ACC sempro
Yanuar Nurdiansyah
16 Mei 2025

Acc Sempro 11 Mei 2025

Diksy M. Firmansyah

IMPLEMENTASI *SMART CONTRACT* PADA PLATFORM *CROWDFUNDING* BERBASIS BLOCKCHAIN ETHEREUM MENGGUNAKAN ALGORITMA KONSENSUS PROOF OF STAKE

PROPOSAL SKRIPSI

Diajukan sebagai salah satu syarat penelitian untuk memenuhi kelulusan program studi S1 Teknologi Informasi Fakultas Ilmu Komputer Universitas Jember

Oleh:

Muhammad Amanda Maulana Malik Ibrahim

212410102035

PROGRAM STUDI TEKNOLOGI INFORMASI

FAKULTAS ILMU KOMPUTER

UNIVERSITAS JEMBER

2025

A. Judul

Implementasi Smart Contract Pada Platform Crowdfunding Berbasis Blockchain Ethereum Menggunakan Algoritma Konsensus *Proof of Stake (PoS)*

B. Latar Belakang

Crowdfunding berasal dari kata "crowd" yang berarti keramaian atau sekelompok orang, dan "funding" yang berarti pengumpulan dana. Crowdfunding adalah metode pengumpulan dana dari banyak orang yang memiliki minat terhadap suatu kegiatan atau bisnis. Crowdfunding memberikan peluang bagi kreator untuk mendapatkan dana dari masyarakat yang tertarik dengan gagasan mereka dan menciptakan potensi untuk mempercepat pengembangan bisnis atau kegiatan yang sedang berjalan. (Aufila et al., 2024)

Sistem crowdfunding tradisional sudah memberikan fungsional dengan baik, namun masih terdapat beberapa tantangan dalam sistem terpusat, terutama terkait dengan kepercayaan dan keamanan. Funder sering kali kesulitan menentukan apakah kampanye pada platform crowdfunding benar-benar sah, funder juga bisa saja dihadapkan pada kasus penipuan, kampanye yang tidak memenuhi syarat sebagai penerima dana, dan risiko penyalahgunaan dana. Selain itu, peran perantara pihak ketiga dalam proses ini menyebabkan biaya operasional yang tinggi. (Chatkar et al., 2023)

Salah satu solusi untuk mengatasi hal ini adalah dengan menerapkan teknologi blockchain. Blockchain, sebagai teknologi desentralisasi, menawarkan tingkat keamanan dan transparansi yang tinggi. Teknologi ini berfungsi sebagai sistem pencatatan yang terdistribusi dan terdesentralisasi, di mana data disimpan dalam blok-blok yang saling terhubung dan terenkripsi serta terverifikasi oleh banyak node. Proses verifikasi ini memastikan bahwa data hampir mustahil dimanipulasi tanpa persetujuan mayoritas jaringan. Dengan demikian, blockchain menjadi solusi

potensial untuk meningkatkan kepercayaan, keamanan dan transparansi dalam sistem penggalangan dana. (Hasan et al., 2024)

Dalam era perkembangan teknologi blockchain terdapat teknologi smart contract yang bersifat objektif untuk menentukan secara spesifik bagaimana proses transaksi akan dikelola dan tindakan apa yang akan diambil ketika suatu peristiwa terjadi. Seluruh data dan transaksi dapat divalidasi secara otomatis, dan dieksekusi oleh kode dalam jaringan blockchain sebagai perjanjian digital, Kontrak ini disimpan dalam blockchain dan didistribusikan ke semua node, sehingga tidak bisa diubah, selayaknya data pada blockchain yang bersifat permanen dan transparan. (Hermawan et al., 2023)

Teknologi blockchain terus berkembang dari tahun ke tahun melalui berbagai cara, salah satunya melalui implementasi smart contract dengan berbagai konsensus tergantung pada jaringan blockchainnya salah satunya adalah *Proof of Stake* (PoS). Teknologi blockchain sebagai fundamental di balik mata uang kripto ini telah merevolusi cara pengelolaan dan pemahaman terhadap aset digital. (Julio et al., 2024)

Penelitian terdahulu yang dilakukan oleh (Baihaqsani, 2023) dengan mengimplementasikan smart contract blockchain pada sistem klaim asuransi. Peelitian ini mendapat hasil bahwa blockchain dapat meningkatkan transparansi, keamanan dan efisiensi pada proses klaim, serta mencegah manipulasi data melalui smart contract menggunakan algoritma *Proof of Work* (PoW). Penelitian lainnya yang dilakukan oleh (Sahputra, 2019) dengan mengimplementasikan smart contract pada sistem voting. Penelitian ini berhasil memastikan integritas data yang sudah di hash dan disimpan pada blockchain melalui pengecekan pada panel administrator.

Beberapa penelitian terdahulu telah membuktikan bahwa permasalahan pada data yang bersifat tetap dan transaksional seperti data asuransi dan voting terdapat

pada transparansi, dan integritas data yang semua permasalahan tersebut bisa diselesaikan menggunakan teknologi blockchain. Berdasarkan latar belakang tersebut, penulis mengusulkan untuk mengimplementasikan smart contract blockchain pada sistem crowdfunding, diharapkan sistem yang dikembangkan dapat menjamin keamanan dan transparansi data. Diharapkan penggalang dana dapat lebih mudah membangun kepercayaan dengan donator melalui transparansi penuh dalam transaksi, sementara penerima dana akan mendapatkan proses pencairan yang lebih cepat dan aman tanpa keterlibatan pihak ketiga yang kompleks.

C. Rumusan Masalah

Berdasarkan uraian latar belakang diatas maka didapatkan rumusan masalah dalam penelitian adalah sebagai berikut:

1. Bagaimana proses perancangan dan implementasi smart contract untuk platform crowdfunding berbasis blockchain Ethereum yang aman dan efisien dengan menggunakan konsensus Proof of Stake (PoS)?
2. Bagaimana mekanisme dan hasil pengujian keamanan transaksi dalam smart contract tersebut ketika digunakan pada platform crowdfunding berbasis blockchain Ethereum?

D. Tujuan Penelitian

Dengan masalah yang sudah disebutkan, tujuan dari penelitian ini yaitu:

1. Menghasilkan smart contract yang dapat menangani proses crowdfunding dan menjamin keamanan data transaksi pada aplikasi berbasis blockchain Ethereum menggunakan konsensus *Proof of Stake* (PoS)
2. Menganalisis hasil pengujian smart contract untuk memastikan keamanan dan integritas data transaksi pada aplikasi berbasis blockchain Ethereum menggunakan konsensus *Proof of Stake* (PoS)

E. Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat bagi beberapa pihak antara lain:

1. Bagi Akademisi dan peneliti

   Menambah wawasan dan pengetahuan mengenai penerapan teknologi blockchain dalam sisi keamanan data pada platform crowdfunding menggunakan algoritma Proof of Stake, serta membantu memberikan referensi penelitian lebih lanjut mengenai penerapan teknologi blockchain.

