

SEMINAR KOLOKIUM

PERANCANGAN DAN IMPLEMENTASI SISTEM PEMILIHAN ELEKTRONIK BERBASIS BLOCKCHAIN MENGGUNAKAN SOLIDITY

Firhan Abdurrahman Gani

NIM : 1207050040

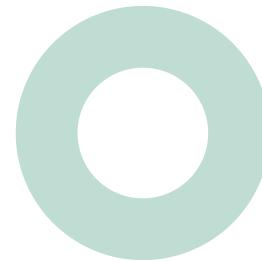
TEKNIK INFORMATIKA

2024

PEMBIMBING:

Dr. Wisnu Uriawan ST., M Kom.
Ichsan Taufik M T.

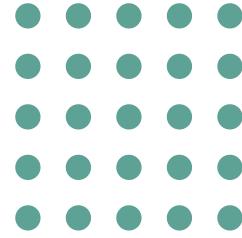
Latar Belakang



Pemilu di Indonesia masih menggunakan metode tradisional dengan pemungutan suara berbasis kertas yang memiliki beberapa kelemahan, seperti biaya besar, kemungkinan kesalahan, kecurangan, lambatnya tabulasi, dan dampak lingkungan dari limbah kertas.

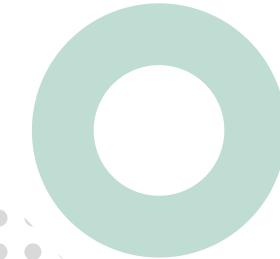
Penggunaan teknologi informasi dalam pemilu dapat meningkatkan efisiensi dan efektivitas, dengan e-voting menjadi alternatif modern yang lebih cepat dan mudah. E-voting menggantikan kertas suara dengan perangkat elektronik.

Teknologi blockchain menawarkan transparansi, keamanan, dan desentralisasi dalam proses pemilu, sehingga prosesnya dapat diverifikasi oleh semua pihak tanpa memerlukan pihak ketiga. namun masih menghadapi tantangan dalam hal kecepatan transaksi dan skalabilitas, terutama untuk pemilu berskala besar.



Rumusan Masalah

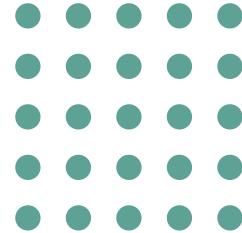
Tujuan Penelitian



- 01.** Bagaimana mendesain dan mengimplementasikan sistem pemilihan elektronik (e-voting) berbasis blockchain?
Membangun sistem pemilihan elektronik yang aman dan transparan berbasis teknologi blockchain.

- 02.** Bagaimana pengujian melalui mock election dan implementasi smart contract dalam sistem pemilihan elektronik (e-voting) dapat tercatat secara aman di blockchain?
Melakukan pengujian melalui mock election dan smart contract dalam sistem pemilihan elektronik (e-voting).

03

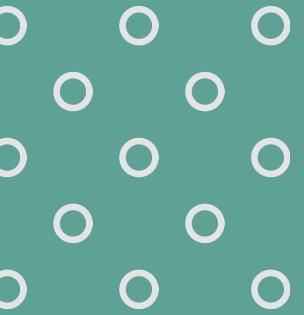


Batasan Masalah



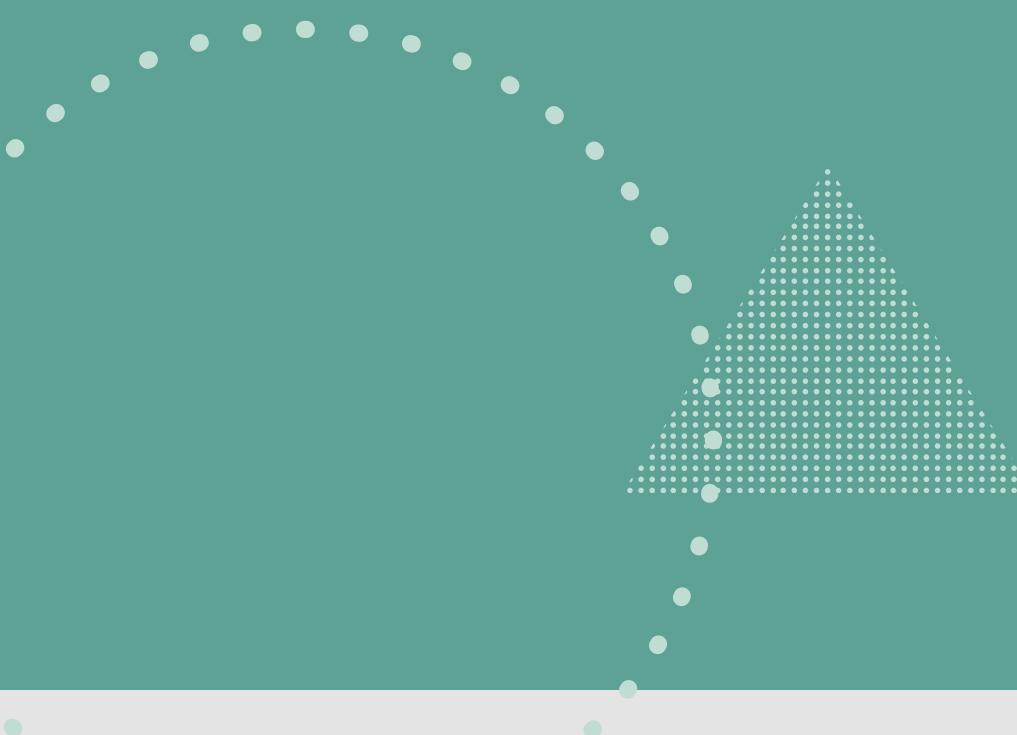
- 01.** Penelitian ini terbatas pada penggunaan teknologi blockchain Ethereum dan bahasa pemrograman Solidity untuk merancang dan mengimplementasikan sistem pemilihan elektronik.
- 02.** Sistem yang dikembangkan akan memungkinkan pemilih untuk memberikan suara mereka secara elektronik, menyimpan dan mencatat suara secara aman di dalam blockchain.
- 03.** Penelitian ini akan memperhatikan skala yang cocok untuk implementasi pemilihan elektronik berbasis blockchain. Namun, skala ekstensif atau implementasi pada tingkat nasional tidak akan menjadi fokus pada tahap ini. Pada blockchain, terutama jaringan publik, dapat menghadapi masalah skalabilitas ketika digunakan untuk jumlah pemilih yang sangat besar. Ini bisa memperlambat proses dan meningkatkan biaya transaksi, penelitian ini akan fokus pada skala pemilihan kepala desa.

04



Kajian Literatur

Landasan teori adalah alur logika atau penalaran yang merupakan konsep dan definisi yang disusun secara sistematis.

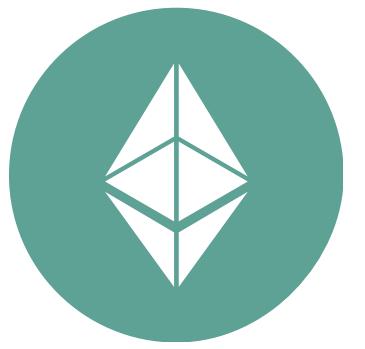


Dasar Teori



Blockchain

sebuah buku besar yang dapat diakses oleh publik dan setiap transaksi yang terjadi dicatat dalam blok yang saling terhubung satu dengan yang lainnya sehingga berbentuk seperti rantai



Ethereum

platform perangkat lunak terdesentralisasi yang berjalan di atas teknologi blockchain



Pemilihan Elektronik

proses pemilihan di mana pemilih menggunakan sistem elektronik, seperti komputer atau perangkat mobile, untuk memberikan suara mereka.



