PENGEMBANGAN NON-INTERACTIVE ZERO KNOWLEDGE PROOF DAN SMART CONTRACT BARU BERBASIS BLOCKCHAIN PADA E-CERTIFICATE

Linda Handayani, S.T., MMSI.
99221912

PROGRAM DOKTOR TEKNOLOGI INFORMASI

UNIVERSITAS GUNADARMA

2023

Daftar Isi

Daftar Tabel

Daftar Gambar

Bab 1

Pendahuluan

1.1 Latar Belakang

Teknologi blockchain adalah salah satu dari beberapa inovasi dalam ilmu komputer yang telah melampaui ketenaran aplikasi awalnya yaitu mata uang kripto. Blockchain mulai digunakan pada mata uang kripto (bitcoin) yang dianggap dapat menyelesaikan masalah transparansi end-to-end. Teknologi ini secara bertahap semakin populer sebagai alat jaringan untuk mempermudah operasi bisnis dengan menerapkan jaringan peer to peer untuk verifikasi dan berbagi data [1]. Karakteristik utama yang dimiliki teknologi blockchain yaitu desentralisasi, transparansi, kekekalan, keamanan, buku besar terdistribusi, tokenisasi, mekanisme konsensus dan smart contract. Hal ini membuat teknologi blockchain terus berkembang ke beragam aplikasi dan model binis berbasis platform yang inovatif.

Teknologi blockchain mengacu pada buku besar transaksi data yang dicatat pada basis data terdistribusi dan dibagikan dengan jaringan yang terdesentralisasi [2]. Jaringan terdesentralisasi memiliki beberapa keunggulan diantaranya menyediakan lingkungan tanpa kepercayaan di mana setiap anggota memiliki salinan data yang sama persis dalam bentuk buku besar yang didistribusikan, meningkatkan rekonsiliasi data di mana setiap kali data diubah maka setiap entitas memiliki akses ke tampilan data bersama secara real-time tanpa membuka peluang kehilangan data atau data yang salah, mengurangi titik kelemahan dalam sistem yang mungkin terlalu bergantung pada aktor tertentu di mana titik lemah ini dapat menyebabkan kegagalan sistem termasuk kegagalan untuk menyediakan layanan yang dijanjikan ser-

ta mengoptimalkan distribusi sumber daya [3]. Fitur smart contract yang dimiliki blockchain memungkinkan transaksi dan pertukaran dokumen dengan menggunakan kontrak digital dan kontrak yang diotomatisasi [4]. Validasi transaksi pada protokol smart contract di antaranya pemrosesan pembayaran atau verifikasi aset yang ditanamkan [5]. Hal ini dapat mengatasi permasalah terkait penipuan atau kesalahpahaman kontrak dengan mengeksekusi kontrak secara otomatis melalui kode yang telah ditentukan untuk menghindari layanan perantara dan menyediakan otomatisasi untuk proses bisnis [6]. Konsensus mengacu kepada mekanisme atau protokol yang digunakan untuk mencapai kesepakatan di antara semua peserta (node) jaringan blockchain tentang keadaan atau urutan transaksi yang valid [7]. Konsensus blockchain digunakan untuk menjaga keandalan, keamanan dan integritas data di seluruh jaringan tanpa adanya pihak otoritas sentral.

Blok adalah catatan data yang terhubung ke dalam sebuah rantai melalui fungsi hash crypto-analytic untuk mencegah pihak yang tidak dikenal dapat membaca dan merusak informasi. Fungsi hash yang digunakan untuk memvalidasi transaksi pada blok untuk mencegah perubahan data yang tercatat [8]. Kemampuan sebuah blok untuk tetap tidak berubah dan tidak diubah disebut kekekalan. Transaksi dikumpulkan bersama dalam satu blok mempertahankan hashing dari blok sebelumnya yang dapat membantu proses validasi blok baru.

Node adalah titik koneksi individual dalam jaringan blockchain yang menjalankan fungsi vital, di antaranya membantu dalam memelihara dan memperbaharui buku besar blockchain secara terdistribusi, memvalidasi transaksi berdasarkan mekanisme konsensus blockchain dan mencegah transaksi ganda dan kecurangan serta membantu penyebaran informasi transaksi ke seluruh jaringan. Node memiliki kemampuan untuk bergabung dan keluar jaringan secara bebas, yang memungkinkan untuk mengakses dan mengubah data di blockchain publik [9].

Blockchain dapat menampilkan detail transaksi yang dapat dilihat oleh siapa saja yang terhubung ke dalam jaringan (transparan). Data sensitif seperti informasi pribadi, informasi kesehatan, data keuangan dan pajak, informasi akun dan kata sandi serta informasi pekerjaan dapat dilihat. Hal ini menjadi tantangan tersendiri pada penerapan blokchain yang memerlukan tingkat privasi yang tinggi.

Kriptografi adalah seni dan ilmu mengamankan komunikasi dan data.

Hal ini merupakan pondasi untuk berbagai aspek keamanan digital, termasuk keamanan internet dan jaringan. Kriptografi memiliki aspek utama yaitu enkripsi di mana proses mengubah informasi menjadi bentuk yang tidak dapat dibaca tanpa kunci rahasia, integritas data di mana menggunakan hash dan fungsi lainnya untuk memastikan bahwa data tidak diubah atau dirusak selama transmisi atau penyimpanan serta autentikasi di mana memastikan bahwa pesan atau transaksi benar-benar berasal dari pengirim yang diklaim. Salah satu metode dalam kriptografi adalah ZKP (Zero Knowledge Proof). ZKP metode yang memungkinkan satu pihak (prover) membuktikan kepada pihak lain (verifier) bahwa suatu pernyataan adalah benar, tanpa mengungkap informasi tambahan apa pun selain dari kenyataan bahwa pernyataan tersebut benar. Sehingga ZKP menjadi relevan dan bermanfaat dalam menyelesaikan tantangan penerapan blockchain untuk meningkatkan privasi.

Penelitian Claudia dkk pada tahun 2020 mengimplementasi prototipe berbasis blockchain untuk manajemen respons permintaan terdesentralisasi yang diperkaya dengan solusi zkp untuk menjaga privasi data produsen energi. Metode yang digunakan adalah penerapan blockchain untuk manajemen sistem respon permintaan yang terdesentralisasi, smart contract digunakan untuk memvalidasi aktivitas produsen dalam program respons permintaan dan ZKP untuk menyembunyikan data energi yang dimonitor dan profil fleksibilitas yang diminta [10]. Penelitian Swagastika dkk pada tahun 2021 mengusulkan sistem manajemen e-waste berbasis berbasis blockchain yang mencakup transparansi, pelacakan, penghematan biaya dan pemantauan otomatis dari pembuatan e-waste. Penelitian ini menghasilkan prototipe pada platform Ethereum beserta evaluasi kelayakan dan kinerja. Sistem menggunakan smart contract untuk mendaftar dan mentransfer kepemilikan. ZKP digunakan untuk proses validasi identitas yang berfokus pada privasi tanpa mengungkap informasi pribadi dari pemangku kepentingan dalam sistem [11].

Penelitian Zhuoliang Qui dkk pada tahun 2023 mengusulkan kerangka klaim asuransi mobil berbasis blockchain menggunakan teknologi ZKP untuk melindungi privasi data pelanggan. Metode yang digunakan adalah penggunaan blockchain dalam membuat sistem terdesentralisasi untuk proses klaim asuransi dan memastikan integritas data asuransi serta menambahkan teknologi ZKP di dalam sistem untuk menjaga privasi data asuransi dan identitas pelanggan. Hal ini mengatasi kekhawatiran privasi dalam skema penerapan

asuransi mobil berbasis blockchain tradisional. Hasil eksperimen menunjukkan bahwa skema ini berperforma baik dalam hal keamanan dan kinerja dan analisis perbandingan dengan skema lain membuktikan efektivitasnya dalam mencapai otorisasi rahasia dan perlindungan privasi[12].

Penggunaan ZKP pada proses verifikasi berbasis blockchain memiliki tantangan terkait skalabilitas di mana jika sistem memerlukan verifikasi berskala besar. ZKP memerlukan interaksi langsung antara prover dan verifier sehingga jika verifikasi dilakukan dengan skala besar maka verifikasi menjadi kurang efisien. Pendekatan Non-Interactive ZKP dapat mengatasi tantangan t.ersebut. Non-interactive ZKP memungkinkan verifikasi bukti tanpa interaksi langsung antara prover (orang yang memberikan bukti) dan verifier (orang yang memverifikasi bukti). Proses ini biasanya melibatkan CSR (Common Reference String) yang dikenal dan dipercaya oleh kedua belah pihak. Hal ini dapat meningkatkan efisiensi transaksi dengan tetap manjaga privasi pengguna.

Penelitian Ya-Che Tsai dkk pada tahun 2019 memperkenalkan Non-Interactive ZKP untuk aplikasi terdesentralisasi. ZKP (Zero Knowledge Rang Proof) memungkinkan pengguna untuk membuktikan bahwa nilai rahasi berada dalam rentang tertentu tanpa harus mengungkapkan nilai sebenarnya. Pada proses interaksi transaksi tidak diperlukan komunikasi antara pengguna dan verifikator selama pembuktian. Hal ini meningkatkan efisiensi yang membuatnya cocok untuk berbagai aplikasi yang diimplementasikan pada Ethereum [13]. Penelitian Gyeongjin Ra dkk pada tahun 2021 mengusulkan manajemen identitas anonim yang dapat diverifikasi (VAIM) yang menghubungkan saluran privasi antar pengguna dengan membangun verifikasi identitas dan penyedia kontrol akses melalui keputusan yang berpusat pada pengguna dan sistem manajemen identitas anoninim. Peningkatkan model identitas klaim blockchain tradisional dengan menggunakan algoritma ZKP untuk mencapai ketidakterhubungan identitas dan mencegah pengungkapan kepemilikan atribut. Evaluasi kinerja lingkungan dan analisis keamanan menunjukkan bahwa skema penelitian mencapai perlindungan privasi yang efisien [14].