2. Bagi *Funder* dan *Fundraiser*

   Penelitian ini diharapkan memberikan wawasan yang bermanfaat bagi pemberi dana (funder) dan penerima dana (fundraiser) mengenai penerapan teknologi blockchain pada crowdfunding, sehingga funder dapat memastikan dana yang mereka berikan diterima dan dikelola dengan baik dan tidak disalahgunakan. Sedangkan fundraiser dapat membangun kepercayaan yang lebih melalui sistem yang lebih transparan dan terdesentralisasi

F. Batasan Masalah

Dalam penelitian ini, penulis memberikan beberapa Batasan masalah untuk menghindari terjadi penyimpangan selama proses penelitian dan penulisan. Beberapa Batasan masalah antara lain:

1. Penelitian tidak membahas aspek off-chain dari platform crowdfunding, meliputi manajemen pengguna dan UI/UX aplikasi.
2. Analisis smart contract mencakup aspek keamanan, fungsionalitas dan non-fungsioanlitas tanpa membandingkan dengan mekanisme crowdfunding konvensional.
3. Pengujian smart contract crowdfunding dilakukan pada jaringan testnet Sepolia Ethereum, tanpa implementasi di mainnet Ethereum.

G. Tinjauan Pustaka

G.1 Penelitian Terdahulu

Beberapa penelitian terhaulu yang berkaitan dengan penelitian penulis ini disajikan pada tabel 1 sebagai berikut:

No	Judul	Hasil	Gap	Kontribusi
1	Implementasi IPFS untuk Mengurangi Gas Fee Smart Contract Ethereum pada Aplikasi Penggalangan Dana (Hutomo Sakti Kartiko, 2023)	Penelitian ini menjelaskan bagaimana cara optimalisasi Gas fee dan memori di blockchain menggunakan *Interplanetary File System* (IPFS) pada *Proof of Work*. Hasil dari penelitian ini menunjukkan penggunaan IPFS dapat menurunkan biaya *Gas fee* rata-rata sebesar 94.39%, meskipun kecepatan transaksi sedikit meningkat sebesar 13.55%.	Menggunakan algoritma consensus yaitu *Proof of Work.* Penelitian berfokus pada penggunaan Interplanetary File System (IPFS) untuk efisiensi *Gas fee* dan memori. Penelitian ini juga berfokus pada sistem yang spesifik yakni penggalangan dana dengan penggunaan IPFS	Memberikan wawasan tentang penggunaan Interplanetary File System (IPFS) untuk efisiensi *Gas fee* smart contract. Penelitian menunjukkan cara Interplanetary File System (IPFS) sebagai penyimpanan terdesentrasisasi pada aplikasi penggalangan dana dan memberikan penjelasan mengenai hasil efisiensi *Gas fee* transaksi yang lebih sedikit pada algoritma consensus *Proof of Work*
2	Implementasi Teknologi Blockchain Dengan Sistem Smart Contract Pada Klaim Asuransi (Baihaqsani, 2023)	Penelitian ini menjelaskan bagaimana mengimplementasikan blockchain pada sistem klaim asuransi dengan menggunakan *Proof of Work*. Hasil penelitian ini menunjukkan blockchain dapat menjamin integritas dan ketetapan data menggunakan smart contract yang berjalan diatas Jaringan Ethereum	Berfokus untuk implementasi blockchain pada klaim asuransi. Penelitian menggunakan algoritma consensus Proof of Work untuk menjamin integritas data. Dan mempelajari bagaimana blockchain menjamin integritas data	Memberikan wawasan tentang implementasi blockchain pada sistem klaim asuransi dan memberikan gambaran tentang penggunaan blockchain pada suatu organisasi yang memiliki regulasi

			pada klaim asuransi	
3	The Privacy Protection Mechanism of Hyperledger Fabric and Its Application in Supply Chain Finance (Chaoqun Ma, 2019)	Penelitian ini menjelaskan bahwa blockchain mulai banyak digunakan di berbagai bidang keuangan, salah satunya pada supply chain finance yang membutuhkan privasi khusus. Hasil penelitian menunjukkan bahwa mekanisme Hyperledger Fabric mampu mengakomodasi kebutuhan keamanan dalam jaringan blockchain pada kasus supply chain finance.	Berfokus pada penerapan mekanisme *Hyperledger Fabric*. Penelitian lebih banyak membahas mengenai mekanisme keamanan Penggunaan mekanisme *Hyperledger Fabric* pada platform *permissioned*	Memberikan wawasan tentang implementasi blockchain pada sistem klaim asuransi. Dan memberikan gambaran tentang penggunaan blockchain pada suatu organisasi yang memiliki regulasi
4	Blockchain Without Waste: Proof-of-Stake (Saleh, 2020)	Hasil penelitian ini menunjukkan bahwa Proof of Stake dapat menciptakan blockchain *permissionless* yang efektif tanpa mengandalkan konsumsi yang tinggi dengan memberlakukan ambang batas minim bagi *validator* atau menetapkan jadwal pemberian imbalan blok atas pembaruan blockchain dengan block-block baru	Berfokus mempelajari dan mengembangkan algoritma *Proof of Stake*. Penelitian menjelaskan beberapa desain jaringan blockchain menggunakan algoritma *Proof of Stake*	Memberikan wawasan penggunaan teknologi blockchain melalui pendekatan algoritma konsensus *Proof of Stake*. Memberikan wawasan desain jaringan pada algoritma *Proof of Stake* yang bisa di kembangkan

Sumber: Diolah oleh peneliti 2024

Berdasarkan penelitian terdahulu yang sudah dilakukan, mendapatkan hasil bahwa teknologi blockchain dapat digunakan untuk menjaga keamanan dan integritas dari data yang disimpan. Menyelesaikan masalah yang

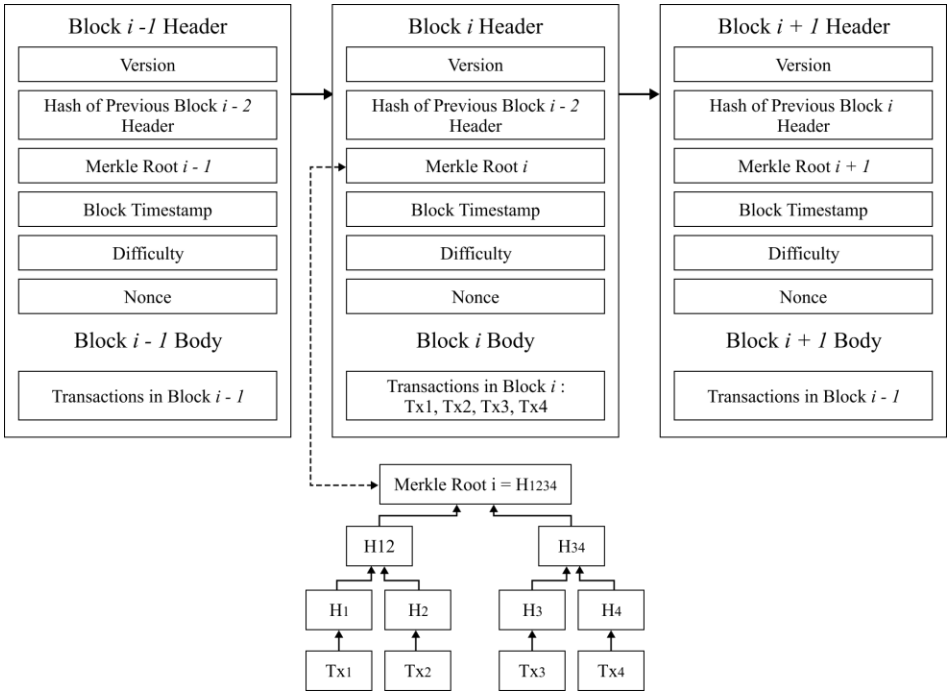
berhubungan dengan kepercayaan, mengurangi campur tangan pihak ke tiga terkait dengan mininimalkan penggunaan biaya operasional. penggunaan blokcahin terbukti efisien karena dapat menjamin integritas dan ketetapan data menggunakan smart contract yang berjalan diatas Jaringan Ethereum pada klaim asuransi (Baihaqsani, 2023).