Solidity

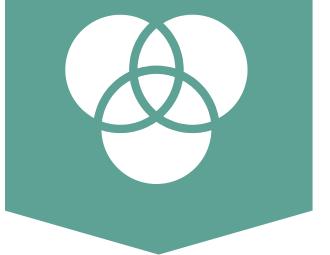
bahasa pemrograman yang digunakan untuk mengembangkan aplikasi berbasis blockchain, dan memungkinkan pengembang untuk mengembangkan aplikasi yang kompatibel dengan ethereum

Metode Penelitian



Plan

Memahami kebutuhan pengguna, menentukan fitur-fitur utama dari sistem e-voting berbasis blockchain



Design

Alur proses pengguna akan disusun untuk memastikan sistem berjalan lancar dari pendaftaran pemilih hingga penghitungan suara.



Development

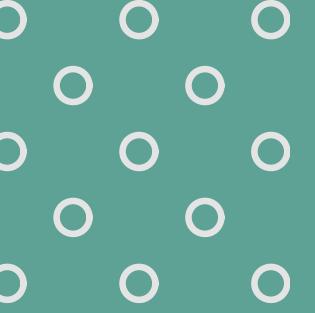
Implementasi desain ke dalam kode yang dapat dijalankan.



Test

Dua metode pengujian utama akan digunakan: Smart Contract Testing dan Mock Election.





Hasil dan Pembahasan



Plan (Perencanaan)

01.

Analisis Berjalan

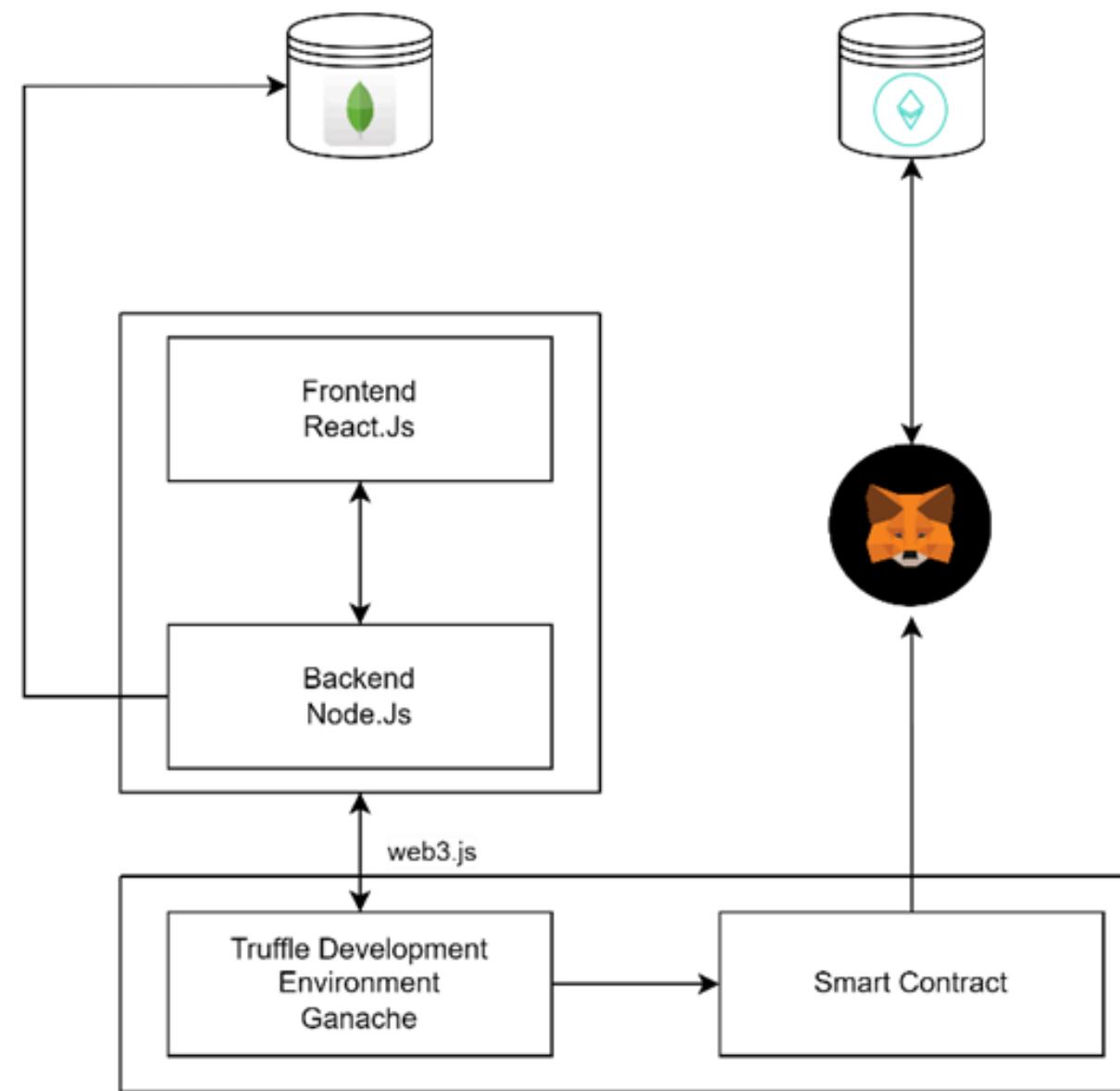
Rendahnya kepercayaan publik terhadap hasil pemilihan, sistem pemilihan tradisional yang digunakan sulit memastikan bahwa data pemilihan tersebut aman, akurat, transparan, otonom, dan anonim, karena manipulasi suara, human error, dan pengawasan yang terbatas.

02.

Analisis Usulan

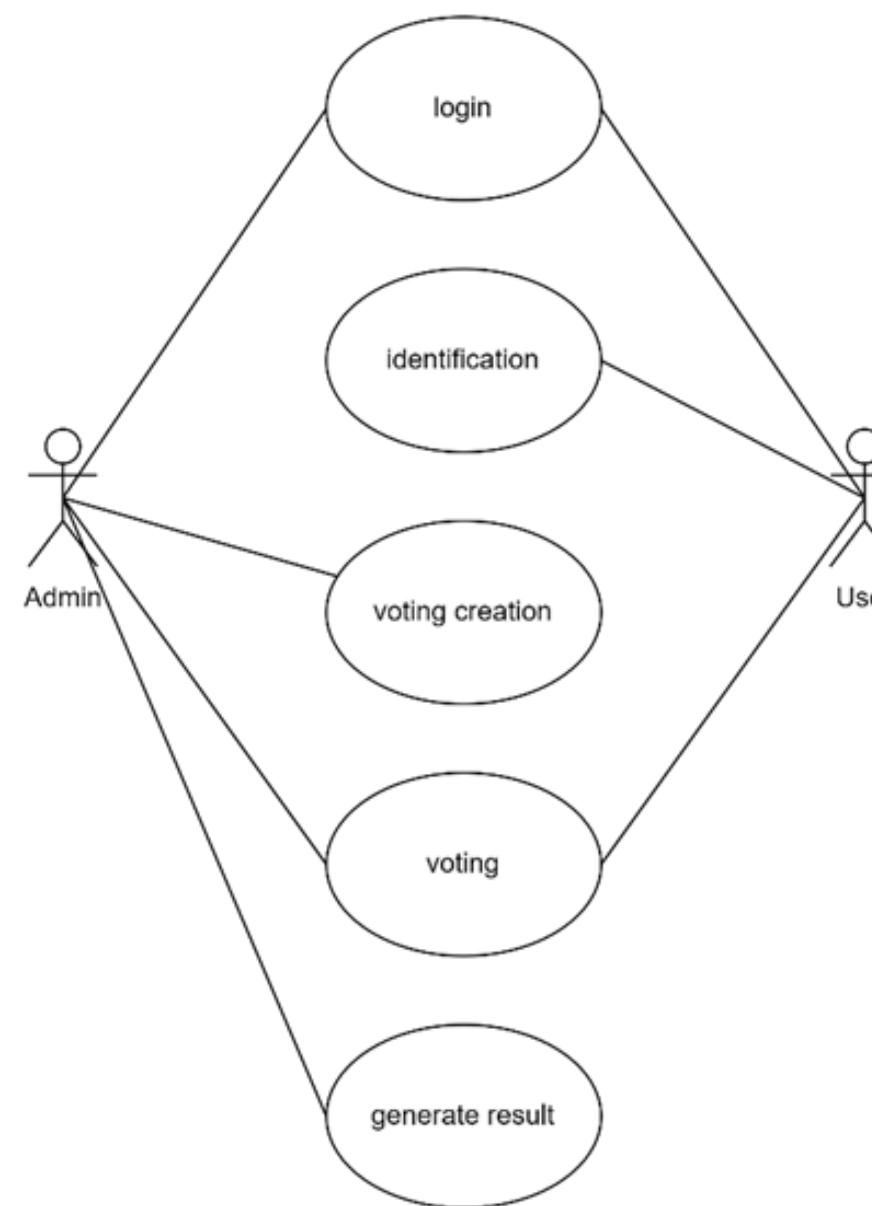
Blockchain dapat menjadi solusi dalam pembuatan sistem pemilihan elektronik yang dapat membuat sistem pemilihan menjadi lebih aman, dengan sifat desentralisasi dan kriptografi, memberikan jaminan keamanan dan akurasi tinggi dalam mencatat suara.