Kepercayaan terhadap dokumen akademik seperti e-certificate sangat penting dalam dunia pendidikan. Namun berbagai masalah seperti pemalsuan, kesalahan administrasi dan transparansi sering menyertai sistem konvensional. Penerapan teknologi Zero-Knowledge Proof (ZKP) dan Blockchain sangat penting untuk mengubah cara kita mengelola e-certificate. Penerapan

ZKP digunakan untuk membuktikan keaslian dan kepemilikan e-certificate tanpa perlu mengungkapkan informasi pribadi atau detail e-certificate sehingga berguna dalam menjaga privasi dan keamanan. Penerapan blockchain pada e-certificate digunakan untuk menyimpan transaksi secara aman di dalam buku besar sertamenciptakan sistem yang andal terhadap pemalsuan karena catatan transaksi disimpan di seluruh rantai. Ketika kedua teknologi ini digabungkan dalam sistem e-certificate maka keamanan sistem akan ditingkatkan karena setiap e-certificate dienkripsi dan dilindungi melalui blockchain dengan menjaga privasi, efisiensi dan integritas data.

Penelitian terkini di bidang pendidikan yang berkaitan dengan sertifikat di antaranya pengembangan sistem berbasis blockchain untuk manajemen sertifikat elektronik. metode yang digunakan adalah Analisis kebutuhan sistem, desain sistem berbasis blockchian, pengembangan smart contract dan integrasi blockchain ke dalam sistem manajemen sertifikat. Teknik pengujian yang dilakukan adalah pengujian sistem, pengujian kecepatan dan efisiensi, pengujian keamanan sehingga hasil yang di dapat bahwa evaluasi sistem manajemen sertifikat elektronik menggunakan smart contract berbasis blockchain adalah efektif dan aman [14]. Implementasi latform untuk melacak pencapaian pembelajaran di luar transkrip dan sertifikat dengan mempertahankan hash digital dan mengelola akses peran melalui penggunaan smart contract di blockchain, tetapi waktu yang dibutuhkan untuk menulis catatan pembelajaran pembelajaran ke blockchain tidak didasarkan pada akses waktu nyata [15].

Penelitian Seong-Kyu pada tahun 2022 mengimplementasikan model empiris untuk aplikasi sertifikat diploma menggunakan pendekatan Mask CNN untuk mengelompokkan node dan konsensus berbasis blockchain untuk mencegah pemalsuan sertifikat akademik dan memastikan keamanan dan keandalan yang tinggi [16]. Penelitian Manjula dkk pada tahun 2022 membahas analisis kinerja pembuatan e-certificate dan verifikasi menggunakan teknologi blockchain dan IPFS. Pengembangan algoritma untuk generasi dan validasi sertifikat, serta pembuatan antarmuka aplikasi untuk otoritas perguruan tinggi dan perusahaan. Hasil yang didapatkan adalah Penggunaan IPFS mengurangi waktu yang dibutuhkan untuk menghasilkan hash transaksi, dan sistem ini dapat meningkatkan keandalan e-certificate [17].

Berdasarkan penelitian di atas, fokus dari penelitian ini adalah tentang pengembangan Non-Interactive ZKP dan smart contract berbasis blockchain.

Obyek yang diteliti adalah sistem manajemen e-certificate. Analisis identifikasi pengguna atau pemangku kepentingan adalah pihak yang terlibat di dalam jaringan terdesentralisasi. Pengguna dan pemangku kepentingan meliputi lembaga pembuat sertifikat, pihak penerima sertifikat dan pihak verifikator. Lembaga pembuat sertifikat akan membuat e-certificate dengan data yang telah divalidasi dan ditanda tangani secara digital serta merekam e-certificate pada blockchain. Lembaga pembuat sertifikat akan menghasilkan pasangan kunci publik/privat yang unik untuk setiap e-certificate. Kunci privat akan diberikan kepada penerima e-certificate secara aman untuk digunakan dalam proses Non-Interactive ZKP. Kunci publik disimpan atau dibagikan dengan cara yang aman dan dapat diakses oleh verifikator untuk memverifikasi klaim tanpa mengungkapkan detail informasi dari pemilik e-certificate. Smart contract digunakan untuk mengeksekusi tindakan secara otomatis seperti penerbitan, verifikasi, pembaruan serta pencabutan e-certificate. Smart contract baru dilakukan ketika memverifikasi dan merekam bukti Non-Interactive ZKP serta memperbarui status e-certificate. Smart contract akan ditempatkan ke dalam jaringan blockchain dan semua data dan transaksi akan disimpan di dalam buku besar terdistribusi.

1.2 Rumusan Masalah

Rumusan masalah yang dibahas dalam penelitian ini adalah:

1. Bagaimana alur proses manajemen e-certificate diterapkan pada teknologi blockchain ?
2. Bagaimana mengintegrasikan Non-Interactive ZKP ke dalam jaringan terdesentralisasi dari sistem blockchain ?
3. Bagaimana penerapan Non-Interactive ZKP dan smart contract berbasis blockchain dapat meningkatkan efisiensi transaksi dengan tetap menjaga privasi pengguna ?
4. Bagaimana evaluasi kinerja dari penerapan Non-Interactive dan smart contract berbasis blockchain dapat meningkatkan keamanan transaksi di dalam sistem manajemen e-certificate ?

1.3 Ruang Lingkup Penelitian

Ruang lingkup yang dibahas pada penelitian ini adalah:

1. Identifikasi pengguna atau pemangku kepentingan dan alur proses bisnis diperoleh dari observasi dan penelitian terkait.
2. Penerapan Non-Interactive ZKP digunakan untuk membuktikan kebenaran klaim e-certificate tanpa mengungkapkan informasi rahasia atau detail informasi dari sertifikat yang berjalan pada jaringan terdesentralisasi.
3. Penerapan smart contract digunakan untuk otomatisasi penerbitan e-certificate kepada enttitas yang berhak, otomatisasi perbaruan atau pembatalan e-certificate dan meningkatkan transparansi dan keamanan karena setiap transaksi atau perubahan yang tercatat dalam blockchain tidak dapat diubah.
4. Simulasi dan pengujian sistem dilakukan pada mesin lokal (docker).

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah mengembangkan sistem manajemen e-certificate dengan menerapkan Non-Interactive ZKP dan smart contract berbasis blockchain yang dapat meningkatkan efisiensi dan keamanan transaksi dengan tetap menjaga privasi pengguna.

1.5 Kontribusi dan Manfaat Penelitian

Kontribusi dan manfaat yang dapat diperoleh dari penelitian inicadalah sebagai berikut:

1. Penelitian dapat digunakan untuk mengembangkan sistem manajemen e-certificate berbasis blockchain dengan mengintegrasikan Non-interactive ZKP untuk menjaga privasi yang efisien.
2. Penelitian ini dapat dijadikan referensi di bidang sains dan praktik dalam menerapkan teknologi blockchain di bidang pendidikan atau pelatihan.

3. Penelitian akan mengukur kinerja dari penerapan gabungan teknologi yaitu kriptografi (Non-Interactive ZKP) dengan blockchain.

Bab 2

Telaah Pustaka

2.1 Blockchain

Setiap peserta blockchain terhubung melalui jaringan P2P (peer to peer). Node klien blockchain membantu peserta bergabung ke jaringan. Setiap node memiliki salinan lokal dari keseluruhan daftar yang terhubung. Saat mengambil daftar untuk pertama kalinya, node menghitung semua hash dan kemudian memverifikasi setiap blok baru untuk memastikan integritas blok. Pasangan kunci asimetri kriptografi digunakan untuk mengidentifikasi identitas peserta. Kunci publik berfungsi untuk identitas publik sedangkan kunci pribadi digunakan untuk menandatangani transaksi dan memastikan keaslian. Peserta lain dapat memverifikasi tanda tangan dengan menggunakan kunci publik yang sesuai. Setelah menambah data ke blockchain, sebuah node mengirimkan permintaan transaksi melalui sebagian besar data seperti alamat pengirim dan penerima, transaksi data dan tanda tangan pengirim. Permintaan transaksi ini kemudian akan diproses oleh setiap node atau validator [18].

Strategi penerapan blockchain tergantung pada domain aplikasinya. Tabel 2.1menjelaskan tiga jenis blockchain berdasakan domain aplikasi.

Tabel 2.1: Jenis blockchain [19]

Properti	**Otoritas Blockchain**		
	Publik	**Konsorsium**	**Pribadi**

Properti	**Otoritas Blockchain**		
	Publik	**Konsorsium**	**Pribadi**
Tipe kewenangan	Konsensus bersifat publik	Konsensus dikelola oleh kelompok peserta yang berpartisipasi	Konsensus dikelola oleh pemilik tunggal
Validasi transaksi	Siapa saja (penambang)	Daftar node yang diizinkan (validator)	
Algoritma konsensus	Tanpa izin (PoW, PoS, PoET)	Dengan izin (PBFT, Tendermint, PoA, etc.)	
Proses interpretasi transaksi	Setiap simpul	Setiap simpul (tanpa izin) atau Daftar simpul yang telah ditentukan sebelumnya (dengan izin)	
Kekekalan data	Ya	Ya	
Jumlah transaksi	Rendah	Tinggi	
Skalabilitas jaringan	Tinggi	Rendah ke sedang	
Infrastruktur	Sangat terde-sentralisasi	Desentralisasi	Distribusi
Fitur	Resistensi terhadap sensor tidak diatur, dukungan lintas-batas aset asli adalah identitas anonim	Diterapkan untuk bisnis yang sangat teregulasi (identitas yang diketahui, standar hukum, dll.) Hasil transaksi yang efisien, transaksi tanpa biaya, aturan infrastruktur lebih mudah dikelola, perlindungan yang lebih baik terhadap gangguan eksternal	

