

BAB I

PENDAHULUAN

A. Latar Belakang

Dalam beberapa tahun terakhir, penggunaan *cryptocurrency* telah berkembang pesat sebagai bentuk aset digital yang menawarkan transparansi, desentralisasi, dan kemudahan dalam transaksi global. Berdasarkan laporan terbaru dari Crypto.com, jumlah pemilik *cryptocurrency* secara global telah mencapai 659 juta pengguna pada akhir tahun 2024, meningkat 13.0% dari 583 juta pada Januari 2024 [1]. Kapitalisasi pasar *cryptocurrency* juga mengalami lonjakan signifikan, mencapai \$3.57 triliun dengan volume perdagangan harian sebesar \$131.06 miliar pada 30 Januari 2025 [2]. Tren ini mencerminkan tingginya minat masyarakat terhadap teknologi *blockchain*, sekaligus meningkatnya kebutuhan akan solusi pengelolaan aset yang aman dan andal.

Namun, keamanan aset *cryptocurrency* masih menjadi tantangan besar. Salah satu metode penyimpanan yang umum digunakan adalah *software wallet*, yaitu dompet digital berbasis aplikasi yang memungkinkan pengguna menyimpan dan mengelola aset mereka melalui perangkat lunak. Meskipun praktis, *software wallet* memiliki kelemahan mendasar dalam aspek keamanan. Ancaman seperti serangan *malware*, *phishing*, dan kerentanan sistem operasi dapat mengekspos *private key*, yang merupakan komponen paling kritis dalam menjaga keamanan aset digital.

Beberapa insiden besar dalam beberapa tahun terakhir menunjukkan betapa rentannya *software wallet* terhadap serangan siber. Salah satu kasus yang paling mencolok adalah peretasan bursa kripto FTX pada November 2022. Dalam insiden tersebut, sekitar \$477 juta dicuri oleh peretas yang tidak teridentifikasi, hanya beberapa saat sebelum FTX

mengumumkan kebangkrutan. Para peretas berusaha menyamarkan jejak transaksi dengan mencuci dana melalui *Decentralized Exchanges (DEX)*, *cross-chain bridges*, dan *crypto mixers* [3].

Insiden serupa juga terjadi pada Binance, salah satu bursa kripto terbesar di dunia, pada Oktober 2022. Sebanyak 2 juta token BNB, dengan nilai lebih dari \$570 juta, dicuri akibat eksploitasi pada BSC Token Hub, yaitu sebuah *cross-chain bridge* yang digunakan untuk mentransfer aset antar jaringan. Setelah berhasil mengeksploitasi sistem, peretas segera mendistribusikan dana curian ke berbagai *liquidity pools* dan mengkonversinya menjadi berbagai aset kripto lain guna menyamarkan aktivitas mereka [4].

Selain masalah keamanan, privasi data juga menjadi isu penting dalam transaksi *cryptocurrency*. *Cryptocurrency* sering dianggap anonim, tetapi pada kenyataannya, sebagian besar jaringan *blockchain* hanya menawarkan *pseudonymity*, bukan *anonymity*. Ini berarti bahwa meskipun transaksi tidak terkait langsung dengan identitas pengguna, peretas dan lembaga tertentu masih dapat melacak alamat *wallet* dan menghubungkannya dengan individu melalui analisis *blockchain* [5].

Untuk mengatasi permasalahan ini, *cold wallet* menjadi solusi yang lebih aman. *Cold wallet* adalah dompet *cryptocurrency* yang beroperasi secara *offline*, sehingga *private key* disimpan dalam perangkat yang tidak terhubung langsung ke internet. Hal ini secara signifikan mengurangi risiko serangan siber. Namun, perangkat *cold wallet* komersial yang tersedia saat ini, seperti Ledger Nano X memiliki harga yang mahal, yang membuatnya sulit diakses oleh pengguna [6].

Sebagai solusi, penelitian ini bertujuan untuk merancang dan mengimplementasikan *cryptocurrency cold wallet* berbasis Raspberry Pi Pico 2. Raspberry Pi Pico 2 dipilih karena merupakan perangkat *microcontroller* yang murah, ringkas, dan fleksibel dalam pengembangan perangkat keras maupun perangkat lunak. Beberapa keunggulan Raspberry

Pi Pico 2, terutama dalam aspek yang telah disebutkan, menjadikannya pilihan yang sangat ideal untuk proyek *cold wallet*.

Dengan pendekatan ini, diharapkan *cryptocurrency cold wallet* berbasis Raspberry Pi Pico 2 dapat memberikan solusi yang lebih aman, dan privasi lebih terjamin.

B. Rumusan Masalah

Berdasarkan latar belakang diatas, dapat dirumuskan masalah sebagai berikut.