Design (Desain)



Arsitektur

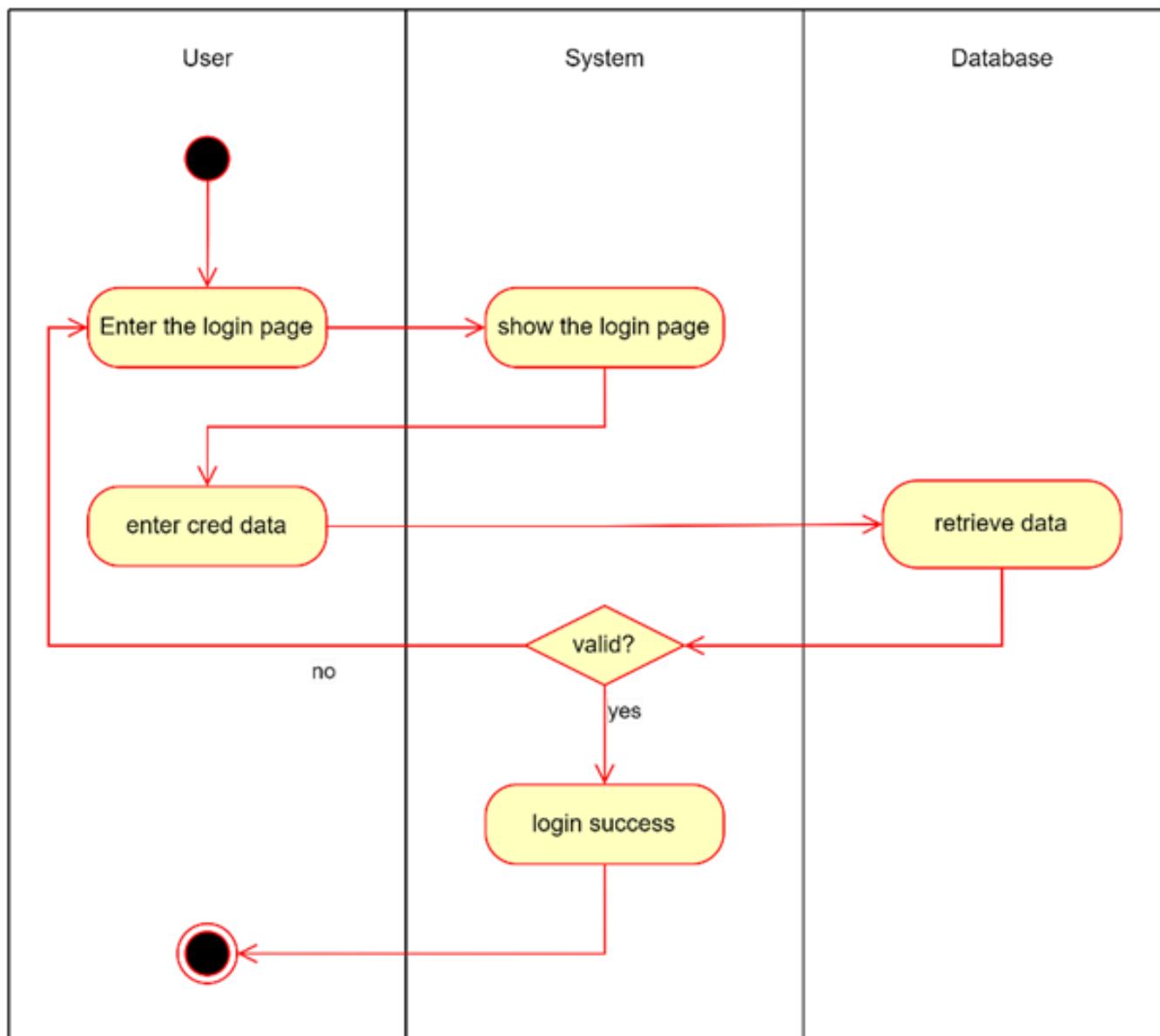
Blockchain dapat menjadi solusi dalam pembuatan sistem pemilihan elektronik yang dapat membuat sistem pemilihan menjadi lebih aman, dengan sifat desentralisasi dan kriptografi, memberikan jaminan keamanan dan akurasi tinggi dalam mencatat suara.