Properti	**Otoritas Blockchain**		
	Publik	**Konsorsium**	**Pribadi**
Contoh teknologi aplikasi	Bitcoin, Ethereum, Ripple, dll	MultiChain, Quorum, HyperLedger, Ethermint, Tendermint, dll	

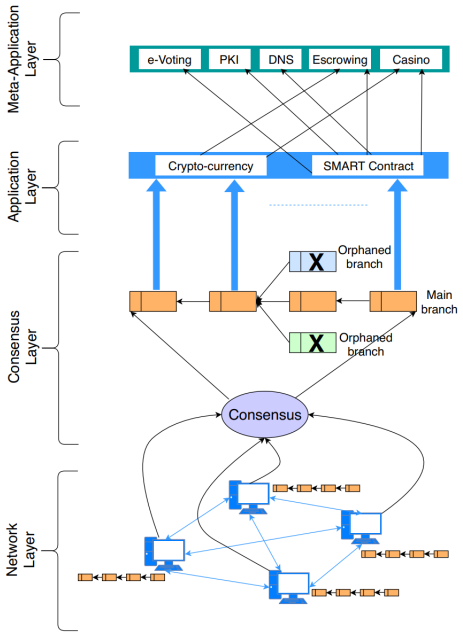
Sistem blockchain terdiri dari beberapa bagian dan melakukan berbagai hal seperti mengumpulkan transaksi, menyebarkan blok, menambah, mencapai konsensus dan menjaga buku besar mata uang kripto utama [20]. Komponen-komponen ini dapat dikelompokkan berdasarkan fungsinya menggunakan lapisan berbeda. Merancang sistem blockchain menggunakan pendekatan berlapis akan jauh lebih modular dan mudah perawatannya. Misalnya, jika bug ditemukan pada salah satu komponen dalam salah satu lapisan sistem blockchain, maka hanya akan mempengaruhi fungsionalitas lapisan tersebut, sementara lapisan lainnya tidak akan terpengaruh. Penelitian Md. Sadek dkk tahun 2020 medefinisikan empat lapisan blockchain yaitu meta aplikasi, aplikasi, konsensus dan jaringan (Gambar 2.1). Di bawah ini adalah fungsi singkat dari lapisan blockchain:

- Lapisan meta aplikasi: lapisan ini digunakan untuk menyediakan overlay di atas lapisan aplikasi untuk mengeksploitasi interpretasi semantik sistem blockchain untuk tujuan lain pada domain aplikasi lain. Misalnya, Bitcoin telah diujicobakan untuk diadopsi di beberapa domain aplikasi seperti DNS yaitu sistem penamaan terdesentralisasi (Namecoin [21]), catatan hash dengan stempel waktu yang tidak dapat diubah dan terdesentralisasi (Proof of Existence), dan PKI yaitu infrastruktur kunci publik (Certcoin).

- Lapisan aplikasi: lapisan ini mendefiniskan interpretasi semantik dari sistem blockchain. Contoh interpretasi semantik adalah mendefinisikan mata uang kripto dan kemudian menyiapkan protokol bagaimana mata uang tersebut dapat dipertukarkan antar entitas yang berbeda. Contoh lainnya adalah membuat protokol untuk memelihara mesin negara yang mewujudkan kemampuan pemrograman dalam blockchain, yang dapat dieksploitasi untuk membuat dan menyebarkan kode yang tidak dapat diubah (yang disebut smart contract). Aplikasi ini juga mendefinisikan mekanisme pemberian penghargaan dalam sistem blockchain.

- Lapisan konsensus: lapisan ini bertanggung jawab untuk menyediakan mekanisme konsensus terdistribusi di blockchain yang pada dasarnya mengatur urutan blok. Komponen penting dari lapisan ini adalah protokol pembuktian (misalnya, bukti kerja dan bukti kepemilikan) yang digunakan untuk memverifikasi setiap blok, yang pada akhirnya digunakan untuk mencapai konsensus yang diperlukan dalam sistem.

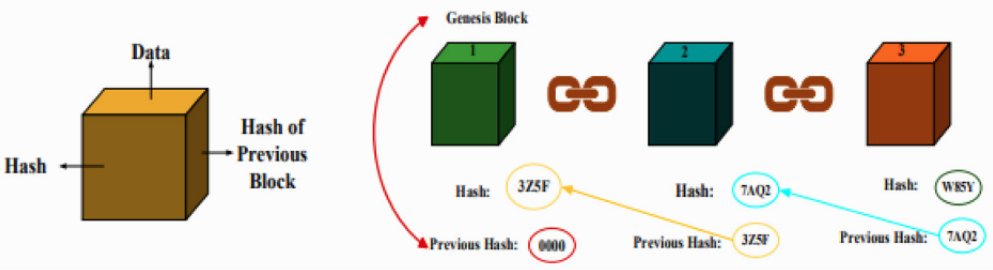
- Lapisan jaringan: lapisan ini bertanggung jawab atas semua operasi jaringan termasuk bergabung dalam jaringan P2P yang mendasarinya, mengikuti jaringan yang mendasarinya dan menerima transaksi dan blok.



Gambar 2.1: Ilustration of Blockchain Layer [22]

Algoritma hashing SHA-1, SHA-2 dan SHA-256 adalah algoritma paling aman dari teknologi blockchain karena konsistensi yang khas dan pengiriman keluaran unik sesuai data masukan. Untuk mengidentifikasi sebuah transaksi, hash adalah kunci unik yang memiliki potensi untuk secara bersamaan menggambarkan seseorang dalam rantai pasokan. SHA adalah badan keamanan nasional yang awanya diproyeksikan untuk federal standar pemrosesan informasi Amerika Serikat. Algoritma memastikan integritas file dan pesan selama transfer, verifikasi kata sandi dan pengenalan data. Panjang pesan SHA-1 kurang dari 264 bit, ukuran data 32 bit dan blok 512 dengan

160 teks yang dapat diproses. Teknologi blockchain terdiri dari campuran elektronik dari blok-blok, setiap blok terdiri dari hash dan data dari blok sebelumnya. Gambar 2.3 menunjukkan komponen hash blok dan jaringan blockchain.



Gambar 2.2: Komponen hash blok dan jaringan blockchain [23]

2.1.1 Properti Blockchain

Sebuah blockchain menunjukkan beberapa properti yang menjadikannya kandidat yang cocok untuk beberapa domain [24]. Berikut ini adalah properti blockchain:

- Konsensus terdistribusi pada rantai (chain state): salah satu sifat penting dari setiap blockchain adalah kemampuannya unruk mencapai konsensus terdistribusi mengenai keadaan rantai tanpa bergantung pada pihak ketiga yang terpercaya. Hal ini membuka peluang untuk membangun dan memanfaatkan sistem di mana status dan interaksi dapat diverifikasi oleh penambang di sistem blockchain publik atau entitas resmi di sistem blockchain hibrid atau pribadi.

- Kekekalan dan ireversibilitas keadaan rantai: konsesus terdistribusi yang melibatkan banyak node memastikan bahwa status rantai menjadi tidak dapat diubah setelah jangka waktu tertentu. Hal ini juga berlaku untuk smart contract yang memungkinkan pengembangan dan pengoperasian program komputer yang tidak dapat diubah.

- Persistensi data (transaksi): data dalam blockchain disimpan secara terdistribusi, memastikan persistensi data selama ada node yang berpartisipasi dalam jaringan P2P.

- Asal data: transaksi adalah mekanisme yang memungkinkan proses penyimpanan data di blockchain manapun. Setiap transaksi harus ditandatangani secara digital dengan menggunakan kriptografi kunci publik yang memastikan bahwa sumber data adalah asli. Dengan menngabungkannya dengan kekekalan dan ireversibilitas blockcahin, akan memberikan instrumen non-penyangkalan yang kuat untuk data apa pun di dalam blockchain.

- Kontrol data terdistribusi: blockchain memastikan bahwa data yang disimpan dalam rantai atau diambil dari rantai dapat dilakukan secara terdistribusi dan tidak menunjukkan satu titik kegagalan pun.

- Akuntabilitas dan transparansi: ketika keadaan rantai dan interaksi antar entitas dapat diverifikasi oleh entitas resmi mana pun, blockchain mendorong akuntabilitas dan transparansi.

2.1.2 Konsensus Blockchain

Sistem blockchain adalah sistem terdistribusi yang mengandalkan algoritma konsensus untuk memastikan kesepakatan tentang status data tertentu di antara node yang didistribusikan. Algoritma konsensus adalah komponen utama yang secara langsung menentukan kinerja dan perilaku sistem. Merancang dan menerapkan protokol konsensus adalah tugas yang menantang karena perlu mempertimbangkan masalah penting seperti ketahanan terhadap kegagalan node, perilaku node, partisi jaringan, latensi jaringan dan input yang rusak [25]. Node yang terdistribusi harus memenuhi dua persyaratan penting untuk mencapai dan mempertahankan konsensus yaitu keadaan mesin (state machine) deterministik dan protokol konsensus untuk menyebarkan masukan secara tepat waktu dan memastikan siaran atom diantara node yang berpartisipasi. Tabel 2.2menunjukkan sifat-sifat siaran atom dalam konsesus terdistribusi.[26] Tabel 2.3 menunjukkan properti protokol konsensus terdistribusi.

Mekanisme konsensus umum dalam sistem blockchain mencakup PoW (Proof of Work), PoS (Proof of Stake), DPoS (Delegated Proof of Stake), PBFT (Practical Byzantine Fault Tolerance) dan RAFT. Beberapa mekanisme konsensus tidak semua cocok untuk diterapkan pada semua skenario aplikasi [27].

Tabel 2.2: Siaran atom properti protokol konsensus terdistribusi

Properti	**Catatan**
Validitas	Hal ini menjamin bahwa jika sebuah pesan disiarkan oleh node yang valid, maka pesan terssebut akan disertakan dengan benar dalam protokol konsensus.
Perjanjian	Hal ini untuk menjamin bahwa jika sebuah pesan dikirimkan ke node yang valid, pesan tersebut pada akhirnya akan terkirim ke semua node yang valid.
Integritas	Hal ini untuk memastikan bahwa pesan disiarkan hanya sekali oleh node yang valid.
Total Order	Hal ini untuk memastikan bahwa semua node menyetujui urutan semua order yang dikirimkan.