1. Bagaimana cara merancang dan mengimplementasikan *cryptocurrency cold wallet* berbasis Raspberry Pi Pico 2 agar lebih aman dan privasi lebih terjamin?
2. Bagaimana cara *cold wallet* ini dapat berinteraksi dengan jaringan blockchain tanpa membahayakan kunci privat pengguna?

C. Batasan Penelitian

Berdasarkan rumusan masalah diatas, batasan penelitian adalah sebagai berikut.

1. Penelitian ini dibatasi pada pengembangan *cryptocurrency cold wallet* berbasis Raspberry Pi Pico 2, dengan fokus pada aspek keamanan dan privasi pengguna dalam penyimpanan aset kripto.
2. *Cold wallet* yang dikembangkan hanya akan digunakan untuk penyimpanan, tanpa mencakup fitur transaksi langsung atau platform perdagangan kripto.
3. Selain itu, penelitian ini hanya akan menguji cold wallet untuk aset kripto populer yaitu Bitcoin (*TestNet4*), serta tidak mencakup penggunaan untuk aset kripto lainnya.

D. Tujuan Penelitian

Berdasarkan rumusan masalah diatas, maka tujuan penelitian ini adalah sebagai berikut.

1. Mengembangkan *cryptocurrency cold wallet* berbasis Raspberry Pi Pico 2 yang lebih aman dan privasi lebih terjamin.
2. Mengembangkan cara berinteraksi dengan jaringan *blockchain* tanpa membahayakan kunci privat pengguna.

E. Metode Penelitian

Metode penelitian yang digunakan adalah metode *waterfall*. Metode ini dianalogikan seperti air terjun karena pada setiap tahapannya dilakukan secara berurutan, dimulai dari perencanaan, pengumpulan data, desain sistem, pengembangan, uji coba, dan analisis hasil.

1. Analisis Kebutuhan Sistem

Pada tahap awal ini, akan dilakukan analisis kebutuhan sistem yang berkaitan dengan topik penelitian, seperti teknologi *blockchain*, keamanan perangkat keras, kriptografi, serta analisis penggunaan Raspberry Pi Pico 2 dalam aplikasi keamanan. Data ini digunakan sebagai dasar untuk perencanaan desain *cold wallet* yang akan dikembangkan.

2. Desain Sistem

Berdasarkan analisa kebutuhan sistem, dilakukan perancangan sistem cold wallet berbasis Raspberry Pi Pico 2. Desain ini mencakup perangkat keras yang digunakan, seperti algoritma ataupun enkripsi yang akan diterapkan sesuai dengan standar Bitcoin dan modern kriptografi. Desain perangkat lunak juga akan mencakup pembuatan antarmuka pengguna menggunakan Tauri sebagai aplikasi *desktop* untuk pengguna.

3. Pengembangan Prototipe

Pada tahap ini, prototipe *cold wallet* dibangun berdasarkan desain yang telah dibuat sebelumnya. Pengembangan dilakukan pada Raspberry

Pi Pico 2 sebagai *cold wallet*, dan perangkat lunak berbasis *desktop* untuk interaksi pengguna.

