian yang akan dilakukan, sekaligus sebagai pembandingan dengan penelitian yang akan dilaksanakan.

Penelitian berjudul “*Creating a Physical Wallet for Cryptocurrencies*” yang dilakukan oleh Daniel Kolev, Martin Kostov, dan Fabien Kunis pada tahun 2022 mengkaji pengembangan *cryptocurrency cold wallet* sebagai solusi penyimpanan aset kripto yang aman. Dalam studi ini, Raspberry Pi Zero digunakan sebagai perangkat utama sistem, sementara *MicroSD card* dimanfaatkan sebagai media penyimpanan *private key*. Peneliti juga mengintegrasikan modul *LCD* sebagai antarmuka visual dan mengembangkan aplikasi desktop untuk memfasilitasi interaksi pengguna dengan sistem secara terstruktur dan aman [7].

Penelitian berjudul “*ColdPi – How to Make an Offline Bitcoin Cold Storage Wallet*” yang dilakukan oleh Garth Freeman pada tahun 2018 juga membahas pengembangan *cold wallet* untuk *cryptocurrency*. Dalam studi ini, Raspberry Pi Zero juga digunakan sebagai perangkat utama sistem, sementara *MicroSD card* dimanfaatkan sebagai media penyimpanan *private key*. Freeman tidak menggunakan modul *LCD* tetapi menggunakan koneksi ke monitor eksternal sebagai tampilan antarmuka dan menyediakan aplikasi desktop untuk memungkinkan interaksi pengguna dengan dompet secara aman dan offline [8].

Pendekatan yang digunakan dalam penelitian di atas memiliki beberapa kelemahan dari segi keamanan. Pertama, Raspberry Pi Zero yang digunakan merupakan *single-board computer* dengan sistem operasi *Raspbian*, yakni sistem operasi umum yang bersifat serbaguna dan tidak secara khusus dioptimalkan untuk kebutuhan keamanan kriptografis. Selain itu, perangkat tersebut terhubung langsung ke internet, yang bertentangan dengan prinsip dasar *cold wallet* yang seharusnya beroperasi sepenuhnya secara offline.

Aspek lain yang menjadi perhatian adalah integrasi antara aplikasi *desktop* dan *firmware* dalam satu perangkat, yang dapat meningkatkan resiko keamanan karena kerentanan pada salah satu komponen dapat membahayakan seluruh sistem. Terlebih lagi, Raspberry Pi Zero tidak mendukung fitur enkripsi *file system* dikarenakan limitasi *bootloader*, sehingga penyimpanan *private key* pada perangkat ini berisiko lebih tinggi apabila hardware hilang ataupun terjadi akses fisik oleh pihak yang tidak berwenang. Faktor-faktor ini secara keseluruhan dapat menurunkan tingkat keamanan dan privasi dari implementasi *cold wallet* yang diusulkan.

Penelitian berjudul “*PiTrezor: A DIY Bitcoin Hardware Wallet Based on Trezor and Raspberry Pi Zero*” yang dilakukan oleh Yannick Heneault pada tahun 2024 juga membahas pengembangan *cold wallet* untuk *cryptocurrency*. Dalam studi ini, Raspberry Pi Zero kembali digunakan sebagai perangkat utama, sementara *MicroSD card* dimanfaatkan sebagai media penyimpanan *private key*. Heneault mengintegrasikan modul *LCD* sebagai antarmuka pengguna dan menyediakan aplikasi desktop untuk berinteraksi dengan dompet secara offline [9].

Berbeda dengan penelitian sebelumnya, sistem ini dirancang agar berjalan sepenuhnya tanpa koneksi internet. Selain itu, *firmware* dan aplikasi *desktop* dipisahkan secara jelas, serta komunikasi antara perangkat dilakukan melalui koneksi *USB*, sehingga meningkatkan keamanan dari sisi arsitektur sistem.

Walaupun begitu, pendekatan ini masih memiliki kelemahan, khususnya terkait penyimpanan data. *MicroSD card* yang digunakan tidak dapat dienkripsi karena keterbatasan pada *bootloader* Raspberry Pi Zero, yang tidak mendukung enkripsi *file system*. Akibatnya, apabila perangkat hilang atau dicuri, pihak yang memperoleh akses fisik terhadap *SD card* berpotensi mengekstrak *private key* secara langsung tanpa hambatan enkripsi. Hal ini tetap menjadi risiko keamanan yang signifikan dalam konteks perlindungan aset kripto.