1. Konsensus Proof of Work (PoW)

   PoW adalah salah satu mekanisme konsensus paling umum dalam blockchain dan digunakan oleh sebagian besar blockchain publik. PoW diterapkan pada bitcoin, di mana penambang menerima imbalan atas kerja mereka berdasarkan komputasinya. Algoritma hash yang ada di blockchain biasanya digunakan untuk menghitung nilai hash [28]. Nilai hash tidak dihitung secara terpisah untuk setiap transaksi, dihitung secara konsisten setelah pembuatan blok. Algoritma hash SHA-256 membutuhkan banyak sumber daya komputasi. Penambang yang memiliki kekuatan komputasi yang lebih besar dapat mengemas transaksi untuk menghasilkan blok lebih cepat. Namun, blok yang dihasilkan hanya oleh satu penambang teridentifikasi, hal ini mengakibatkan pemborosan sumber daya yang sangat besar. Gambar 2.3 menunjukkan proses dari konsensus PoW. Blok akan dibuat jika nilai hash penambang sama dengan nilai target. Jika tidak, penambang akan menyesuaikan nonce untuk menghitung ulang. Fitur mekanisme konsensus PoW dapat menjamin keamanan penambang.

   - Kelebihan dari mekanisme konsensus PoW adalah sebagai berikut:

     (a) Desentralisasi yang menyeluruh.

Tabel 2.3: Properti protokol konsensus terdistribusi

Properti	**Catatan**
Keamanan / Konsistensi	Protokol konsensus dianggap aman (atau konsisten) hanya ketika semua node menghasilkan keluaran valid yang sama sesuai dengan aturan protokol untuk siaran atom yang sama.
Ketersediaan	Jika semua node yang berpartisipasi dan tidak mengalami kesalahan menghasilkan keluaran (menunjukkan penghentian protokol), maka protokol tersebut dianggap aktif.
Toleransi Kesalahan	Hal ini menunjukkan kemampuan jaringan untuk bekerja sebagaimana mestinya di tengah kegagalan node

(b) Untuk menjamin keamanannya, biaya serangan lebih tinggi daripada penambang asli.

(c) Proses konsensus dapat menerima banyak node.

(d) Semakin besar daya komputasi yang digunakan suatu node, semakin besar kemungkinan node tersebut mendapat hadiah blok baru.

- Kekurangan dari mekanisme konsensus PoW adalah sebagai berikut:

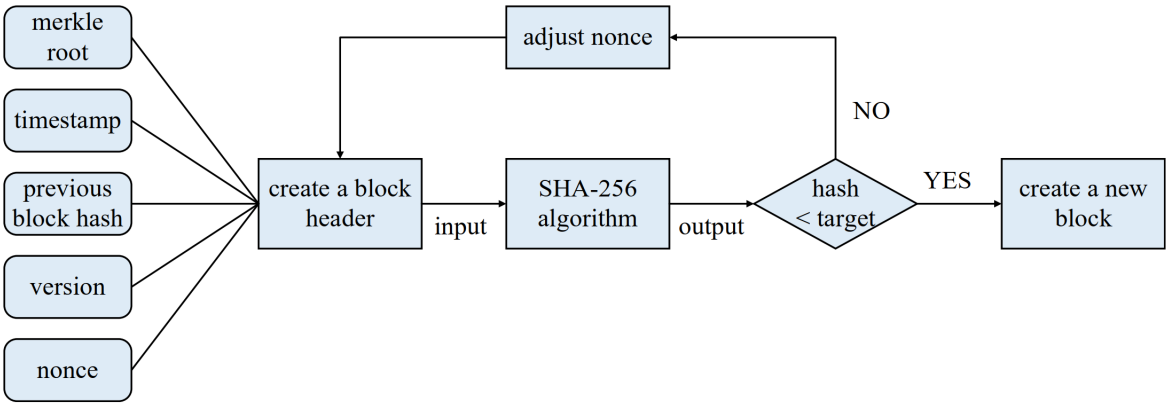
  (a) Banyak tenaga komputasi dan energi yang diperlukan untuk penambangan.

  (b) Konsensus dicapai dalam waktu yang lama dan waktu konfirmasi blok sulit dipersingkat untuk menjamin desentralisasi.

  (c) Untuk membuat blockchain baru harus menemukan algoritma hash baru atau menghadapi serangan kekuatan komputasi bitcoin.

Untuk mengatasi permasalahan yang ada di dalam konsensus PoW, beberapa solusi seperti . The Greedy Heaviest-Observed Sub-Tree (GHOST) [29] mengeksploitasi strategi sub-pohon untuk menghasilkan rantai

utama untuk penambang egois. Ethereum [28] menggunakan pohon awalan merkel dan bukan pohon merkel, dan memperkenalkan struktur blok paman yang secara signifikan mengurangi waktu pembuatan blok, sehingga meningkatkan throughput hingga 15 TPS. Bitcoin-NG [30] memperbaiki struktur blok dengan membaginya menjadiblok kunciuntuk pemilihan pemimpin dan mikroblok karena memuat entri buku besar, memberikan ide baru untuk perluasan blockchain.



Gambar 2.3: Mekanisme konsensus PoW [31]

2. Konsensus Proof of Stake (PoS)

   Mekanisme konsensus PoS menghemat waktu dan daya komputasi dibandingkan dengan mekanisme konsensus PoW. Blackcoin dan Ethereum adalah contoh proyek berbasi blockchain yang secara bertahap beralih dari PoW ke PoS. Dalam konsensus PoS semua rencana harus disetujui oleh penambang dengan mayoritas saham. Gambar 2.4 menunjukkan proses dari konsensus PoS yang dijabarkan sebagai berikut:

   (a) Blokir pemilihan produsen. Penambang menjamin koin mereka untuk dijadikan mata uang. Semakin panjang mata uang, semakin besar kemungkinan penambang menjadi produsen blok, yang memenuhi kesenjangan di mana hash (block_header) adalah nilai hash dan coinage adalah jumlah dikalikan dengan sisa waktu penggunaan koin yang dimiliki seseorang penambang. Koin mempengaruhi kemampuan menghitung nilai hash daripada daya komputasi. Oleh karena itu, masalah pemborosan sumber daya dalam jumlah besar diselesaikan melalui mekanisme konsensus

PoS.

(b) Blokir ususlan. Produsen blok mengumpulkan transaksi di blockchain. Kemudian transaksi yang sah tersebut dikemas ke dalam blok baru yang akan disiarkan di sistem blockchain.

(c) Validasi blok. Node verifikasi memverifikasi blok baru. Jika verifikasi berhasil, blok ditambahkan untuk memperbarui blockchain. Kemudian putaran konsensus berikutnya dimulai. Jika tidak, blok yang diusulkan akan dibuang dan produsen blok baru dipilih di blockchain.

Kelebihan dari konsensus PoS adalah sebagai berikut:

(a) Menghemat banyak daya komputasi dan energi karena node tidak mengonsumsi daya komputasi ekstra untuk penambang.

(b) Menghemat waktu dalam menghasilkan blok dan mencapai konsensus, sehingga meningkatkan efisiensi konsensus.

Kekurangan dari konsesnsus PoS adalah sebagai berikut:

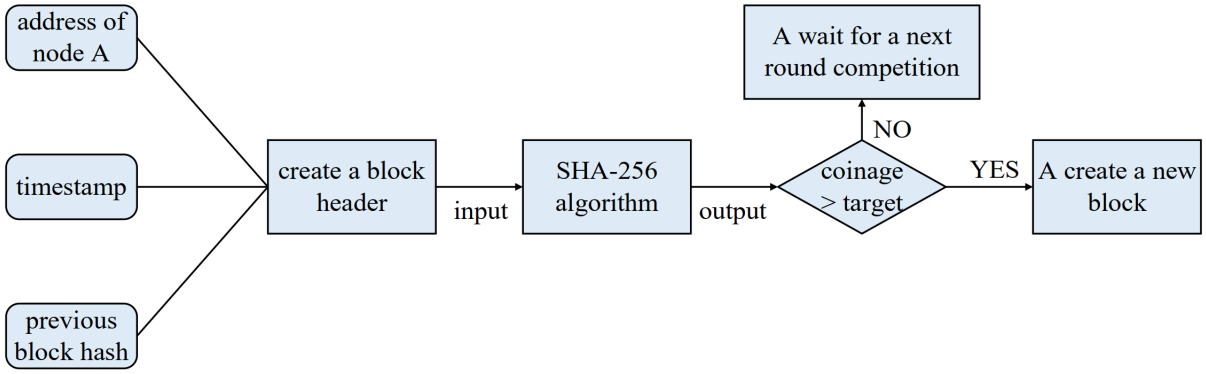
(a) Algoritma rumit dan sulit diimplementasikan.

(b) Penambang menyimpan token untuk mendapatkan keuntungan dibandingkan menjualnya, sehingga membuat penambang yang memiliki lebih banyak token rentan.

(c) Penambang berbiaya rendah dan mudah disrang, sehingga keamanannya buruk.

Untuk mengatasi permasalahan yang ada di konsensus PoS, beberapa solusi seperti: Blackcoin [**?**] telah meningkatkan ketimpangan yang harus dipenuhi untuk penambangan sebagai proofhash < target * koin. Node harus tetap online untuk akumulasi taruhan guna menyelesaikan serangan koin. Ouroboros [32] menambahkan konsep periode. Jika node untuk menghasilkan blok tidak online pada setiap periode, putaran tidak menghasilkan blok. Verifikator memverifikasi legalitas transaksi dan mengemas transaksi yang sah ke node. Oleh karena itu, serangan jarak jauh teratasi.