Penggunaan blockchain pada *finance supply chain* juga efektif untuk menjaga keamanan data menggunakan desain private blockchain *Hyperledger Fabric* (Chaoqun Ma, 2019). Pada penelitian (Hutomo Sakti Kartiko, 2023), juga menunjukkan bahwa penggunaan blockhain pada sistem crowdfunding, khususnya algoritma *Proof of Work* memakan memori dan daya yang besar sehingga perlu proses efisiensi menggunakan Interplanetary File System (IPFS). Pada penelitian yang dilakukan oleh (Saleh, 2020), menjelaskan bahwa algoritma konsensus proof of stake lebih efisien untuk transaksi yang bersifat kompleks. Oleh karena itu pada penelitian ini, memilih Ethereum yang sudah menggunakan konsensus *Proof of Stake* akan digunakan pada jaringan blockchain crowdfunding.

G.2 Blockchain

Blockchain adalah teknologi terdesentralisasi yang memungkinkan penyimpanan data secara aman, transparan, dan tidak dapat diubah melalui jaringan yang tersebar atau terdesentralisasi. Dalam blockchain, data disimpan dalam buku besar terdistribusi. Teknologi blockchain menyediakan integritas dan ketersediaan yang memungkinkan pengguna dalam jaringan blockchain untuk menulis, membaca, dan memverifikasi transaksi yang tercatat dalam buku besar terdistribusi. Namun, teknologi ini tidak memungkinkan penghapusan atau modifikasi terhadap transaksi dan informasi lain yang tersimpan di buku besar tersebut. Sistem blockchain didukung dan diamankan oleh elemen-elemen kriptografi dan enkripsi, seperti tanda tangan digital, fungsi hash, dan sebagainya. Elemen-elemen ini menjamin bahwa transaksi

yang dicatat dalam buku besar dilindungi integritasnya, diverifikasi keasliannya, dan tidak dapat diubah (Huaqun Guo, 2022)



Gambar G.1 Struktur Blockchain

Pada struktur blockchain di pisah menjadi dua bagian yaitu block header dan block body, block header berisi mengenai metadata block yang terdiri dari beberapa bagian yakni:

Bagian Header Block:

a. Version: Versi blockchain
b. Hash of Previous Block: Hash dari header block sebelumnya
c. Merkle Root: Hash dari semua transaksi dalam block
d. Timestamp: Waktu pembuatan block
e. Difficulty: Tingkat kesulitan untuk menambang di block ini
f. Nonce: Nilai yang diubah selama proses penambangan untuk menemukan hash yang sesuai

Sedangkan pada bagian block body berisi semua data transaksi yang sudah terenkripsi di dalam block tersebut.

G.3 Smart Contract

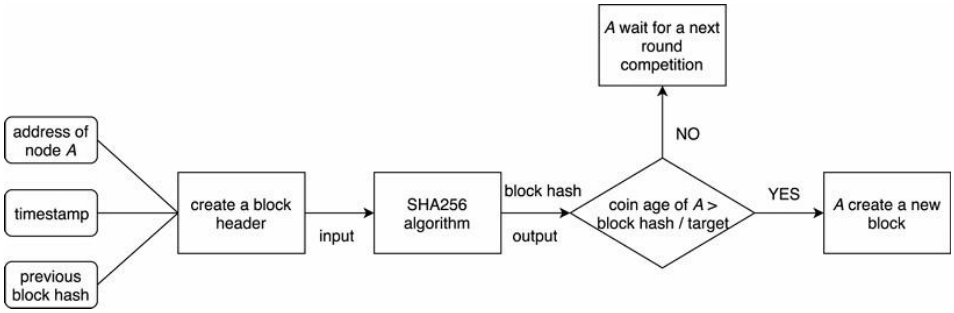
Smart contract adalah program yang berjalan di atas blockchain yang secara otomatis mengeksekusi, mengelola, atau mendokumentasikan peristiwa sesuai dengan syarat dan ketentuan yang telah diprogramkan. Smart contract memungkinkan pelaksanaan kode yang objektif dalam mengatur proses secara otomatis. Salah satu tujuan utama pengembangan smart contract di Ethereum adalah mengatasi keterbatasan Bitcoin. Smart contract menawarkan otonomi, efisiensi, akurasi, serta penghematan biaya, tanpa memerlukan perantara. Selain itu, smart contract tidak harus melibatkan dua pihak atau bersifat mengikat secara hukum (Huaqun Guo, 2022)

G.4 Konsensus Proof of Stake

Algorima konsensus adalah algoritma yang berfungsi sebagai mekanisme utama pada jaringan blockhain yang bertugas untuk mencapai kesepakatan pada smart contract di dalam jaringan blockchain. Konsensus berjalan dengan memanfaatkan sumberdaya mayoritas pengguna untuk menjaga integritas sistem. Konsensus memastikan bahwa transaksi yang dicatat di blockchain tidak berbahaya, tidak duplikat dan tidak double spending. Mekanisme konsensus menjadi inti dari seluruh kegiatan di blockchain,

Algoritma konsensus proof of Stake (PoS) dikembangkan untuk mengatasi konsumsi daya yang besar pada Proof of Work (PoW). Dalam Proof of Stake pengguna tidak perlu memecahkan masalah matematika untuk mencapai konsensus (nonce), melainkan cukup menggunakan beberapa cryptocurrency untuk di taruhkan (Staking). Pencipta blok baru dipilih secara acak dari uang pengguna yang telah melakukan staking, tanpa seorang pun dapat memprediksi gilirannya. Sistem ini mengurangi pemborosan sumber daya PoW dan mendorong pemegang koin untuk meningkatkan waktu

penyimpanan, yang meningkatkan keamanan blockchain. (Jannah Yusoff, 2022)



Gambar G.2 Alur Algoritma Proof of Stake

G.5 Kriptografi

Kriptografi adalah seni dan ilmu yang digunakan untuk menyembunyikan pesan, dengan tujuan menjaga kerahasiaan informasi. Pesan yang belum dienkripsi disebut plaintext, sedangkan setelah proses enkripsi, pesan tersebut menjadi ciphertext. Kriptografi mempelajari dan menerapkan teknik komunikasi yang aman dari ancaman pihak ketiga.