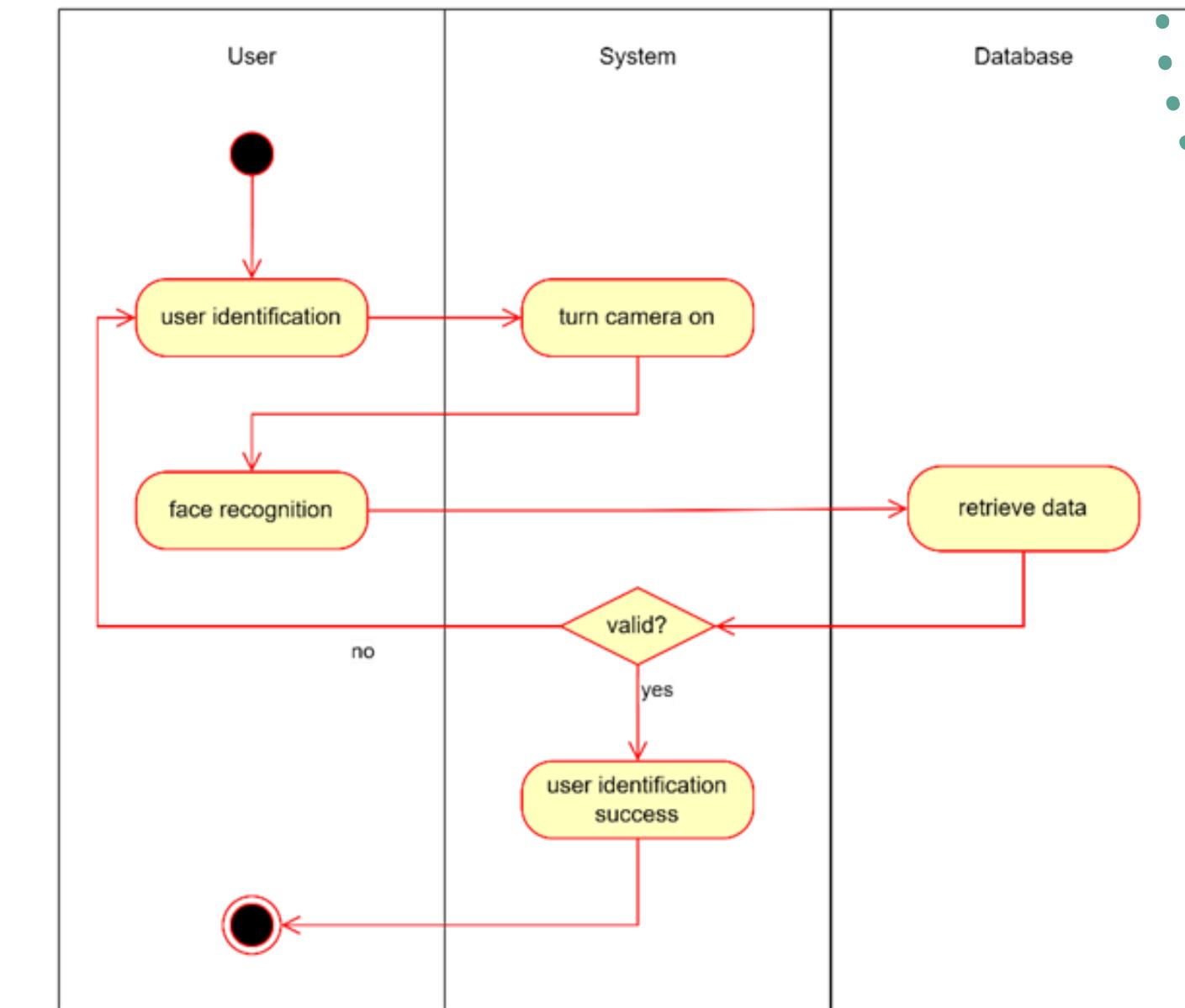
Use Case Diagram

Use case diagram adalah cara umum untuk mengomunikasikan fungsi-fungsi utama sistem perangkat lunak. Use-case diagram yang paling sederhana adalah representasi interaksi pengguna dengan sistem yang menunjukkan hubungan antara pengguna dan berbagai kasus penggunaan di mana pengguna terlibat.