3. Konsensus Delegated Proof of Stake (DPoS)



Gambar 2.4: Mekanisme konsensus PoS [31]

Konsensus DPoS adalah evolusi dari konsensus PoS. Setiap pemegang saham memiliki pengaruh sesuai dengan jumlah saham mereka, dan suara 51% pemegang saham tidak dapat diubaj dan mengikat. Setiap pemegang saham juga dapat memberikan hak suaranya kepada delegasi untuk mencapai persetujuan 51%. Setiap delegasi diberi waktu untuk menghasilkan blok. Blok baru dapat dibuat setiap 30 detik di DPoS. Delegasi akan menerima pembayaran sebesar 10% dari biaya transaksi yang terdapat dalam satu blok. Jika seorang delegasi tidak memenuhi tanggung jawabnya, seperti tidak menghasilkan blok, hak suaranya akan dicabut. Selanjutnya, delegasi baru akan dipilih untuk menggantikannya di jaringan blockchain. Gambar 2.5 menunjukkan proses dari konsensus DPoS.

Kelebihan dari konsensus DPoS adalah sebagai berikut:

(a) Menghemat energi dan daya komputasi karena mirip dengan konsensus PoS.

(b) Menghemat waktu dalam menghasilkan blok baru dan meningkatkna efisiensi pencapaian konsensus.

(c) Konsensus efektif dapat dicapai melalui verifikasi delegasi terpilih.

Kekurangan dari konsensus DPoS adalah sebagai berikut:

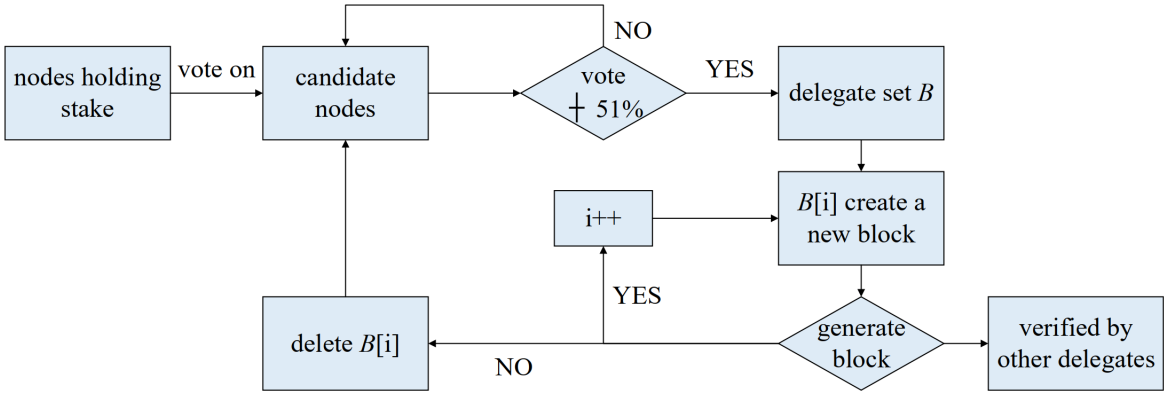
(a) Kurang terdesentralisasi

(b) Masih memerlukan koin dalam mekanisme konsensus DPoS.

(c) Node dengan hak tinggi dapat memilih dirinya sendiri dan menyuap node lain untuk memilihnya dalam proses pemilihan delegasi

yang menyebabkan kecurangan.

Mekanisme konsensus DPoS dapat memverifikasi transaksi pada tingkat kedua dan memberikan keamanan yang lebih tinggi dibandingkan PoS yang ada dalam waktu singkat, menahan serangan dengan kepemilikan kurang dari 51%. Setiap perubahan pada sistem (termasuk pembaruan versi, penambahan fungsi, modifikasi taruhan, dll.) harus disetujui oleh lebih dari 51% pemegang saham. Blok-blok tersebut dihasilkan secara berurutan, artinya probabilitas transaksi dari awal siaran hingga lebih dari 1/2 blok yang dikonfirmasi adalah 99,9%. Dalam keadaan normal, pemblokiran baru dianggap tidak dapat diubah jika lebih dari separuh saksi memberikan konfirmasi. Throughput EOS bisa mencapai jutaan, namun pemilihan saksi menghabiskan banyak sumber daya sehingga menghasilkan throughput yang tidak memuaskan. Dan pembuatan blok tersebut sangat bergantung pada 21 saksi sehingga menimbulkan masalah sentralisasi.



Gambar 2.5: Mekanisme konsensus DPoS [31]

4. Konsensus PBFT

PBFT adalah protokol replikasi mesin status seminalis, yang mengharuskan status dipertahankan olrh semua node sistem. PBFT mengizinkan tidak lebih dari sepertiga jumlah total node dalam jaringan sebagai node Bizantium. Ini terutama terdiri dari tiga protokol dasar, di antaranya protokol konsistensi adalah intinya [33]. Konsensus PBFT, klien dan node konsensus (termasuk node utama dan cadangan) bekerja sama untuk menyelesaikan proses konsensus. Spesifik, seluruh node

jaringan memilih blok penghasil node utama. Node utama akan menerima permintaan klien. Setelah pihak utama dan cadangan menyetujui permintaan, akan diputuskan apakah permintaan tersebut dapat dilaksanakan atau tidak. Gambar 2.6 menunjukkan proses dari konsensus PBFT yang dijabarkan sebagai berikut:

(a) Permintaan (request): Klien mengirimkan permintaan ke node utama.

(b) Pra-persiapan (pre-prepare): Node utama menetapkan nomor urut yang sesuai dengan permintaan. Kemudian pesan pra-persiapan dibuat dan disiarkan ke node cadangan.

(c) Persiapan (prepare): Setelah menerima pesan pra-persiapan, setiap node cadangan menyiarkan sebuah pesan persiapan ke node cadangan lainnya. Semua node cadangan menyiarkan pesan satu sama lain.

(d) Commit: Semua node memvalidasi pesan dan menyiarkan pesan commit. Permintaan akan dieksekusi jika verifikasi berhasil.

(e) Reply: Klien menunggu tanggapan dari node yang berbeda, Jika klien menerima respon yang benar f + 1 pesan balasan yang identik (f adalah jumlah bizantium), ini mengindikasikan bahwa node-node dalam jaringan telah mencapai konsensus.

Kelebihan dari konsensus PBFT adalah sebagai berikut:

(a) Konsistensi dan kebenaran hasil konsensus yang tinggi.

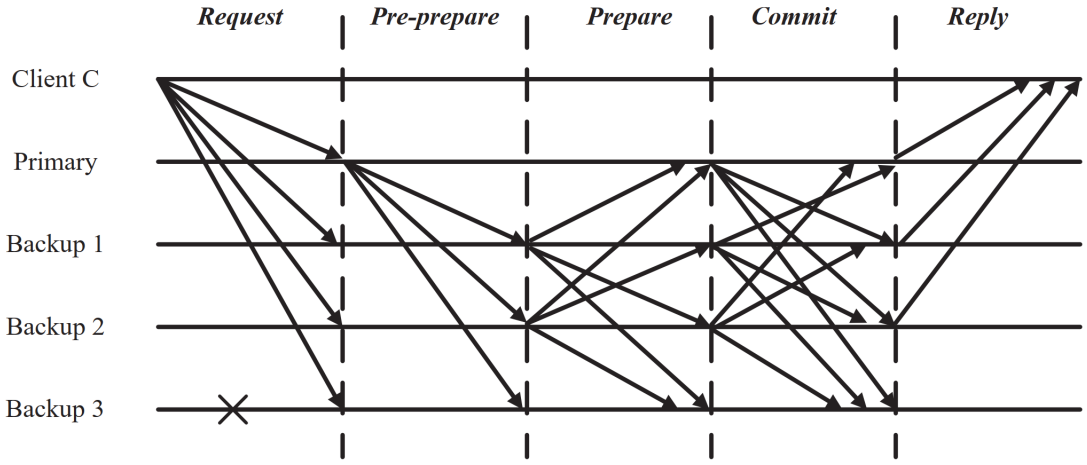
(b) Waktu konfirmasi konsensus cepat.

Kekurangan dari konsensus PBFT adalah sebagai berikut:

(a) Kompleksitas algoritma yang tinggi.

(b) Efidiensi konsensus menjadi rendah jika terlalu banyak node yang bergabung. Node dapat mengakses sistem dan menyiarkan node komunikasi hanya setelah diotentikasi, sehingga menghasilkan skalabilitas mekanisme konsensus PBFT yang buruk. Node utama mengurutkan pesan permintaan dan mengusulkan blok dan

mengirimkan pesan pra-persiapan ke semua node konsensus dengan waktu kompleksitas O(n). Karena penerapan mode komunikasi banyak ke banyak, setiap cadangan harus menyiarkan pesan persiapan dan commit dengan kompleksitas waktu O(2n). Kemudian, kompleksitas waktu dari semua pencadangan adalah O(2n) x O(n) = O($2n^2$). Oleh karena itu, kompleksitas waktu dari protokol konsistensi adalah O(n^2). Selain itu, kinerja protokol konsistensi menurun secara signifikan seiring dengan bertambahnya jumlah node.