Komunikasi yang aman memastikan bahwa pesan atau data yang ditransfer antara dua pihak tidak dapat diakses oleh pihak lawan. Dalam dunia kriptografi, lawan adalah entitas yang berusaha mendapatkan informasi berharga dan merusak prinsip-prinsip keamanan. Kerahasiaan data, integritas data, autentikasi, dan non-repudiasi adalah prinsip dasar dalam kriptografi modern. Kekuatan kriptografi diukur dari waktu dan sumber daya yang diperlukan untuk mengembalikan plaintext. Hasil dari kriptografi yang kuat adalah ciphertext yang sangat sulit dipecahkan tanpa alat dekripsi yang tepat, bahkan dengan semua kekuatan komputasi yang ada saat ini (Archana B U, 2023)

G.6 Ethereum

Ethereum adalah cryptocurrency terbesar kedua berdasarkan kapitalisasi pasar. Platform ini merupakan sistem komputasi terdistribusi *open source* yang dirancang untuk mendukung *smart contract*, memungkinkan pengembang membangun aplikasi terdesentralisasi dengan mudah dengan tekbologi blockchain. Berbeda dengan Bitcoin yang hanya mencatat transaksi antar alamat, blockchain Ethereum juga menyimpan alamat dengan kode yang dapat dijalankan oleh Ethereum Virtual Machine (EVM).

Transaksi pada blockchain Ethereum mencakup data input untuk program yang kemudian diproses oleh EVM menggunakan bahasa pemrograman yang sesuai. Dasar utama dari sistem Ethereum adalah akun, yang diperlukan untuk mengirimkan transaksi. Terdapat dua jenis akun di Ethereum: Akun yang Dimiliki Secara Eksternal (*Externally Owned Accounts/EOA*), yang digunakan langsung oleh pengguna untuk transaksi, dan Akun Kontrak (*Contract Accounts*), yang memungkinkan interaksi dengan kontrak lain serta transaksi internal. Setiap akun memiliki pasangan kunci, yaitu kunci pribadi dan kunci publik. Pemahaman mengenai perbedaan antara kunci pribadi, transaksi, pengirim, serta penggunaan nilai hash sangat penting untuk melacak transaksi di blockchain. (Dzulfikar & Susanto, 2020)

G.7 Decentralized App (Dapps)

Decentralized App atau Dapps adalah program berbasis blockchain yang berjalan pada infrastruktur jaringan *peer-to-peer*, terdesentralisasi dan tidak terpusat pada suatu pihak manapun. Jaringan peer-to-peer adalah jaringan di mana dua pengguna berinteraksi atau berbagi informasi tanpa intervensi pihak pusat. Dalam Dapps semua data transaksi dilindungi dengan kriptografi yang berfungsi untuk mengamankan komunikasi anatara dua block dari sumber pihak ketiga. Dapps umumnya menggunakan uang kripto internal sebagai pendorong utama ekosistemnya dan telah diterapkan dalam berbagai bidang, seperti energi, asuransi, dan keuangan. Perbandingan antara aplikasi blockchain

terpusat dan terdesentralisasi menunjukkan perbedaan signifikan dalam keamanan data. Berikut ini adalah beberapa perbedaan dari *centralized app* (Apps) dan Dapps. (Raza et al., 2024)

Centralized App	Decentralized App
Apps beroperasi menggunakan sebuah arsitektur *client-server*	Dapps menggunakan smart contract untuk berinteraksi dengan *client*
Database pengguna dapat diakses dan terhubung pada backend server	Menggunakan jaringan peer-to-peer pada backend
Membutuhkan arahan dari superadmin (pusat) untuk menetapkan *role* dan *permission*	Tidak ada arahan dari pihak superadmin (pusat)
Kerentanan terhadap keamanan dan privasi	Aman, Tidak tapat diubah dan dapat diatur secara mandiri

Tabel 2. Perbandingan Centralized App dan Decentralized App

G.8 Thirdweb

Thirdweb merupakan sebuah *tools* dan *utility* yang cukup lengkap untuk membatu para developer Web3/Dapps untuk berinteraksi dengan berbagai jaringan blockchain, seperti Ethereum yang langsung dari proyek Javascript. Tools ini menyediakan integrasi fitur blockchain ke aplikasi front-end menjadi lebih mudah (Kolomoyets & Kynash, 2023).

G.9 Hardhat JS

Hardhat adalah framework berbasis Node.js yang dikembangkan oleh Nomic Fundation yang memilii banyak fitur, seperti dukungan pengembangan, pengujian menggunakan Javascript dan juga proses deploy smart contract. Hardhat memiliki kelebihan yang sangat fleksibel dan bisa dikonfigurasi sesuai dengan kebutuhan. Para pengembang bisa mengatur berbagai bagian dari siklus pengembangan proyek, sehingga memiliki kontrol yang detail terhadap bagaimana framework ini (Helms & McGahon, 2023).

G.10 Mythril

Mythril adalah salah satu framework paling matang untuk analisis *smart contract* di blockchain yang dirancang khusus untukEthereum Virtual Machine (EVM). Mythril menggunakan teknik *symbolic execution*, yaitu teknik yang mengevaluasi perilaku program dengan menggunakan input simbolik (bukan

nilai tetap) untuk menelusuri semua kemungkinan eksekusi kerentanan dalam kontrak pintar. Mythril lebih unggul dibandingkan dengan analisis statis ringan (*lightweight static analysis*), Mythril cenderung menghasilkan lebih sedikit *alert*, tetapi mampu menunjukkan kemungkinan nyata dari serangan yang teridentifikasi (Bonomi et al., 2023).

H. Metodologi Penelitian

Bagian ini mencakup informasi mengenai jenis penelitian, objek yang diteliti, lokasi, serta tahapan yang dilakukan selama penelitian. Selain itu, tahapan dalam proses pengumpulan data atau informasi yang digunakan untuk menyelesaikan penelitian ini juga dijelaskan secara rinci di bagian ini.

H.1 Jenis Penelitian

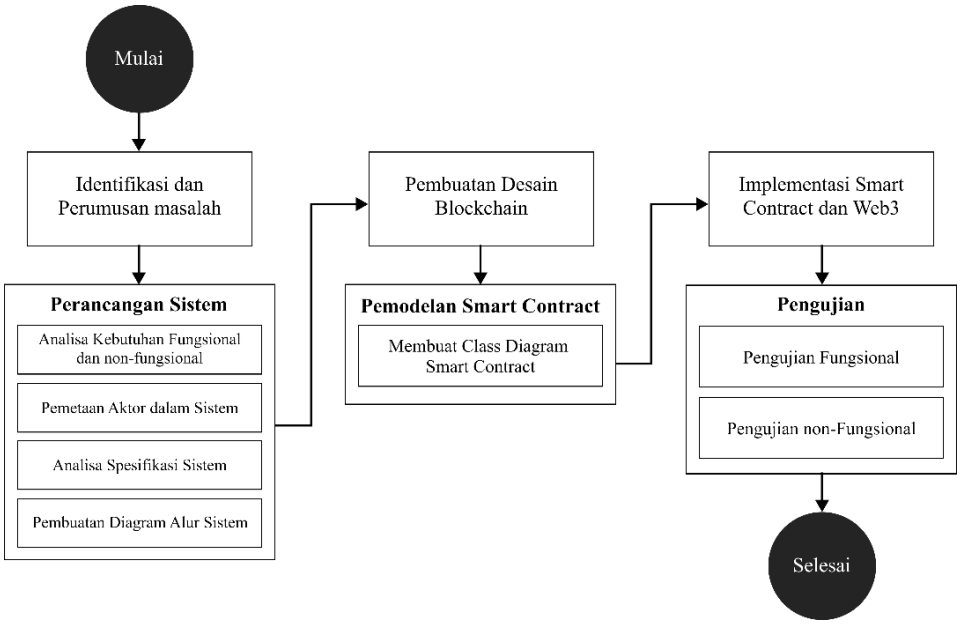
Metode dalam penelitian ini merupakan penelitian pengembangan (RnD). Penelitian pengembangan diawali dengan proses analisis terhadap permasalahan yang diidentifikasi dan diatasi dengan mengembangkan sebuah model atau produk. Produk atau model yang dikembangkan dirancang untuk menjawab permasalahan yang ada. (Maruwu, 2024).