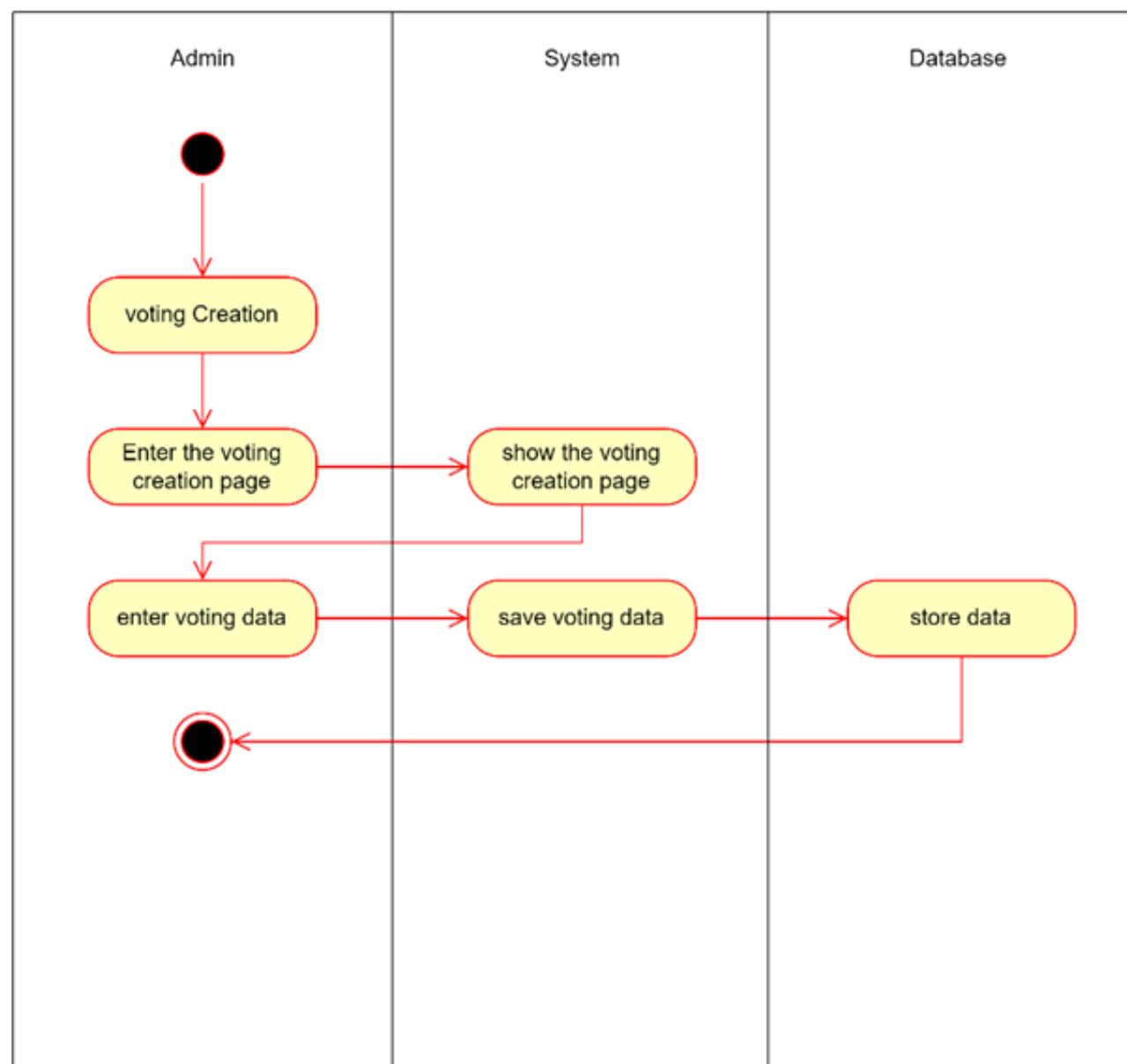
use-case login



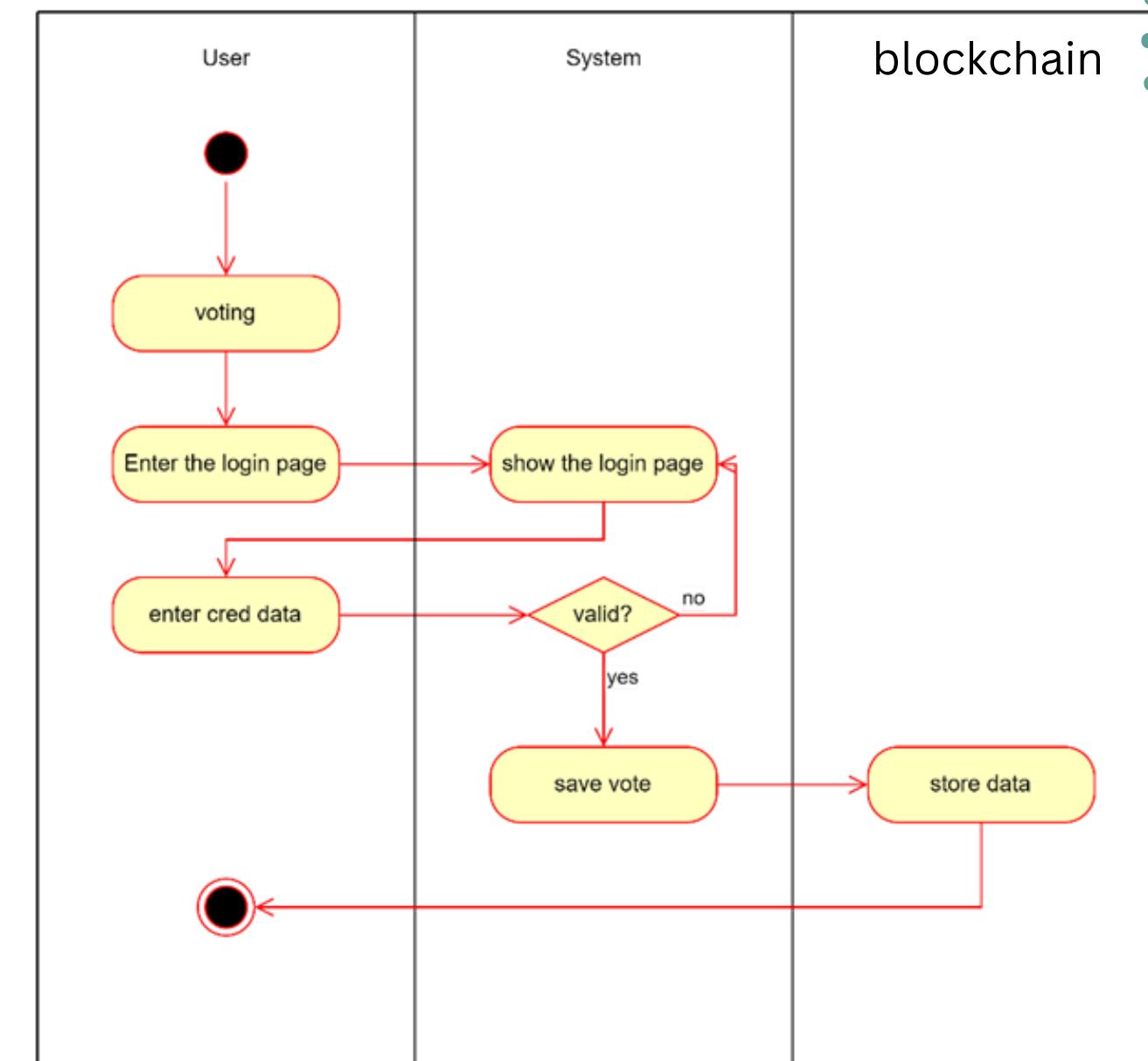
use-case user identification



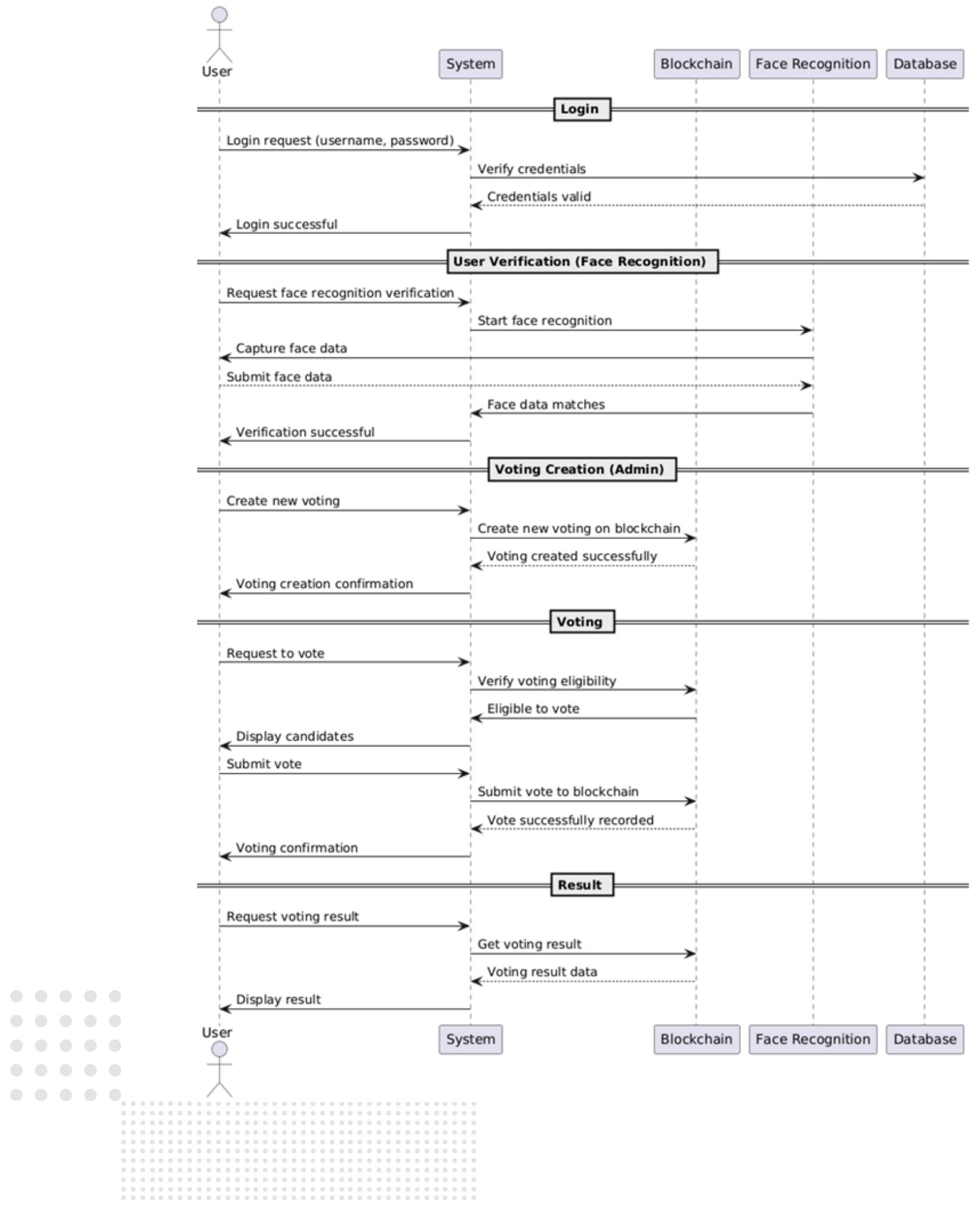
use-case voting creation



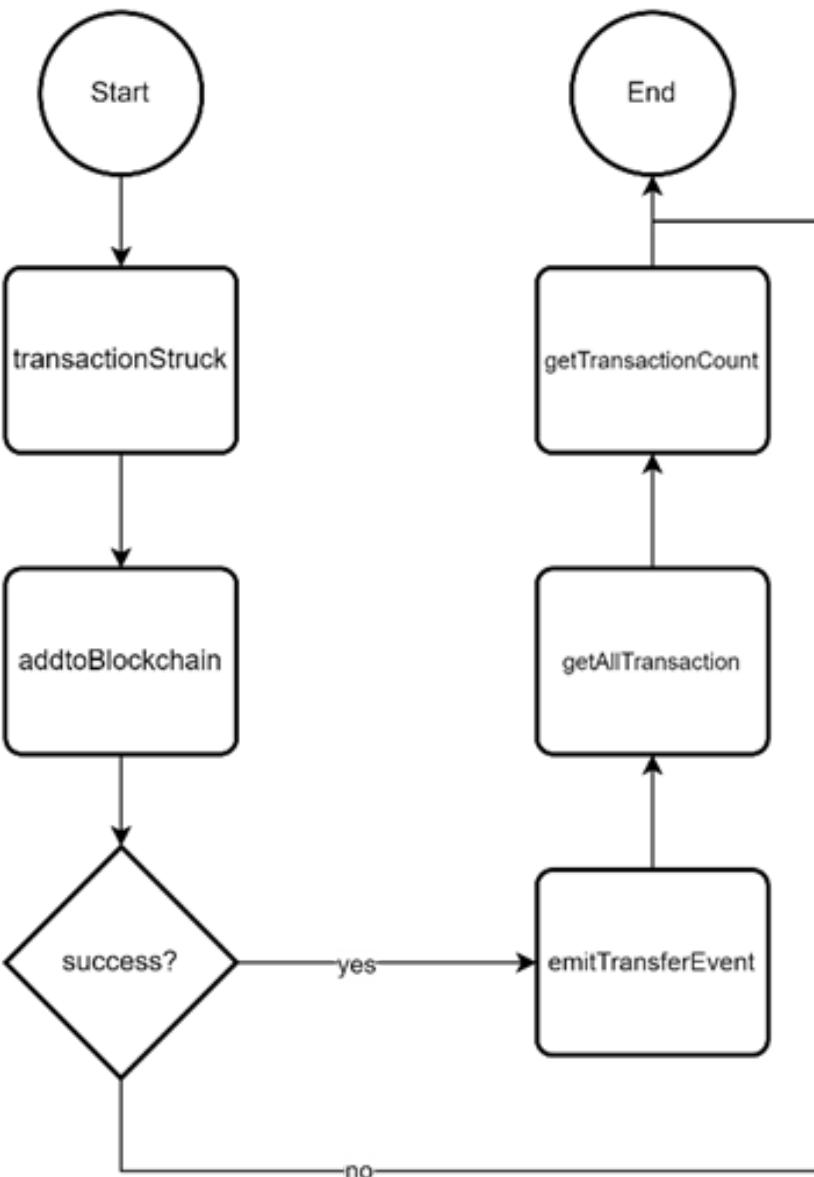
use-case voting



Sequence Diagram



Develop (Pengembangan)