Gambar 2.6: Mekanisme konsensus PBFT [31]

5. Konsensus RAFT

   RAFT adalah protokol konsistensi yang kuat untuk mencapai konsensus di bawah kegagalan non-bizantium [34]. Ini menjamin bahwa dalam kasus kegagalan node-bizantium, sistem masih dapat menangani permintaan klien. Klaster RAFT biasanya memiliki lima node, sehingga sistem kehilangan dua node. Setiap node mempunyai tiga keadaan, yaitu pemimpin, pengikut dan kandidat. Pemimpin bertanggung jawab untuk menyinkronkan log, mengatasi permintaan klien dan memantau node tetap berhubungan dengan pengikut. Pengikut, saat memulai, semua node berada dalam status pengikut. Jika node tidak menerima pesan pemimpin, maka node akan menjadi kandidat. Kandidat bertanggung jawab untuk memilih. Setelah mengubah pengikut menjadi kandidat, semua node memulai pemilihan. Setelah pemimpin terpilih

maka calon tersebut mengubah statusnya menjadi pemimpin. Gambar 2.7 menunjukkan proses dari konsensus RAFT dan terdiri dari dua tahap yaitu sebagai berikut:

(a) Pemilihan pemimpin
    i. Semua node dimulai sebagai pengikut dan pemilihan dimuali.
    ii. Jika pengikut tidak menerima permintaan utama dari pemimpin, node tersebut menjadi node kandidat dan tetap demikian sampai seorang pemimpin terpilih atau sampai putaran pemilihan baru dimulai.
    iii. Jika lebih dari separuh node setuju makan kandidat tersebut akan mengirimkan permintaan suaranya ke node lain dan menjadi pemimpin. Jika pemilihan berakhir tanpa pemenang maka pemilihan baru dimuali.
    iv. Setelah pemilihan berakhir, pemimpin secara berkala mengirimkan inti ke node lain untuk menunjukkan bahwa pemimpin masih berjalan. Kemudian waktu pemilihan untuk node ini direset.

(b) Replikasi log
    i. Klien menyampaikan perintah kepada pemimpin. Setelah menerima perintah, pemimpin menambahkan perintah ke log lokal. Jika status perintah tidak di commit maka mesin replikasi tidak akan menjalankan perintah.
    ii. Pemimpin kemudian menyalin perintah ke node lain dan menunggu mereka menulis perintah ke log. Jika node yang ada gagal, pemimpin akan mencoba lagi hingga semua node telah menyimpan perintah ke log. Kemudian pemimpin menyampaikan perintah dan mengembalikan hasilnya kepada klien.

Pemimpin mengirimkan perintah ke node lain melalui inti berikutnya. Node lain kemudian menerapkan perintah dari pemimpin ke status mesin. Kemudian setiap node tetap konsisten.

Kelebihan dari konsensus RAFT adalah sebagai berikut:

(a) Menawarkan efisiensi transmisi jaringan dan konsensus yang tinggi.

(b) Menghemat energi karena tidak ada penambangan.

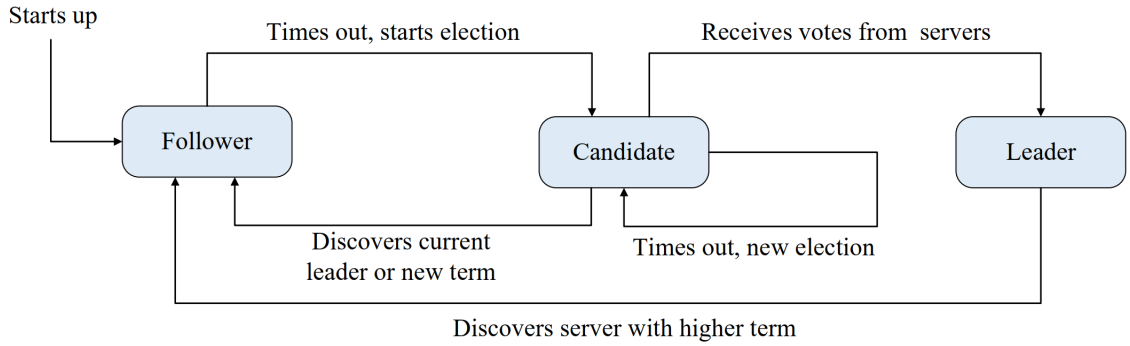
(c) Algoritma lebih sederhana karena tidak mempertimbangkan node-bizantium.

Kekurangan dari konsensus RAFT adalah sebagai berikut:

(a) Desentralisasi tidak tuntas karena terlalu bergantung pada pemimpin.

(b) Terdapat percabangan singkat dalam jaringan karena sejumlah fluktuasi atau persaingan jaringan yang menyebabkan konfirmasi berulang.

(c) Performa buruk dalam skenario konkurensi tinggi karena pemungutan suara berurutan.



Gambar 2.7: Mekanisme konsensus PBFT [31]

Gambar 2.8 menunjukkan hasil perbandingan mekanisme konsesus.

	PoW	PoS	DPoS	PBFT	RAFT
Decentralization	Complete	Complete	Complete	Incomplete	Incomplete
Numbers of nodes	Unlimited	Unlimited	Unlimited	Limited	Unlimited
Energy consumption	High	Low	Low	Low	Low
Block generation	Long	Short	Short	Short	Short
Transaction confirmation	Long	Short	Short	Immediate	Immediate
Scalability	High	High	High	Low	Low
Throughput	Low	Low	High	High	High
Consistency	Probability	Probability	Probability	Finality	Finality
Fault tolerance	50%	50%	50%	33%	50%
Permission	No	No	No	Yes	Yes
Example	Bitcoin	Peercoin	EOS	Tendermint	Etcd

Gambar 2.8: Mekanisme konsensus PBFT [31]

2.2 Ethereum

Ethereum adalah platform terbuka dan terdesentralisasi yang menampilkan kelengkapan turing dan mendukung berbagai aplikasi turunan. Sebagian besar smart contract dan jaringan terdesentralisasi dibuat dengan menggunakan ethereum [35]. Jika blockchain bitcoin dianggap sebagai jaringan pembayaran global, maka ethereum akan menjadi sistem komputasi global. Ethereum adalah sebuah platform terbuka yang mirip dengan Android (dikembangkan Google). Ini menyediakan infrastruktur yang memungkinkan pengembang untuk membuat aplikasi. infrastruktur dikembangkan dan dikelola oleh pengembang ethereum. Karakteristik utama ethereum adalah sebagai berikut:

1. Tidak dapat dirusak, pihak ketiga tidak dapat memodifikais data apapun.

2. Aman, kesalahan yang berasal dari faktor personil dapat dihindari.

3. Permanen, blockchain tidak berhenti beroperasi meskipun sebuah komputer atau server individu mengalami kerusakan.

EVM (Ethereum Virtual Machine) adalah blockchain yang dapat diprogram. EVM memungkinkan pengembang untuk menjalankan program apa pun dengan cara yang mereka inginkan. Pengembang menginstruksikan EVM untuk menjalankan aplikasi dengan menggunakan bahasa tingkat tinggi yang

disebut solidity . Solidity adalah bahasa pemrograman yang digunakan untuk mrngimplementasikan smart contract dan mirip seperti JavaScript. Setelah smart contract yang diprogram dengan solidity selesai, sebuah kompiler yang disebut solc diperlukan untuk mengubah kode solidity menjadi bytecode kontrak yang kemudian ditafsirkan oleh EVM, Selanjutnya instruksi yang telah dikompilasi digunakan dalam ethereum.

2.3 Smart contract

Smart contract adalah logika dan kode khusus yang disebarkan dan dijalankan dalam lingkungan virtual platform blockchain yang mengatur transaksi yang didigitalkan dan dikodifikasikan antar akun. Smart contract membantu dalam mentransfer aset digital antar akun sebagai transaksi atom. Smart contract sangat mirip dengan kelas berorientasi objek karena dapat membuat dan menggunakan objek dari kelas lain. Keunggulan dari smart contract dapat membuat instance dari kontrak dan menjalankan fungsi untuk melihat dan memperbaharui data kontrak bersama dengan eksekusi beberapa logika [18].

Tujuan dari smart contract dalam blockchain adalah mendukung pengelolaan siklus lengkap dari kontrak legal yang cerdas termasuk pembuatan template dokumen legal dan perjanjian oleh pihak-pihak yang terkait yang bersifat transparan dan menjadikan efisiensi komersial, menurunkan biaya transaksi serta memungkinkan transaksi anonim.Smart contract dapat menambah atau membaca data, tetapi memperbaharui data sebenarnya merupakan fungsi penambahan data yang mengubah keadaan saat ini. Smart contract paling baik digunakan untuk membaca status saat ini, menjalankan logika pada status tersebut dan memperbarui (menambahkan)status. Klien smart contract biasanya melakukan logika tingkat tinggi aplikasi dan menyakinan UX. Klien tidak hanya bertindak sebagai antarmuka ke smart contract, namun dalam banyak hal, mewakili aplikasi kepada pengguna.

Cara kerja smart contract pada blockchain, di antaranya sebagai berikut:

1. Pembuat kontrak : Seorang pengembang menulis kode smart contract yang mencakup aturan dan ketentuan transaksi atau perjanjian.

2. Penyebaran di blockchain : Smart contract tersebut kemudian diterbitkan ke blockchain. Setelah diterbitkan, kontrak tersebut menjadi