H.2 Objek Penelitian

Objek dari penelitian ini adalah smart contract yang nantinya akan di deploy pada jaringan blockchain dan konsensus *Proof of Stake*. Smart contract yang dihasilkan kemudian akan digunakan untuk menangani proses transaksi pada platform crowdfunding.

H.3. Tahapan Penelitian

Pada bagian ini berisi tahapan yang dilakukan peneliti selama penelitian berlangsung, berikut beberpa tahapan penelitian ditunukkan pada gambar G.5.



Gambar G.5 Tahapan penelitian

H.3.1 Identifikasi dan Perumusan Masalah

Identifikasi masalah dilakukan melalui pencarian berita, kejadian di lingkungan sekitar dan di internet untuk mengetahui permasalahan yang terjadi. Berdasarkan beberapa kasus yang ditemukan, seperti dugaan penyelewengan dana oleh Yayasan Rumah Penghafal Qur'an (RFPS) pada tahun 2022, pengelola dana terduga hanya menyalurkan sebagian kecil dana donasi berkisar antara Rp 300.000 (tiga ratus ribu rupiah) hingga Rp 50.000.000 (lima puluh juta rupiah) dari total donasi RP 1,6 miliar (jawapos.com, 2022). Terdapat juga kasus lembaga filantropi Aksi Cepat Tanggap (ACT) yang memotong dana donasi secara tidak transparan untuk kepentingan operasional dan kepentingan pribadi pengelola dana seperti membeli rumah dan perabotnya, serta menerima gaji dan fasilitas lainnya dengan nilai ratusan juta rupiah (tempo.co, 2022).

Hal tersebut menimbulkan krisis kepercayaan pada pengelola dana pihak ketiga, sehingga para donator kesulitan untuk memilih proyek yang sah (Gada, 2021). Sistem penggalangan dana yang tersentralisasi menyebabkan

ketergantungan pada pihak ketiga untuk evaluasi dan pengelolaan risiko, sehingga mengurangi desentralisasi dan mengingkatkan kemungkinan kesalahan atau kolusi dalam proyek. Ketergantungan pihak ke tiga juga menyebabkan biaya layanan yang tinggi (Xu, 2023). Selanjutnya, peneliti melakukan kajian literatur terkait untuk mengatasi masalah. Kajian lieteratur berupa artikel ilmiah, buku, jurnal atau website yang membahas seputar smart contract, blockchain dan implementasinya. Dengan memanfaatkan blockchain, seluruh transaksi donasi dapat dicatat secara transparan dan tidak dapat dimanipulasi.

H.3.2 Perancangan Sistem

Pada tahap ini akan dilakukan proses perancangan sistem berbasis blockchain Ethereum. Perancangan sistem dimulai dengan melakukan analisa kebutuhan fungsional dan kebutuhan non-fungsional, analisa pemetaan aktor dalam sistem, analisa spesifikasi sistem dan pembuatan alur sistem. Analisa kebutuhan fungsional dan non-fungsional meliputi identifikasi fitur utama yang harus dimiliki oleh sistem agar dapat beroperasi sesuai dengan tujuan yang telah di tentukan dengan melakukan observasi pada platform penggalangan online sejenis yang sudah ada.

Kebutuhan fungsional mencakup proses pengiriman Ether dari pengirim ke penerima melalui smart contract, pencatatan transaksi crowdfunding dan proses staking pada blockhain, serta mekanisme pembagian dan penarikan reward. Sementara itu, kebutuhan non-fungsional mencakup aspek teknis seperti terdesentralisasi sistem, transparansi transaksi, dan interaksi smart contract dengan user dan jaringan blockchain. Berdasarkan observasi didapatkan kebutuhan fungsional dan non-fungsional sistem dengan penyesuaian sebagai berikut:

Kebutuhan Fungsional	Kebutuhan non-Fungsional
User dapat mengirimkan Ether ke smart contract	Menggunakan smart contract untuk berinteraksi dengan jaringan blockchain
Smart contract mencatat transaksi donasi pada blockchain	Sistem dibuat terdesentralisasi atau tanpa perantara pihak ke tiga

User dapat mengambil staking token untuk melakukan staking	Smart contract mencatat transaksi crowdfunding dan staking pada blockchain
User dapat melakukan penarikan reward setelah melakukan staking	Transaksi pada blockchain dapat di lacak transparansinya

Tabel 3. Kebutuhan fungsional dan non-fungsional

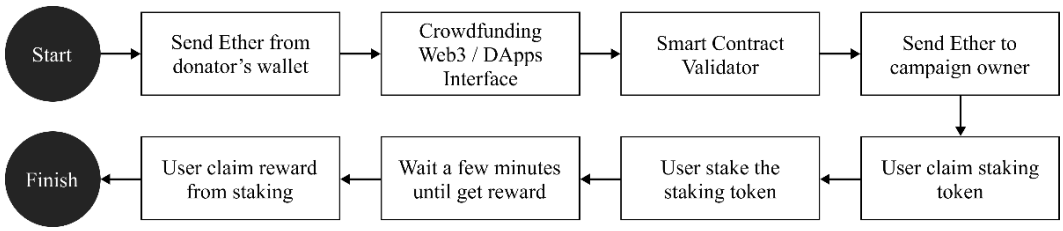
Analisa pemetaan aktor dalam sistem mencakup identifikasi aktor yang terlibat pada penggunaan sistem crowdfunding, meliputi campaign owner, donator/backer/funder, smart contract blockhain dan web3 interface. Analisa spesifikasi sistem meliputi teknologi dan tools apa saja yang nantinya akan digunakan untuk membangun aplikasi berbasis blockchain yang terdesentralisasi, meliputi bahasa pemrograman yang digunakan untuk smart contract dan frontend, jenis blockchain dan konsensus yang digunakan, library yang digunakan untuk integrasi, dan platform Ethereum Virtual Machine (EVM) yang nantinya digunakan untuk debugging smart contract dan deploy smart contract. berikut ini adalah hasil analisa spesifikasi sistem dan tools yang digunakan.