Flowchart Smart Contract

Pada langkah ini, sistem siap menerima input untuk memulai transaksi voting. Struktur `transactionStruct` mendefinisikan data seperti `receiver`, `user_id`, `election_id`, dan `candidate_id`. Fungsi `addtoBlockchain` menambahkan transaksi ke blockchain, memperbarui `transactionCounter`, dan menyimpan transaksi ke array `transactions`. Jika transaksi berhasil, `eventTransfer` akan dipancarkan untuk memberi tahu jaringan tentang transaksi baru. Jika gagal, proses dihentikan. Setelah tercatat, pengguna dapat menggunakan fungsi `getAllTransaction` untuk melihat semua transaksi, atau `getTransactionCount` untuk mengetahui jumlah total transaksi.

```
// SPDX-License-Identifier: UNLICENSED
pragma solidity ^0.8.0;

contract Transaction{
    uint256 transactionCounter;

    event Transfer(address from,address receiver,string user_id,string election_id,string candidate_id,uint timestamp);

    struct TransactionStruct {
        address from;
        address receiver;
        string user_id;
        string election_id;
        string candidate_id;
        uint timestamp;
    }

    TransactionStruct[] transactions;

    function addToBlockchain(address payable receiver,string memory user_id,string memory election_id,string memory candidate_id) public {
        transactionCounter+=1;

        transactions.push(TransactionStruct(msg.sender,receiver,user_id,election_id,candidate_id,block.timestamp));
        emit Transfer(msg.sender,receiver,user_id,election_id,candidate_id,block.timestamp);
    }

    function getAllTransaction() public view returns (TransactionStruct[] memory){
        return transactions;
    }

    function getTransactionCount() public view returns (uint256){
        return transactionCounter;
    }
}
```

Hasil pengembangan antarmuka admin-voting creation

The screenshot displays the 'Beranda' (Home) page of the 'evoting' application. On the left, a dark sidebar menu lists several options: Beranda, Pemilih, Kandidat, Pemilihan, Fase Pemilihan, Hasil, and Logout. The main content area shows a form titled 'Pemilihan'. The 'Judul *' field contains the value 'TEST-PILKADES'. Below it, a 'Pilih Kandidat' section lists three entries: '3204291708870006', '3204292802750006', and '3204291004930001'. At the bottom of the form is a blue 'SIMPAN' button.

Hasil pengembangan antarmuka user-voting

The screenshot shows a web-based voting platform with a blue header bar. The header contains the logo 'evoting-blockchain' and navigation links for 'Beranda', 'Pemilihan', and 'Hasil'. The main content area has a title 'Kandidat TEST-PILKADES' and displays three candidate profiles in separate boxes:

- CS** (Purple circle)
3204291708870006
Nama : Calon Satu
Alamat: Gunungleutik
[PILIH](#)
- CK** (Green circle)
3204292802750006
Nama : Calon Kedua
Alamat: Gunungleutik
[PILIH](#)
- CK** (Orange circle)
3204291004930001
Nama : Calon Ketiga
Alamat: Gunungleutik
[PILIH](#)

At the bottom of the content area, there is a footer with the text '©evoting-blockchain'.

Hasil pengembangan antarmuka user-login

The screenshot shows a user login form for the 'evoting-blockchain' application. The header features a blue bar with the logo and name 'evoting-blockchain' on the left, and navigation links 'Beranda', 'Pemilihan', and 'Hasil' on the right. Below the header, a message 'Login untuk Melanjutkan' is displayed. The form contains four input fields: 'NIK *' with value '3204291106980006', 'Election Id *' with placeholder '.....', 'Candidate Name *' with value '3204291004930001', and 'Password *' with placeholder '.....'. A blue 'PILIH' button is located below the form. The footer displays the copyright notice '©Devoting-blockchain'.

evoting-blockchain

Beranda Pemilihan Hasil

Login untuk Melanjutkan

NIK *

3204291106980006

Election Id *

.....

Candidate Name *

3204291004930001

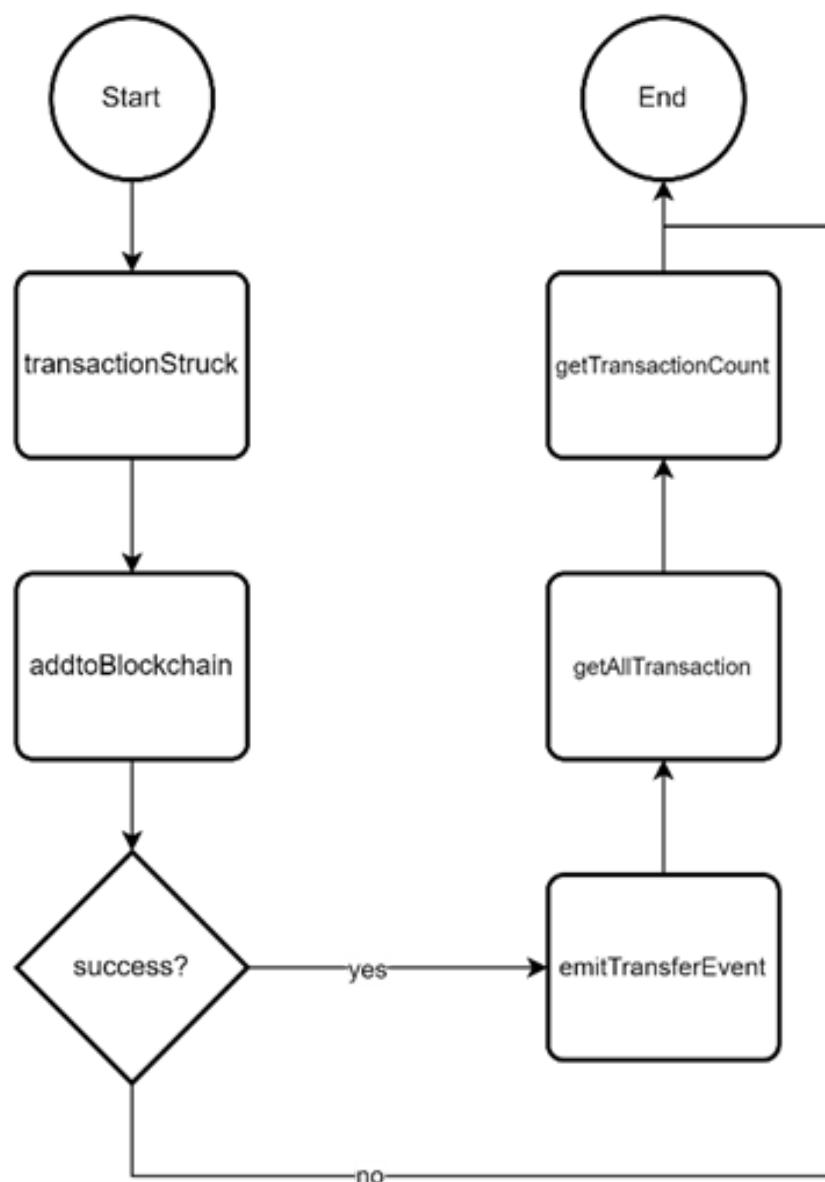
Password *

.....

PILIH

©Devoting-blockchain

Test (Pengujian)



Smart Contract

Smart Contract Testing bertujuan untuk memastikan bahwa kode smart contract yang ditulis dalam Solidity bekerja sesuai spesifikasi.