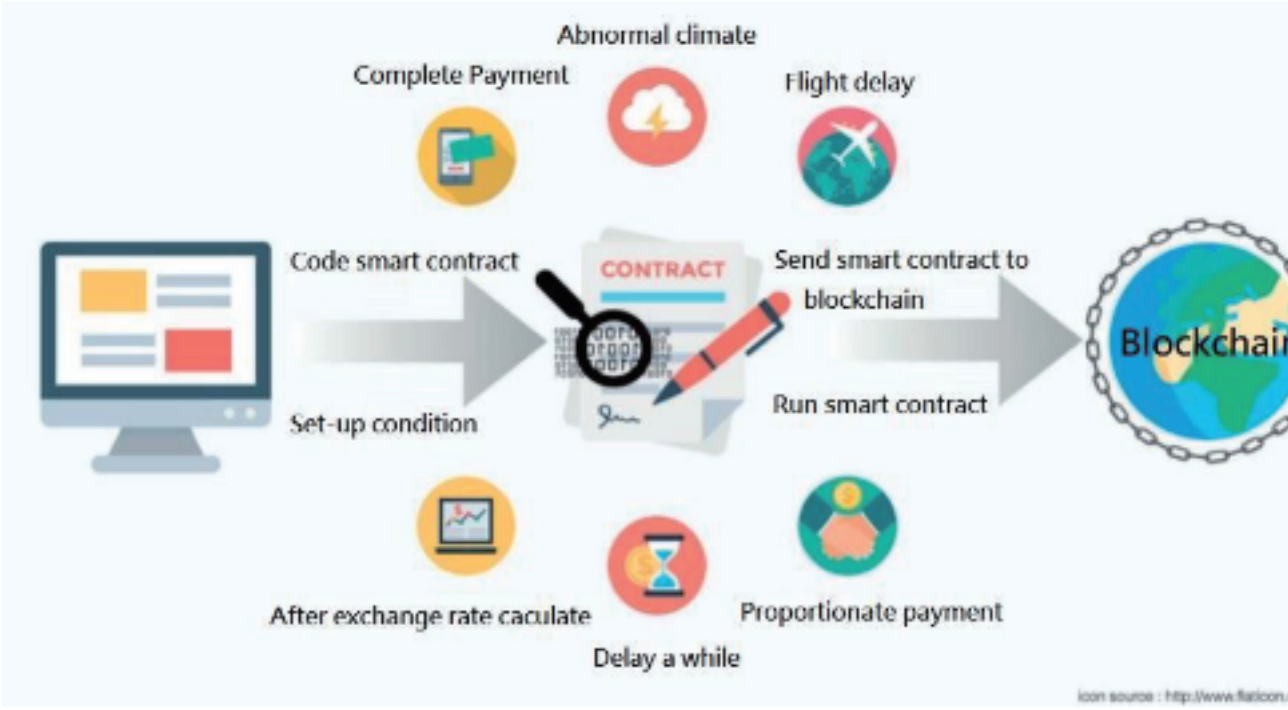
tidak dapat diubah dan dapat diakses oleh siapa saja di jaringan.

3. Pemicu eksekusi : Smart contract dieksekusi secara otomatis ketika kondisi yang ditentukan dalam kontrak terpenuhi. Ini bisa berupa penerimaan pembayaran, pencapaian tanggal tertentu atau memenuhi syarat lain yang telah ditentukan dalam kode.

4. Verifikasi dan eksekusi : Transaksi yang dihasilkan oleh eksekusi smart contract diverifikasi oleh jaringan blockchain dan kemudian ditambahkan ke dalam blockchain sebagai blok baru. Ini menjamin keamanan dan ketidakberubahan catatan transaksi.

5. Otomatisasi dan efisiensi : Smart contract menghilangkan kebutuhan untuk perantara, mengurangi biaya transaksi dan meningkatkan efisiensi dengan menjalankan proses secara otomatis.

Smart contract yang digunakan dalam blockchain disalin ke setiap node untuk mencegah perusakan kontrak. Dengan operasi terkait dijalankan komputer dan layanan yang disediakan oleh Ethereum, kesalahan manusia dapat dikurangi untuk menghindari perselisihan mengenai kontrak tersebut. Gambar 2.9 menunjukkan contoh bagaimana pengembang dapat dengan mudah menggunakan smart contract untuk transaksi mata uang kripto. Bahasa pemrograman tingkat tinggi yang digunakan adalah solidity, serpent dan LLL. Saat ini sebagaian pengembang menggunakan solidity untuk menulis smart contract dan mengkompilasi instruksi ke dalam bytecode untukdieksekusi oleh EVM.



Gambar 2.9: Penggunaan smart contract [36]

2.4 Zero Knowledge Proof (ZKP)

Konsep dasar ZKP adalah pembuktian pernyataan melalui protokol interaktif[37]. Dalam proses ini, pembuktian memberikan sejumlah informasi kepada verifikato sehingga dapat memverifikasi bahwa informasi tersebut akurat dan yakin akan kebenarannya tanpa mengetahui bagaimana pembukti mendapatkan informasi tersebut. Informasi ini mungkin berkaitan dengam pembuktian tentang gambar hash asli atau kesadaran anggota dalam pohon merkle dengan diketahui akar merkle. Struktur praktis untuk NIZK (Non-Interactive Zero Knowledge) telah didemonstrasikan di Ethernet.

ZKP sering digunakan dalam penerapan kriptografi, seperti konstruksi skema enkripsi kunci publik, tanda tangan digital, sistem pemungutan suara, sistem lelang, e-cash, komputasi multiparty yang aman dan komputasi yang dialihdayakan yang dapat diverifikasi. Parameter yang dapat digunakan untuk mengukur kinerja ZKP seperti waktu pembuktian, waktu pemeriksaan, ukuran pesan yang dipertukarkan, jumlah putaran di mana prover dan verifier berinteraksi. Interaksi dari sebuah sistem pembuktian diukur dengan jumlah pesan yang dikirimkan oleh prover kepada verify. Sebuah pergerakan

terdiri dari satu pesan dari satu pihak ke pihak lainnya, sementara sepasang gerakan berurutan membuat sebuah putaran

Definisi formal NIZK dijelaskan di bawah ini:

- KeyGen (1^λ) –> crs: input adalah parameter keamanan λ ; output adalah string referensi umum crs.
- Prov(crs, u,w) –> Π: input adalah misal $u$dari beberapan NP-language L_R dan para saksi w ; keluaran adalah ZKP Π
- Verify(crs, u,Π) –> $\frac{1}{0}$: input adalah bukti Π ; keluaran adalah 1 untuk penerimaan atau 0 untuk penolakan.

ZKP memiliki tiga sifat utama yang harus dipenuhi, di antaranya sebagai berikut [38]:

1. Kelengkapan: menyatakan bahwa jika pembukti (prover) dan pemeriksa (verifier) mengikuti protokol maka pemeriksa menerima validitas dari sebuah pernyataan yang benar.
2. Soundness: menjamin bahwa pembukti tidak dapat menipu pemeriksa untuk menerima validitas pernyataan yang salah, bahkan jika pembukti menyimpang dari spesifikasi protokol.
3. Zero-knowledge: mencegah verifier untuk mempelajari apa pun dari protokol selain dari validitas pernyataan.

2.5 State of the Art

Tabel 2.4 menjelaskan terkait penelitian terkini yang membahas terkait penerapan kriptografi yaitu Zero Knowledge Proof dengan blockchain serta pengembangan sistem manajemen e-certificate. Potensi yang bisa didapatkan dari kesenjangan literatur penelitian adalah optimalisasi kinerja yang dihasilkan, skalabilitas dan perbandingan metode yang digunakan dari sisi protokol ZKP dan smart contract pada teknologi blockchain.

Tabel 2.4: Perbandingan penelitian terkait

No	Nama Peneliti	Judul	Metode	Hasil
1	Ya-Che Tsai, Raylin Tso, Zi-Yuan Liu dan Kung Chen (2019)	An Improved Non-Interactive Zero-Knowledge	Skema Non-Interactive ZKRP dengan memanfaatkan smart contract di Ethereum untuk memastikan keamanan dan fleksibilitas. Melakukan perbandingan efisiensi dan keamanan ZKRP yang diusulkan dengan skema yang sudah ada	Skema memiliki fitur non-interaktif dan efisiensi yang membuat cocok untuk diterapkan diberbagai aplikasi. Solusi yang didapatkan lebih efisien dari penelitian sebelumnya.
2	Harikrishnan M dan Lakshmy KV (2019)	Secure Digital Service Payments using Zero Knowle-dge Proof in Distri-buted Network	Penggunaan ZKP seperti zkSNARKS dan zkSTARK untuk meningkatkan keamanan dan privasi dalam pembayaran layanan digital di lingkungan jaringan terdistribusi	Penggunaan ZKP seperti zkSNARKS dan zkSTARK untuk meningkatkan keamanan dan privasi dalam pembayaran layanan digital dilingkungan jaringan terdistribusi memiliki protensi yang besar dalam melindungi privasi pengguna.

Tabel 2.4: Perbandingan penelitian terkait

No	Nama Peneliti	Judul	Metode	Hasil
3	Andreas Cerulli dan Jens Groth (2019)	Efficient zero-knowledge proofs and their application	Pendekatan penelitian kualitatif dan deskriptif naratif untuk mengumpulkan dan menganalisis data dengan berfokus pada teknologi kriptografi yaitu ZKP	Kontribusi pada struktur ZKP yang efisien secara komputasi untuk pemenuhan sirkuit aritmatik dan eksekusi RAM yang benar dan mengatasi hambatan efisiensi protokol kriptografi
4	Claudia Daniela Pop , Marcel Antal, Tudor Cioara, Ionut Anghel dan Ioan Salomie (2020)	Blockchain and Demand Response: Zero-Knowledge Proofs for Energy Transactions Privacy	Implementasi manajemen respons permintaan terdesentralisasi berbasis blockchain yang diperkaya dengan solusi ZKP unruk menjaga privasi data produsen energi. Smart contract digunakan untuk memvalidasi aktivitas produsen dalam program respons permintaan	Implementasi prototipe berbasis blockchain untuk manajemen response permintaan terdesentralisasi yang diperkaya dengan solusi ZKP untuk menjaga privasi data produsen energi. Evaluasi menunjukan bahwa solusi dapat memastikan privasi data energi produsen yang disimpan di blockchain dan mendeteksi inkonsistensi data yang menunjukkan adanya manipulasi data.

Tabel 2.4: Perbandingan penelitian terkait

No	Nama Peneliti	Judul	Metode	Hasil
5	Ling Cao dan Zheyi Wan (2020)	Anonymous scheme for blockchain atomic swap based on zero-knowledge proof	Pemasalahan logaritma diskrit pada kurva eliptik dan skema komitmen pedersedn dan zkSNARKS untuk memnfaatkan teknologi kriptografi untuk menciptakan sistem transaksi yang aman, andal dan anonim.	Implementasi zkSNARKS , skema komitmen pedersedn dan ZKP sangat relevan dengan konteks pertukaran aset anonim dan aman . Penggunaan smart contract dalam blockchain menciptakan pertukaran aset secara otomatis.