Komponen	Tools dan Teknologi
Blockchain	Ethereum (Sepolia Ethereum Testnet)
Konsensus	Ethereum (Proof of Stake)
Bahasa Smart Contract	Solidity
Provider EVM	Remix, Thirdweb
Library Web3	Ethers JS, Thirdweb Provider
Frontend	React JS
Backend	Ethereum (Sepolia Ethereum Testnet)

Tabel 4. Tools dan teknologi yang digunakan

Pada sistem yang akan dibuat, pemiliki kampanye akan membuka kampanye pada aplikasi yang nantinya bisa menerima donasi dari donator. Para donator akan mengirim Ether dari wallet kripto mereka lewat interface aplikasi, Ether yang didonasikan tidak langsung dikirim ke wallet pemilik kampanye, namun akan di terima oleh smart contract untuk divalidasi dan dicatat pada blockchain. Ether yang didonasikan secara otomatis akan dikirim oleh smart contract ke pemilik kampanye

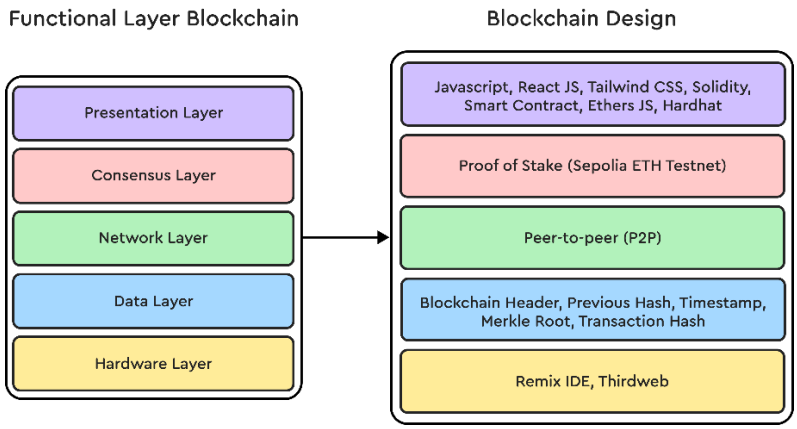
jika sudah divalidasi. User bisa melakukan klaim staking token untuk menaruhkan token mereka dan nantinya akan mendapat reward. Berikut ini adalah alur transaksi pada aplikasi crowdfunding.



Gambar G.6 Alur transaksi web3 crowdfunding

H.3.3 Pembuatan Desain Blockchain

Pembuatan desain blockchain dilakukan dilakuakan berdasarkan analisa spesifikasi sistem dan jaringan blockchain yang dipilih, dengan mempertimbangkan setiap layer dalam arsitektur blockchain untuk memastikan integritas yang optimal antara smart contract, konsensus dan infrastruktur jaringan. Setiap layer memiliki peran masing-masing, seperti Presentation Layer yang bertanggung jawab atas tampilan antarmuka pengguna menggunakan bahasa pembangun website, serta interaksi dengan smart contract melalui library Ethers JS. Consensus Layer mengadopsi *Proof of Stake* (PoS) pada jaringan blockchain Sepolia ETH untuk memvalidasi transaksi, sementara Network Layer menggunakan mode Peer-to-Peer (P2P) untuk komunikasi antar node dalam jaringan, dan Data Layer yang memastikan keamanan dan validitas data transaksi yang disimpan dengan menerapkan Transaction Hash, Hash Algorithm dan pencatatan data transaksi. Berikut ini adalah desain blockchain yang akan digunakan berdasarkan layer fungsional pada blockchain.



Gambar G.7 Desain blockchain layer

H.3.4 Pemodelan Smart Contract

Pada tahap ini dilakukan pemodelan smart contract yang akan digunakan nantinya. Pemodelan dilakukan dengan menentukan kontrak apa saja yang akan digunakan pada aplikasi crowdfunding. Berdasarkan alur sistem yang sudah dibuat didapatkan smart contract yang akan digunakan sebagai berikut.

Kontrak	Keterangan
Crowdfunding Contract	Kontrak yang digunakan untuk menangani proses penggalangan dana dan penyaluran dana dari donator ke pemilik kampanye.
Token Drop Contract	Kontrak yang akan digunakan untuk proses klaim staking token yang nantinya digunakan pada proses staking.
Staking Token dan Reward Token Contract	Kontrak yang digunakan untuk membuat token staking dan token reward.
Staking Contract	Kontrak yang digunakan untuk menangani proses staking, perhitungan reward token dan distribusi reward.

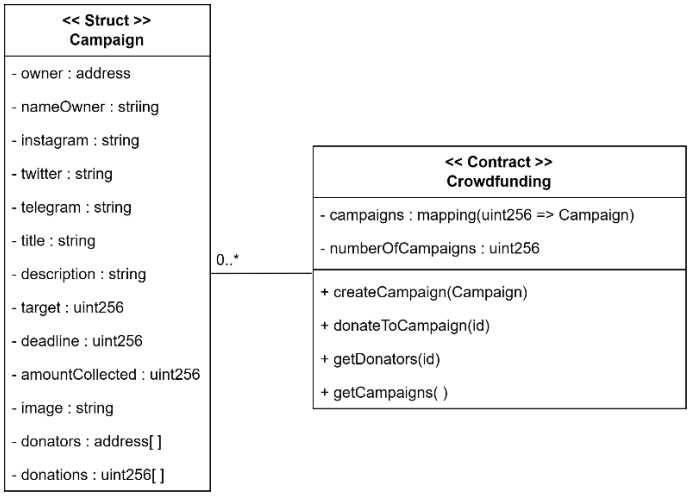
Tabel 5. Nama kontrak dan keterangan kontrak

Untuk lebih memudahkan proses implementasi, pemodelan smart contract juga akan menggunakan Class Diagram untuk menetapkan atribut dan method dari ssetiap kontrak. Atribut dan method akan didefinisikan pada diagram dan akan dijelaskan maksud dan tujuannya. Pada tahap ini juga dilakukan pembuatan proses staking. Staking adalah bagian yang paling populer dari konsensus *Proof of Stake*

(PoS), dimana para user bisa menaruhkan token mereka dalam periode waktu tertentu dan akan mendapat reward berdasarkan token yang mereka staking. Pemodelan spesifikasi smart contract dan class diagram adalah sebagai berikut:

1. Kontrak Crowdfunding
    a. Membuat dan menyimpan data kampanye
    b. Mengambil data kampanye
    c. Mengambil data donator dan ether
    d. Mengirim Ether dari donator ke pemilik kampanye

    Detail dari struktur data kontrak crowdfunding adalah sebagai berikut:



Gambar G.8 Class Diagram Kontrak Crowdfunding

Berikut ini penjelasan dari class diagram kontrak crowdfunding diatas:

Nama	Struct Campaign
Dekripsi	Mendefinisikan struktur dari data campaign
Atribut	owner, nameOwner, instagram, twitter, telegram, title, description, target, deadline, amountCollected, image, donators, donations

Tabel 6. Keterangan Struktur Campaign

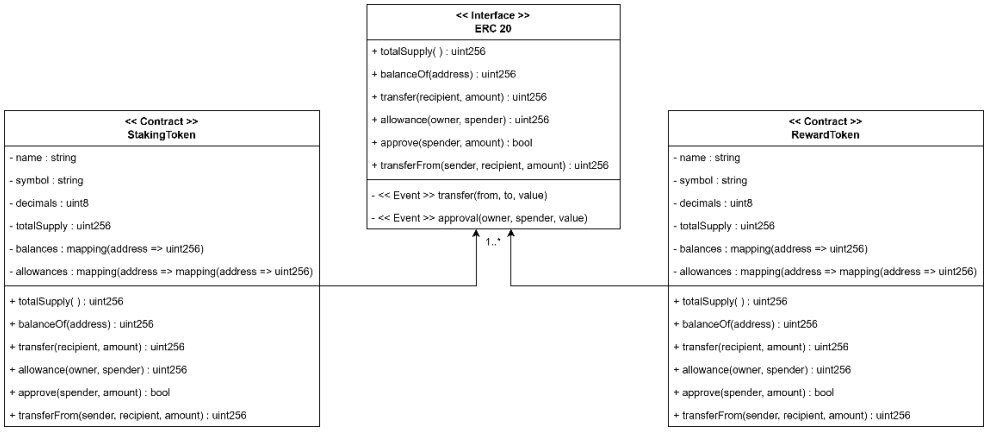
Nama	Crowdfunding Contract

Dekripsi	Kontrak yang mengatur transaksi ether pada crowdfunding	
Atribut	campaigns, numberOfCampaign	
Method	createCampaign(Campaign)	Method untuk membuat campaign dengan parameter struct dari campaign
	donateToCampaign(id)	Method untuk mengirim ether ke campaign tertentu
	getDonators(id)	Method untuk mengambil data donator dan jumlah ether yang mereka donasikan
	getCampaigns()	Method untuk mengambil data semua campaign untuk di tampilkan