Skenario Mock Election Untuk Admin

No	Skenario	Tujuan	Langkah Uji	Input	Output yang Diharapkan	Status
1	Login Admin	Memastikan bahwa sistem memungkinkan pengguna untuk login dengan menggunakan kredensial yang valid.	1. Masukkan username dan password yang valid. 2. Klik tombol "Login".	o Username: "Admin" o Password: "Admin123"	Admin berhasil login dan diarahkan ke halaman dashboard.	Sukses ▾
2	Pendaftaran Pemilih	Memastikan bahwa sistem memungkinkan pemilih untuk mendaftar dengan informasi yang lengkap dan valid.	1. Masukkan data diri lengkap pada form pendaftaran. 2. Klik tombol "Daftar".	o Nama: "John Doe" o NIK: "1234567890123456" o Alamat: "Jl. Merdeka No. 1"	Pesan konfirmasi bahwa pendaftaran berhasil dan data pemilih disimpan di database.	Sukses ▾
4	Pendaftaran Kandidat	Memastikan bahwa admin dapat mendaftarkan kandidat pemilihan menggunakan kredensial yang valid	1. Klik menu "Kandidat" 2. Klik tombol "Tambah Kandidat" 3. Isi form dengan informasi kandidat seperti nama, email, deskripsi dan foto.	o Nama kandidat o Email kandidat o Deskripsi o Upload foto	Admin berhasil menambahkan kandidat kedalam daftar kandidat	Sukses ▾
7	Membuat Pemilihan	Membuat pemilihan baru oleh admin	1. Klik tombol "Buat Pemilihan Baru" pada antarmuka admin. 2. Isi form dengan informasi pemilihan seperti nama pemilihan, tanggal, dan kandidat. 3. Klik tombol "Simpan"	o Nama pemilihan o Tanggal pemilihan o Kandidat	Pemilihan baru berhasil dibuat dan muncul di daftar pemilihan	Sukses ▾
8	Logout	Memastikan bahwa sistem memungkinkan pengguna untuk logout.	1. Klik tombol "Logout" di antarmuka pengguna 2. Verifikasi bahwa pengguna diarahkan ke halaman login atau beranda.	Klik tombol "Logout"	Pengguna berhasil logout dan diarahkan ke halaman login atau beranda.	Sukses ▾

Skenario Mock Election Untuk Pemilih

No	Skenario	Tujuan	Langkah Uji	Input	Output yang Diharapkan	Status
1	Login Pengguna	Memastikan bahwa sistem memungkinkan pengguna untuk login dengan menggunakan kredensial yang valid.	1. Masukkan username dan password yang valid. 2. Klik tombol "Login".	o NIK : "1234567890987654" o Password: "johndoepassword"	Pengguna berhasil login dan diarahkan ke halaman dashboard.	Sukses ▾
2	Pemilihan Kandidat	Memastikan bahwa sistem memungkinkan pemilih untuk memilih kandidat yang diinginkan.	1. Login sebagai pemilih yang sudah terdaftar. 2. Pilih kandidat dari daftar kandidat yang tersedia. 3. Klik tombol "Submit".	o Pilihan Kandidat: "Kandidat A"	Suara berhasil disimpan dan pesan konfirmasi ditampilkan.	Sukses ▾
4	Hasil Pemilihan	Memastikan bahwa sistem memungkinkan pemilih untuk melihat hasil pemilihan	1. Klik halaman "Hasil" di antarmuka pengguna 2. Lihat hasil pemilihan	o Lihat hasil pemilihan	Pengguna berhasil diarahkan menuju halaman hasil dan sistem memperlihatkan hasil pemilihan.	Sukses ▾

Hasil Simulasi

CURRENT BLOCK 27	GAS PRICE 20000000000	GAS LIMIT 6721975	HARDFORK MERGE	NETWORK ID 5777	RPC SERVER HTTP://127.0.0.1:7545	MINING STATUS AUTOMINING	WORKSPACE HEAVY-BOUNDARY	SWITCH	⚙️
TX HASH 0x38d26b331c1d47d36dc1e0cafb7e3baa124c5107f853d171c99b582ca9ad5863								<button>CONTRACT CALL</button>	
FROM ADDRESS 0x56ccAEDD66547dD131Bc2B9dFA3eF830A88FBC7A					TO CONTRACT ADDRESS Transaction		GAS USED 175993	VALUE 0	
TX HASH 0x531d2dbac4288b7af16287fac086da2738f533c543aa176b797e2b573853dc87								<button>CONTRACT CALL</button>	
FROM ADDRESS 0x56ccAEDD66547dD131Bc2B9dFA3eF830A88FBC7A					TO CONTRACT ADDRESS Transaction		GAS USED 175993	VALUE 0	
TX HASH 0x84ef43216aa35437e035b47c16c4ef2c079ad49a21eacbb719fce131dfd10f55								<button>CONTRACT CALL</button>	
FROM ADDRESS 0x56ccAEDD66547dD131Bc2B9dFA3eF830A88FBC7A					TO CONTRACT ADDRESS Transaction		GAS USED 175993	VALUE 0	
TX HASH 0x061186fa59292a9705095e5bc0fae966ad425ac40dfcb791515581ac8db0eccb								<button>CONTRACT CALL</button>	
FROM ADDRESS 0x56ccAEDD66547dD131Bc2B9dFA3eF830A88FBC7A					TO CONTRACT ADDRESS Transaction		GAS USED 175993	VALUE 0	

Penelitian ini melakukan pengujian terhadap smart contract dan simulasi pemilihan (mock election), di mana hasil pengujian sistem pemilihan elektronik (e-voting) dinyatakan memenuhi kebutuhan untuk skala pemilihan kepala desa. Validitas ini terlihat dari hasil pengujian smart contract yang berhasil di-compile tanpa masalah, serta simulasi yang berjalan sesuai dengan fungsi yang diharapkan. Dalam proses pengujian ini, total sebesar 0,09503622 ETH digunakan, mencakup mulai dari deploy smart contract hingga 26 transaksi untuk proses voting.

Kesimpulan

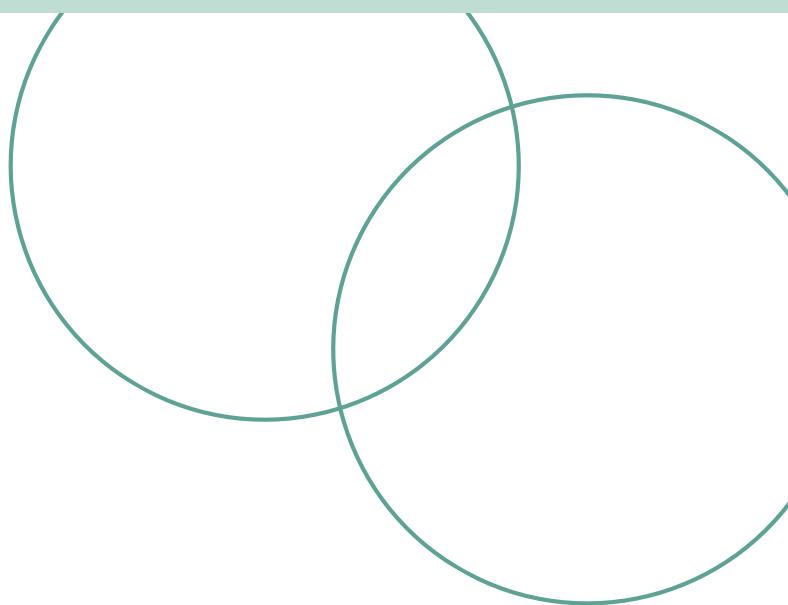
Teknologi blockchain, dengan fitur desentralisasi dan keamanan berbasis kriptografi, mampu memberikan keamanan, transparansi, anonimitas, dan efisiensi yang lebih baik dibandingkan sistem manual.

Penggunaan smart contract memastikan bahwa semua suara yang diberikan tidak dapat diubah setelah tercatat di blockchain, serta hanya pemilih yang terverifikasi yang dapat memberikan suara.