4. Uji Coba dan Pengujian Keamanan

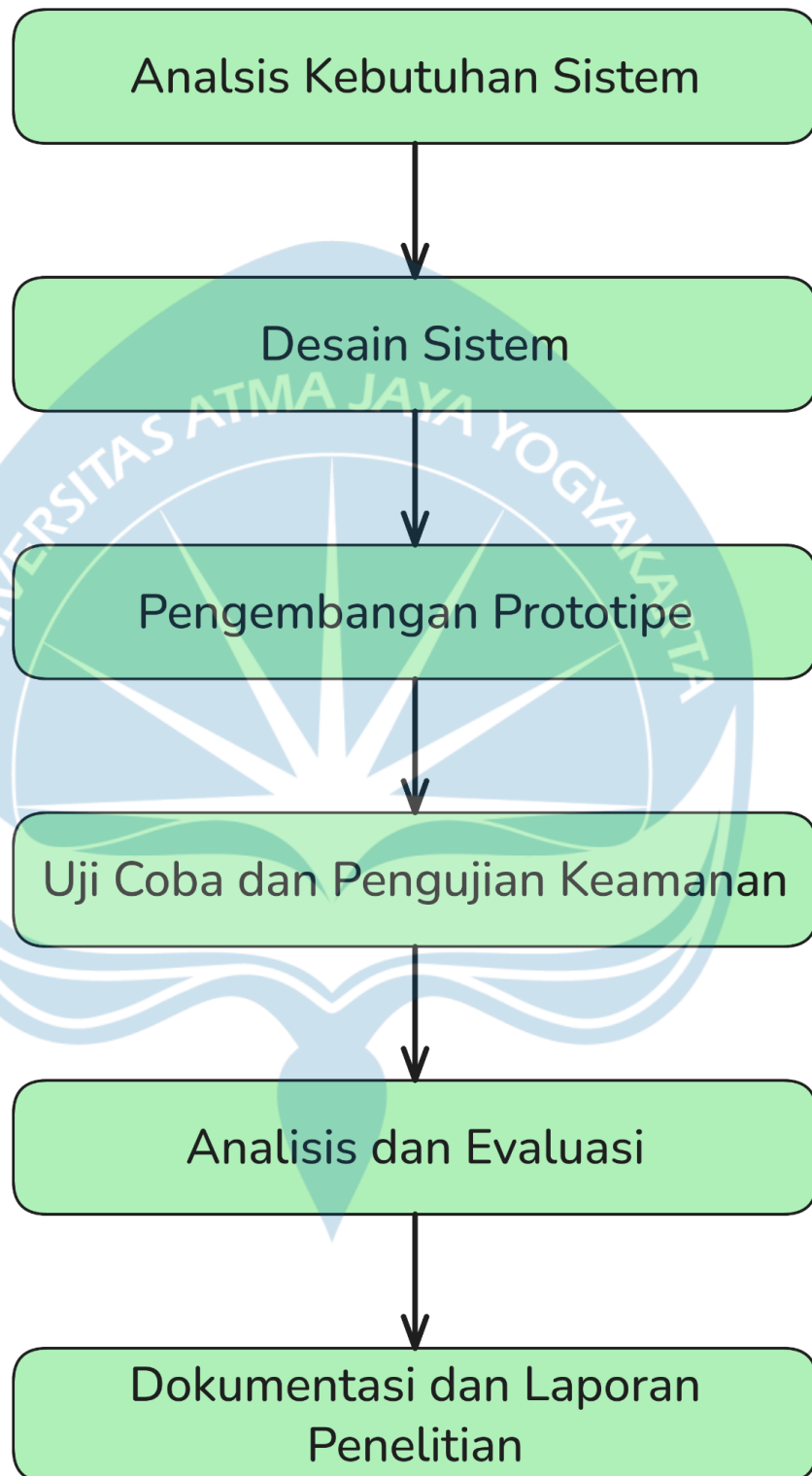
Setelah prototipe selesai, dilakukan serangkaian uji coba dan pengujian keamanan untuk memastikan bahwa *cold wallet* yang dibangun dapat berfungsi dengan baik dan aman. Pengujian ini mencakup uji fungsionalitas untuk memastikan *wallet* bekerja sesuai dengan kebutuhan, serta pengujian keamanan untuk melindungi kunci privat dan data pengguna.

5. Analisis dan Evaluasi

Tahap ini adalah melakukan analisis hasil pengujian untuk menilai keberhasilan sistem. Evaluasi dilakukan berdasarkan keamanan, efisiensi, dan pengalaman pengguna dalam menggunakan *cold wallet* berbasis Raspberry Pi Pico 2.

6. Dokumentasi dan Laporan Penelitian

Pada tahap terakhir ini, semua hasil penelitian yang telah dilakukan, termasuk desain, prototipe, pengujian, dan analisis, dikumpulkan dan disusun dalam bentuk laporan penelitian yang lengkap dan sistematis. Dokumentasi yang baik akan memastikan bahwa hasil penelitian dapat dipahami dengan jelas oleh pembaca, serta memberikan dasar yang kuat untuk pengembangan lebih lanjut.



Gambar 1.1 Metode Penelitian

F. Sistematika Penulisan

BAB 1 PENDAHULUAN

Bab ini memaparkan latar belakang, rumusan masalah, batasan masalah, tujuan, dan metode penelitian, serta sistematika penulisan.

BAB 2 TINJAUAN PUSTAKA

Bab ini membahas tentang penelitian terdahulu yang relevan dengan tema penelitian saat ini sehingga dapat dibandingkan dengan penelitian yang sedang dilakukan.

BAB 3 LANDASAN TEORI

Bab ini memaparkan teori-teori beserta penjelasannya yang menjadi landasan dalam penelitian ini.

BAB 4 ANALISIS DAN PERANCANGAN SISTEM

Bab ini menyajikan analisis sistem, menguraikan permasalahan dan solusi dalam bentuk perancangan data, arsitektur, dan antarmuka.

BAB 5 IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini menguraikan implementasi sistem dan antarmuka, serta menyajikan pengujian fungsionalitas perangkat lunak beserta hasil pengujian terhadap pengguna.