Tabel 7. Keterangan Kontrak Campaign

2. Kontrak Staking Token dan Reward Token
   a. Melakukan persetujuan alamat
   b. Mengirim ether ke alamat yang disetujui

   Detail dari struktur kontrak token staking dan token reward adalah sebagai berikut:



Gambar G.9 Class Diagram Staking Token dan Reward Token

Berikut ini penjelasan dari class diagram kontrak kedua token diatas:

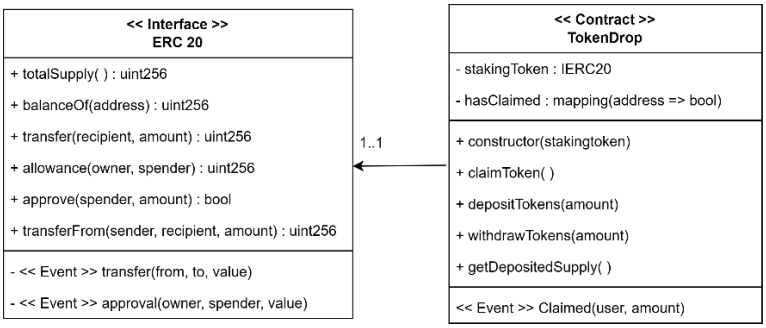
Nama	Staking Token Contract dan Reward Token Contract

Dekripsi	Kontrak yang digunakan untuk membuat token staking dan reward yang mengimplementasikan standard interface dari ERC20	
Atribut	name, symbol, decimals, totalSupply, balances, allowances	
Method	totalSupply()	Method untuk inisiasi total jumlah pasokan token staking dan reward
	balanceOf(address)	Method untuk melihat saldo dari alamat wallet tertentu
	transfer(recipient, amount)	Method untuk melakukan transfer ke alamat dompet dengan jumlah token tertentu
	allowance(owner, spender)	Method untuk melakukan persetujuan pihak ketiga menggunakan token pengguna
	approve(spender, amount)	Method untuk melakukan persetujuan ke alamat pengirim dengan jumlah token tertentu
	transferFrom(sender, recipient, amount)	Method untuk memindahkan token dari alamat pengirim ke penerima dengan jumlah token tertenu

Tabel 8. Keterangan Kontrak Staking Token dan Reward Token

3. Kontrak Token Drop
   a. Menerima deposit token
   b. Mengirim token ke alamat tertentu

   Detail dari struktur token drop adalah sebagai berikut:s



Gambar G.10 Class Diagram Kontrak Token Drop

Berikut ini penjelasan dari class diagram kontrak kedua token diatas:

Nama	Token Drop Contract	
Dekripsi	Kontrak yang mengatur proses klaim token staking	
Atribut	stakingToken, hasClaimed	
Method	constructor(stakingToken)	Method untuk menginisiasi alamat dari staking token ketika kontrak pertama kali dideploy
	claimToken()	Method yang digunakan untuk melakukan klaim staking token
	depositToken(amount)	Method untuk deposit jumlah staking token tertentu oleh smart contract deployer
	withdrawTokens(amount)	Method untuk mengambil kembali token dengan jumlah tertentu oleh smart contract deployer
	getDepositedSupply()	Method untuk mengambil data jumlah token yang sudah masuk pada kontrak token drop

Tabel 9. Keterangan Kontrak Token Drop

4. Kontrak Staking
    a. Menerima staking token
    b. Melakukan kalkulasi reward token
    c. Mengirimkan reward token

    Detail dari struktur kontrak staking adalah sebagai berikut:

Gambar G.11 Class Diagram Kontrak Staking

Nama	Staking Contract	
Dekripsi	Kontrak yang mengatur proses staking, kalkulasi dan pembagian reward	
Atribut	rewardToken, stakingToken, rewardTokenBalance, stakingTokenBalance, timeUnit, rewardNumerator, rewardDenominator, stakeBalance, stakeTimeStamp	
Method	constructor()	Method yang pertama kali dijalankan ketika deploy smart contract
	stake(uint256)	Method untuk melakukan staking
	unstake(uint256)	Method untuk membatalkan proses staking
	claimRewards()	Method untuk klaim reward setelah melakukan staking
	depositRewardToken(uint256)	Method untuk deposit reward token oleh smart contract deployer
	withdrawRewardToken(uint256)	Method untuk mengambil kembali token reward yang telah di deposit
	calculateReward(address)	Method untuk menghitung jumlah reward setelah melakukan staking
	getStakeInfo(address)	Method untuk melihat staking info

Tabel 10. Keterangan Kontrak Staking

H.3.5 Implementasi Smart Contract dan Web3

Pada tahap ini dilakukan implementasi desain dan kerangka yang sudah di buat pada tahap sebelumnya, dan diimplementasikan dalam bentuk sistem dan kode. Implementasi terdapat dua fase yaitu implementasi smart contract dan implementasi Web3 atau Dapps.

a. Implementasi Smart Contract

   Implementasi smart contract dilakukan berdasarkan model kontrak yang sudah dilakukan pada tahap sebelumya, peneliti akan mengimplementasikan semua attribute dan method yang ada pada class diagram yang sudah dibuat. Implementasi smart contract dilakukan menggunakan Remix IDE untuk memudahkan proses debugging secara langsung pada Ethereum Virtual Machine (EVM). Setelah proses debugging selesai, smart contract akan di deploy ke jaringan testnet Sepolia ETH menggunakan platform Thirdweb untuk selanjutnya akan diintegrasikan dengan aplikasi.

b. Implementasi Web3

   Implementasi Web3 dilakukan setelah proses deploy smart contract, pada fase ini akan dimulai dengan membuat user interface menggunakan bahasa pembangun website dan akan diintegrasikan menggunakan library dari Thirdweb dan Ethers JS. Implementasi web3 melibatkan extension dari browser yaitu metamask wallet untuk bisa berinteraksi dengan aplikasi berbasis blockchain.