Terima Kasih





Proses Penelitian

Proses 1

Proses Satu

Proses penelitian dapat anda tuliskan pada halaman ini

Proses 2

Proses Dua

Proses penelitian dapat anda tuliskan pada halaman ini

Proses 3

Proses Tiga

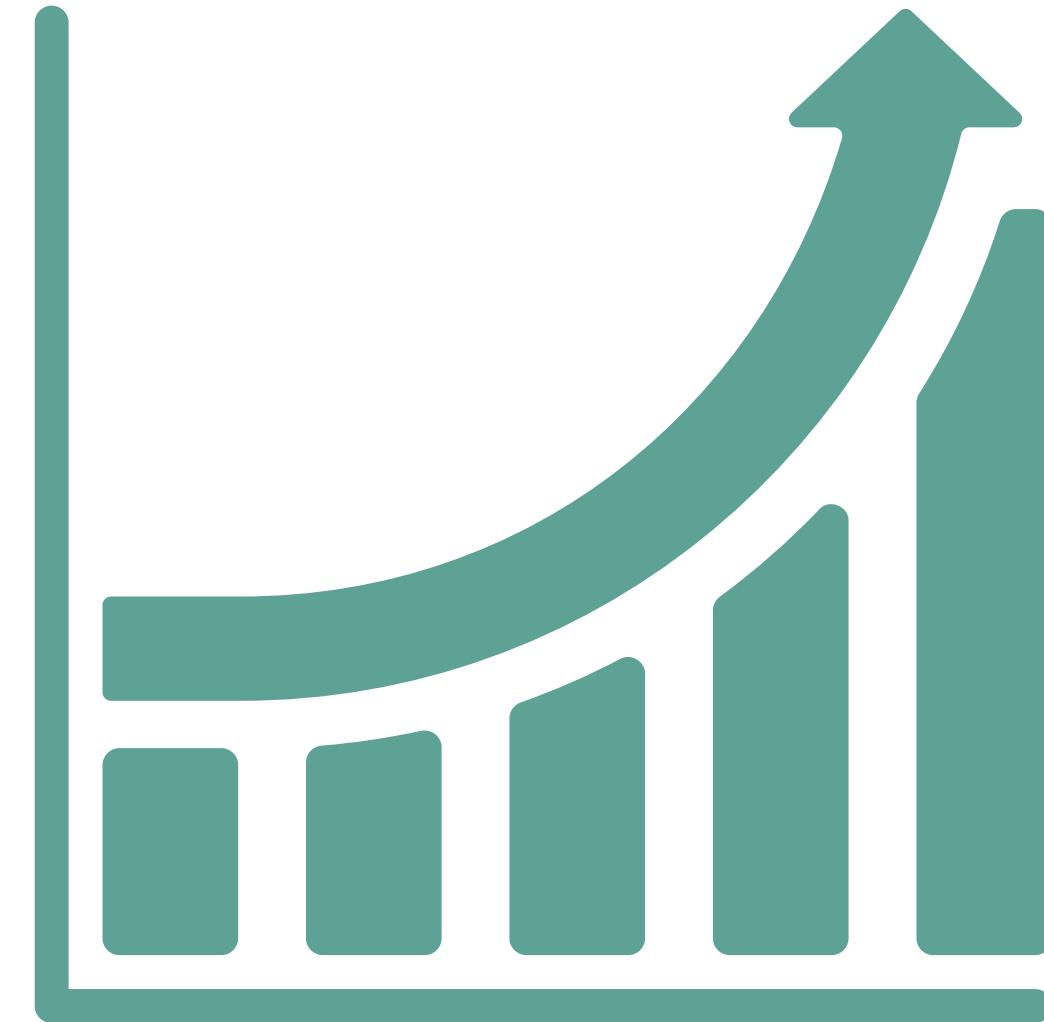
Proses penelitian dapat anda tuliskan pada halaman ini

Proses 4

Proses Empat

Proses penelitian dapat anda tuliskan pada halaman ini





Grafik & Penelitian Hasil Penelitian

Hasil penelitian dapat
anda tuliskan pada
halaman ini

Tujuan Penelitian

01.

Tujuan Satu

Tujuan yang ingin dicapai dari dilakukannya penelitian untuk menjawab bagian rumusan masalah

02.

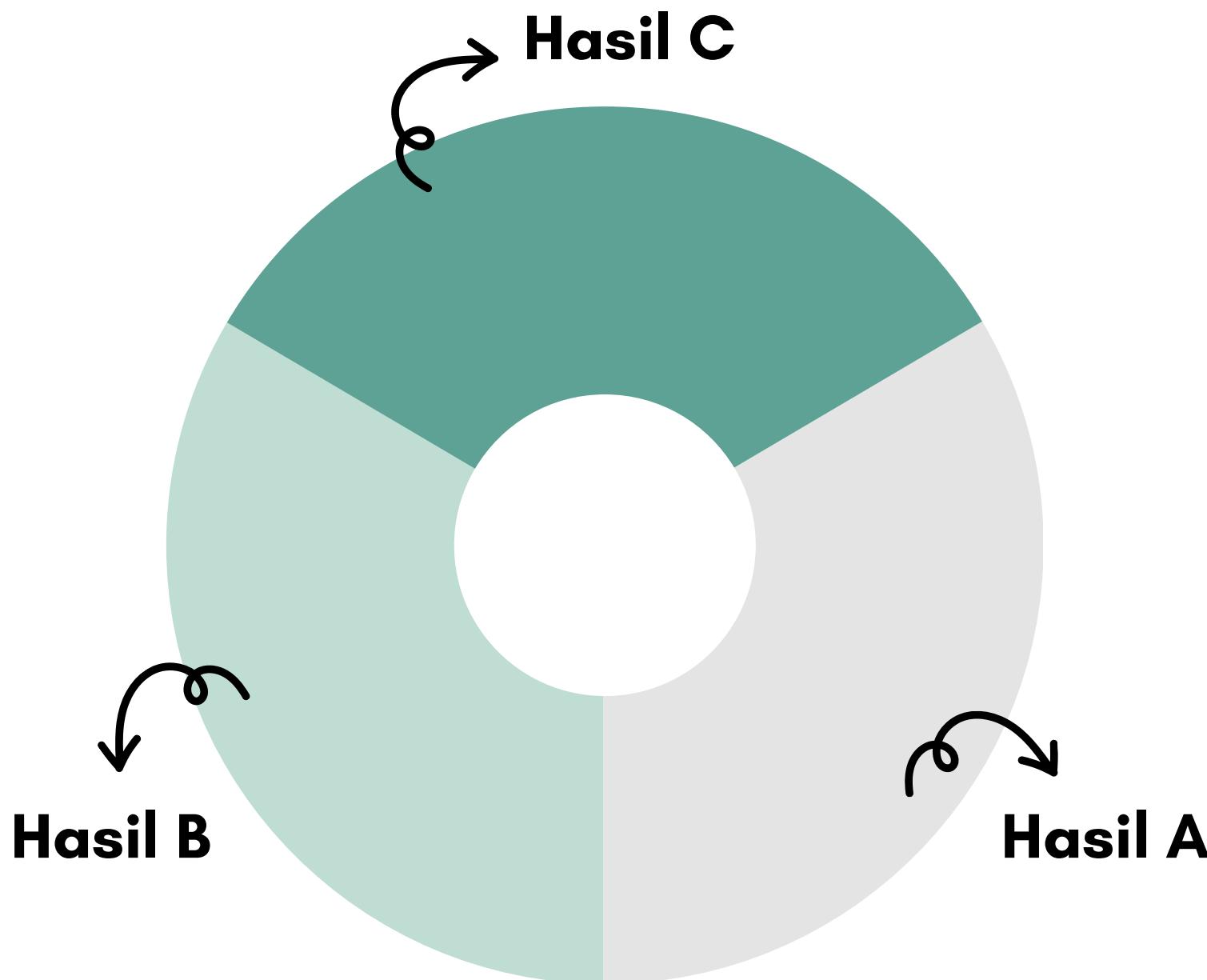
Tujuan Dua

Tujuan yang ingin dicapai dari dilakukannya penelitian untuk menjawab bagian rumusan masalah

03.

Tujuan Tiga

Tujuan yang ingin dicapai dari dilakukannya penelitian untuk menjawab bagian rumusan masalah



Hasil A

Hasil penelitian dapat anda tuliskan pada halaman ini

Hasil B

Hasil penelitian dapat anda tuliskan pada halaman ini

Hasil C

Hasil penelitian dapat anda tuliskan pada halaman ini