Berdasarkan seluruh penelitian yang telah dibahas, dapat disimpulkan bahwa masing-masing pendekatan memiliki karakteristik, keunggulan, dan keterbatasan tersendiri. Penelitian oleh Daniel, dkk. (2022) dan Freeman (2018) sama-sama menggunakan Raspberry Pi Zero sebagai inti sistem *cold wallet*, namun keduanya masih mengintegrasikan sistem operasi umum (*Raspbian*), tidak memisahkan *firmware* dari aplikasi *desktop*, dan membiarkan perangkat terhubung ke internet, yang menimbulkan risiko keamanan.

Sementara itu, penelitian oleh Heneault (2024) menunjukkan peningkatan dari sisi arsitektur keamanan, dengan pemisahan *firmware* dan aplikasi *desktop*, serta pengoperasian perangkat secara offline. Namun, kendala enkripsi pada media penyimpanan masih menjadi kelemahan utama, terutama karena *bootloader* Raspberry Pi Zero tidak mendukung enkripsi *by default*. Dengan demikian, meskipun ada kemajuan pada pendekatan Heneault, belum ada solusi yang sepenuhnya aman dalam konteks perlindungan *private key* terhadap akses fisik.

Tabel 2.1 Perbandingan Penelitian

Pembanding	Daniel Kolev, dkk. [7]	Garth Freeman [8]	Yannick Heneault [9]	Penulis (2025)*)
Judul Penelitian	<i>Creating a Physical Wallet for Cryptocurrencies</i>	<i>ColdPi – How to Make an Offline Bitcoin Cold Storage Wallet</i>	<i>PiTrezor: A DIY Bitcoin Hardware Wallet Based on Trezor and Raspberry Pi Zero</i>	Design dan Implementasi Cryptocurrency Cold Wallet berbasis Raspberry Pi Pico 2
Perangkat utama	Raspberry Pi Zero	Raspberry Pi Zero	Raspberry Pi Zero	Raspberry Pi Pico 2
Jenis perangkat	<i>Single Board Computer</i>	<i>Single Board Computer</i>	<i>Single Board Computer</i>	<i>Microcontroller</i>
Media penyimpanan	<i>MicroSD Card</i>	<i>MicroSD Card</i>	<i>MicroSD Card</i>	<i>Flash Memory Microcontroller</i>
Enkripsi penyimpanan	Tidak ada	Tidak ada	Tidak ada	Ada
Berjalan offline	Tidak	Tidak	Ya	Ya
Display utama	<i>LCD</i>	Monitor eksternal	<i>LCD</i>	Tidak ada
Aplikasi desktop	Ada	Ada	Ada	Ada
Fitur	Dapat membuat <i>wallet</i> , dapat membuat <i>address</i> , dapat melakukan dan memverifikasi transaksi, dapat me-restore <i>wallet</i> , dapat me-reset <i>wallet</i> .	Dapat membuat <i>wallet</i> , dapat membuat <i>address</i> , dapat melakukan dan memverifikasi transaksi, dapat me-restore <i>wallet</i> , dapat me-reset <i>wallet</i> .	Dapat membuat <i>wallet</i> , dapat membuat <i>address</i> , dapat melakukan dan memverifikasi transaksi, dapat me-restore <i>wallet</i> , dapat me-reset <i>wallet</i> .	Dapat membuat <i>wallet</i> , dapat membuat <i>address</i> , dapat melakukan dan memverifikasi transaksi, dapat me-restore <i>wallet</i> , dapat me-reset <i>wallet</i> .

*) Penelitian yang dilakukan

Kesimpulan dari Tabel 2.1 adalah penelitian yang sekarang dilakukan tidak menggunakan *Single Board Computer* tapi menggunakan *Microcontroller*. Dan juga media penyimpanan *private key* sudah tidak menggunakan *MicroSD Card* tapi menggunakan *Flash Memory Microcontroller*.