H.3.6 Pengujian

Pada tahap ini akan dilakukan pengujian smart contract, pengujian bertujuan untuk mengetahui kelebihan dan kelemahan dari smart contract dan sistem yang telah dibuat. Pengujian akan dibagi menjadi dua fase yaitu uji fungsionalitas dan non-fungsionalitas.

a. Uji fungsionalitas

Uji Fungsionalitas dilakukan pada smart contract menggunakan Hardhat JS, Hardhat JS digunakan untuk menguji apakah smart contract yang dirancang bisa berjalan sesuai dengan kebutuhan atau tidak. Pengujian ini juga dilakukan pada aplikasi untuk menguji integrasi antara smart contract dengan user interface.

b. Uji non-fungsionalitas

Uji fungsionalitas dilakukan dengan memeriksa potensi celah keamanan pada smart contract dengan menggunakan Mythril, penggunaan tools untuk mendeteksi kerentanan pada smart contract meningkatkan akurasi dan efisiensi ketika testing (Khan & Namin, 2024). serta melakukan uji smart contract secara On-chain pada Sepolia exploler untuk dilihat data yang disimpan serta melakukan dekripsi untuk menguji transparansi data yang disimpan pada blockchain.

I. Luaran yang Diharapkan

Luaran yang diharapkan dari penelitian ini, yaitu:

a. Proposal Skripsi
b. Artikel Ilmiah Yang di Publikasikan
c. Sistem crowdfunding berbasis teknologi blockchain Ethereum

J. Jadwal Kegiatan

Jadwal kegiatan dalam penelitian ini akan dijabarkan pada tabel berikut.

No	Tahapan Penelitian	Bulan Ke-				
		1	2	3	4	5
1	Identifikasi dan Perumusan Masalah					
2	Perancangan Sistem					
3	Pembuatan Desain Blockchain					
4	Pemodelan Smart Contract					

5	Implementasi Smart Contract dan Web3					
6	Pengujian					
7	Analisis Hasil dan Penarikan Kesimpulan					

K. Daftar Pustaka

Aditiya Hermawan, D. P. (2023). Pemanfaatan Smart Contract dalam Transformasi Supply Chain melalui Teknologi Blockchain. *Jurnal Edukasi dan Penelitian Informatika (JEPIN)*, 1-2.

Archana B U, V. N. (2023). Overview of Cryptography. *Data Analytics and Artificial Intelligence*, 2.

Arunmozhi Manimuthu, R. S. (2019). A literature review on Bitcoin: Transformation of crypto currency into a global phenomenon. *IEEE Engineering Management Review*, 1-2.

Aufila, I. Z., Musfiroh, M. F., & Hinawati, T. (2024). Securities Crowdfunding Sebagai Instrumen Pembiayaan Usaha. *Journal of Management, Economics, and Entrepreneur Mikro Kecil Menengah (Umkm)*, 3-4.

Baihaqsani, A. K. (2023). Implementasi Teknologi Blockchain Dengan Sistem Smart Contract Pada Klaim Asuransi. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, 5.

Bonomi, S., Stefano, C., & Emilio , C. (2023). On the Efficacy of Smart Contract Analysis Tools. *34th International Symposium on Software Reliability Engineering Workshops (ISSREW)* (pp. 37-38). Rome: IEEE.

Budi Sahputra, T. D. (2024). Pemanfaatan Teknologi ETH Blockchain Untuk Aplikasi E-Voting Dengan Memanfaatkan Server Lokal. *Jurnal Ilmiah Teknik Informatika dan Sistem Informasi (JUTISI)*, 31-32.

Chaoqun Ma, X. K. (2019). The Privacy Protection Mechanism of Hyperledger Fabric and Its Application in Supply Chain Finance. *Springer Opern*, 9.

Chatkar, H. V., Singh, H. G., Sonavane, A. S., Singh, S., & Pulgam, N. (2023). Crowdfunding using Blockchain. *International Conference on Emerging Trends in Engineering & Technology - Signal and Information Processing (ICETET - SIP)*, 1-2.

Dzulfikar, F., & Susanto, A. (2020). Implementation of Smart Contracts Ethereum Blockchain in Web-Based Electronic Voting. *TRANSFORMTIKA*, 58.

Eleazer Gottlieb Julio Sumampouw, I. S. (2024). ANALISIS VERIFIKASI PROOF OF STAKE (POS) NFT DENGAN TEKNOLOGI SMART CONTRACT. *Jurnal Pendidikan Teknologi Informasi dan Komunikasi (EduTIK)*, 15-16.

Gada, S. (2021). Blockhcain-Based Crowdfunding: A Trust Building Model. *International Conference on Artificial Intellegence an Machine Vision (AIMV)* (pp. 3-4). Mumbai: IEEE.

Hasan, S. A., Al-Zahra, W. N., & Auralia, A. S. (2024). Implementasi Teknologi Blockchain dalam Pengamanan Sistem Keuangan pada Perguruan Tinggi. *Jurnal Manajemen, Pendidikan dan Teknologi Informasi (MENTARI)*, 12.

Helms, C., & McGahon, C. (2023). *An Overview of Solidity Development Frameworks.* Fidelity Center for Applied Technology (FCAT).

Huaqun Guo, X. Y. (2022). A survey on blockchain technology and its security. *Blockchain: Research and Applications*, 1.

Hutomo Sakti Kartiko, T. R. (2023). Implementasi IPFS untuk Mengurangi Gas Fee Smart Contract Ethereum pada Aplikasi Penggalangan Dana. *Jurnal Edukasi dan Penelitian Informatika (JEPIN)*, 8.

Jannah Yusoff, Z. M. (2022). A Review: Consensus Algorithms on Blockchain . *Journal of Computer and Communications, 2022, 10, 37-50*, 41 - 42.

jawapos.com. (2022, 12 14). *hukum dan kriminal*. Retrieved from radarsemarang.jawapos.com: https://radarsemarang.jawapos.com/hukum-dan-kriminal/721404033/diduga-gelapkan-dana-kemanusiaan-yayasan-rfps-dipolisikan

Kolomoyets, M., & Kynash, Y. (2023). Modern approaches to interact Smart-Contracts in React.js development with Thirdweb framework. *18th International Conference Computer Science and Information Technologies (CSIT).* Lviv, Ukraine: IEEE.

Liu, J. (2023). Digital Signature and Hash Algorithms Used in Bitcoin and Ethereum . *Third International Conference on Machine Learning and Computer Application (ICMLCA 2022),* (pp. 15 - 18). SPIE.

Maruwu, M. (2024). Metode Penelitian dan Pengembangan (R&D): Konsep, Jenis, Tahapan dan Kelebian. *Jurnal Ilmiah Profesi Pendidikan*, 1120 - 1230.

Raza, H., Ali, R., Iqbal, J., & Awais, M. (2024). Secure Room-Sharing Decentralized App Development on Ethereum Blockchain Using Smart Contract. *Journal of Informatic and Web Engineering*, 148 - 150.

Saleh, F. (2020). Blockchain Without Waste: Proof-of-Stake. *SSRN Electronic Journal*, 21.

tempo.co. (2022, 8 4). *hukum*. Retrieved from www.tempo.co: https://www.tempo.co/hukum/ppatk-temukan-176-yayasan-filantropi-mirip-act-yang-selewengkan-uang-sumbangan-312917

Xu, Y. (2023). A decentralized Trust Management Mechanism for Crowdfunding. *Information Sciences*, 2-6.

Zulfiqar Ali Khan, A. S. (2024). A Survey of Vulnerability Detection Techniques by Smart Contract Tools. *IEEE Access*, Volume 12, 70906.

LAMPIRAN

a. Wireframe Web3