Tabel 2.4: Perbandingan penelitian terkait

No	Nama Peneliti	Judul	Metode	Hasil
6	Swagatika Sahoo, Arnab Mukherjee dan Raju Halder (2021)	A unified blockchain-based platform for global e-waste manage-ment	Implementasi blockchain pada platform Ethereum pada manajemen e-waste. Evaluasi eksperimental menunjukan kelayakan dan kinerja sistem yang diusulkan.	Proposal sistem manajemen e-waste berbasis blockchain yang mencakup transparansi, pelacakan, penghematan biaya dan pemantauan otomatis dari pembuat e-waste menggunakan ethereum. Validasi identitas yang berfokus pada privasi, tokenisasi untuk pengalihan produk, bak sampah pintar berbasis IoT, dan mekanisme pembayaran.

Tabel 2.4: Perbandingan penelitian terkait

No	Nama Peneliti	Judul	Metode	Hasil
7	Wanxin Li, Collin Meese, Zijia Gary Zhong, Hao Guo dan Mark Nejad (2021)	Location-aware Verification for Autonomous Truck Platooning Based on Blockchain and Zero-knowledge Proof	Teknologi ZKP dan blockchain berizin. Prototipe dilakukan menggunakan platform Hyperledger dan diuji menggunakan alat benchmark Hyperledger Caliper. Sistem blockchain berizin juga digunakan sebagai pengendali arsitektur dan sebagai buku besar transaksi yang tidak dapat dimanipulasi untuk merekam kunci verifikator, skor reputasi, dan catatan platoon.	Protokol verifikasi berbasis blockchain dan privacy menggunakan ZKP dan teknologi blockchain berizin dapat meningkatkan efisiensi dan keamanan platooning truk otonom di dunia nyata. Eksperimen yang dilakukan menunjukkan bahwa sistem yang diusulkan dapat diterapkan dalam platooning truk otonom dengan kinerja yang sesuai untuk kebutuhan dunia nyata.

Tabel 2.4: Perbandingan penelitian terkait

No	Nama Peneliti	Judul	Metode	Hasil
8	Lang Qin, Feng Ma, Hao Geng Xie dan Sheng Li Zhang (2021)	A Distributed Authentication Scheme Based on Zero-knowledge Proof	Integrasi AI, ZKP dan blockchain di mana : AI digunakan untuk pengenalan wajah untuk memastikan keunikan dan keabsahan identitas pengguna, ZKP digunakan untuk mengenkripsi dan mendukung data wajah guna mencegah informasi identitas pengguna bocor dan blockchain digunakan untuk infrastruktur utama untuk menyimpan dan memproses data identitas pengguna.	Pengembangan skema otentikasi identitas yang didistribusikan berbasis ZKP pada sistem blockchain. Skema ini menggunakan teknik pengenalan wajah untuk memastikan keabsahan identitas serta mengendalikan node-node jahat.

Tabel 2.4: Perbandingan penelitian terkait

No	Nama Peneliti	Judul	Metode	Hasil
9	Lei Liu, Jiahua Wan dan Yue W (2022)	Computer Assisted Design of Intelligent E-Certificate System Based on Blockchain Technology	Analisis kebutuhan sistem, desain sistem berbasis blockchian, pengembangan smart contract dan integrasi blockchain ke dalam sistem manajemen sertifikat.	Pengembangan sistem berbasis blockchain untuk manajemen sertifikat elektronik. Teknik pengujian yang dilakukan adalah pengujian sistem, pengujian kecepatan dan efisiensi, pengujian keamanan sehingga di dapat bahwa evaluasi sistem adalah efektif dan aman.

Tabel 2.4: Perbandingan penelitian terkait

No	Nama Peneliti	Judul	Metode	Hasil
10	Seong-Kyu Kim (2022)	Blockchain Smart Contract to Prevent Forgery of Degree Certificates: Artificial Intelligence Consensus Algorithm	Manajemen node blockchain, AI menggunakan Mask CNN dan pengelompokkan node. Penelitian ini menggunakan algoritma konsensus dan model empiris untuk aplikasi sertifikat diploma	Implementasi Mask CNN dan konsensusu Pow dan PoS serta penerapan model empiris untuk aplikasi sertifikasi diploma. Hasil menunjukkan blockchain dapat digunakan untuk mencegah pemalsuan sertifikat akademik dan memastikan keamanan serta otentikasi sertifikat secara efisien dan memiliki tingkat keandalan yang tinggi.

Tabel 2.4: Perbandingan penelitian terkait

No	Nama Peneliti	Judul	Metode	Hasil
11	Manjula K Pawar, dkk (2022)	Performance Analysis of E-Certificate Generation and Verification using Blockchain and IPFS	Analisis kinerja pembuatan e-sertifikat dan verifikasi menggunakan teknologi blockchain dan IPFS, pengembangan algoritma untuk generasi dan validasi sertifikat, serta pembuatan antarmuka aplikasi untuk otoritas perguruan tinggi dan perusahaan	Penggunaan IPFS mengurangi waktu yang dibutuhkan untuk menghasilkan hash transaksi, dan sistem ini dapat meningkatkan keandalan sertifikat elektronik.

Tabel 2.4: Perbandingan penelitian terkait

No	Nama Peneliti	Judul	Metode	Hasil
12	Zhuoliang Qiu, Zhijun Xie, Xianliang Jiang , Chuan Ran dan Kewei Chen (2023)	Novel Blockchain and Zero-Knowledge Proof Technology-Driven Car Insurance	Penggunaan blockchain, smart contract dan ZKP untuk memastikan integritas data asuransi. pelaksanaan terdesentralisasi dari proses klaim asuransi, dan menjaga privasi data asuransi dan identitas pengguna. Analisis keamanan yang mendalam dan evaluasi kinerja dari sistem yang diusulkan	Kerangka klaim asuransi mobil berbasis ZKP yang terdesentralisasi untuk mengatasi kekhawatiran privasi dalam skema asuransi mobil berbasis blockchain tradisional. Skema ini mencapai perlindungan privasi dengan menambahkan teknologi ZKP di atas jaringan desentralisasi
13	Aleksander Berentsen, Jeremias Lenzi, and Remo Nyffenegger (2023)	An Introduction to Zero-Knowledge Proofs in Blockchains and economics	Penggunaan ZKP dalan teknologi blockchain serta memberikan contoh bagaimana ZKP digunakan pada proses pembayaran yang melindungi privasi dan skalabilitas melalui rollups serta meningkatkan efisiensi dalam aplikasi blockchain.	Membandigkan protokol zkSNARK dan zkSTARK dan membahas aplikasi dalam blockchain. Menjelaskan konsep komitmen dalam Zcah dan bagaimana ZKP digunakan untuk membuktikan validitas transaksi tanpa mengungkapkan informasi sensitif.

Tabel 2.4: Perbandingan penelitian terkait

No	Nama Peneliti	Judul	Metode	Hasil
14	Zhipeng Wang, Stefanos Chaliaso, Kaihua Qin, Liyi Zhou, dkk (2023)	On How Zero-Knowledge Proof Blockcha-in Mixers Improve, and Worsen User Privacy	Analisis empiris terhadap penggunaan mixer ZKP yang memberikan pemahaman terhadap privasi pengguna). Menggunakan pelacakan aliran koin untuk menyelidiki keterkaitan antara penggunaan mixer ZKP dengan serangan di sektor DeFi dan ekstraksi nilai blockchain. Pengukuran empiris terhadap klaim ukuran set anonimitas yang dijalankan oleh mixer ZKP untuk mengevaluasi tingkat akurasi	Penggunaan mixer ZKP dalam ekosistem blockchain sangat terkait dengan serangan di sektor DeFi dan ekstraksi nilai blockchain (BEV). Klaim ukuran set anonimitas yang dijalankan oleh mixer ZKP sebagian besar tidak akurat. ZKP mixers menarik pengguna yang tidak peduli privasi, yang pada akhirnya tidak berkontribusi pada meningkatkan privasi pengguna mixer lainnya

Tabel 2.4: Perbandingan penelitian terkait

No	Nama Peneliti	Judul	Metode	Hasil
15	Zhiguo Wan, Yan Zhou dan Kui Ren (2023)	zk-AuthFeed: Protecting Data Feed to Smart Contracts With Authenti-cated Zero Knowle-dge Proof	Merancang zk-AuthFeed, sebuah skema data feed off-chain yang terotentikasi dengan zero knowledge untuk mencapai privasi dan otentisitas data untuk smart contract. Skema ini memanfaatkan ZKP untuk memastikan bahwa smart contract dapat berjalan tanpa mengakses input pribadi, sehingga mempertahankan privasi dari input data feed tersebut. Penggunaan zk-DASNARK dalam zk-AuthFeed, bertujuan untuk mengatasi tantangan pemberian data yang terotentikasi ke dalam smart contract sambil mempertahankan privasi dan otentisitas data.	Rancangan zk-AuthFeed, sebuah skema data feed off-chain yang terotentikasi dengan zero knowledge berbasis zk-DASNARK, yang bertujuan untuk memastikan privasi dan autentikasi data untuk smart contract. Solusi untuk tantangan pemberian data yang terotentikasi ke dalam smart contract sambil mempertahankan privasi dan otentisitas data.

Bab 3

Metodologi Peneliti

Penelitian ini menggunakan metode penelitian kuantitatif pada pengembangan non-interactive zero knowledge proof dan smart contract berbasis blockchain pada e-certificate. Metode ini berfokus pada penerapan untuk memastikan sistem yang efisien, aman dan dapat diandalkan. Non-interactive zero knowledge proof digunakan untuk meningkatkan privasi yang efisien terkait data atau informasi kepemilikan dan keaslian tanpa mengungkapkan detail informasi dari sertifikat. Smart contract digunakan untuk otomatisasi proses penerbitan e-certificate dan mengeluarkan e-certificate kepada entitas yang berhak. Smart contract dapat mengatur pembaruan, pembatalan atau pengakhiran e-certificate dan setiap catatan atau perubahan yang tercatat dalam blockchain adalah permanen dan tidak dapat diubah. Semua data dan transaksi disimpan di dalam buku besar terdistribusi dan di jaringan terdesentralisasi.

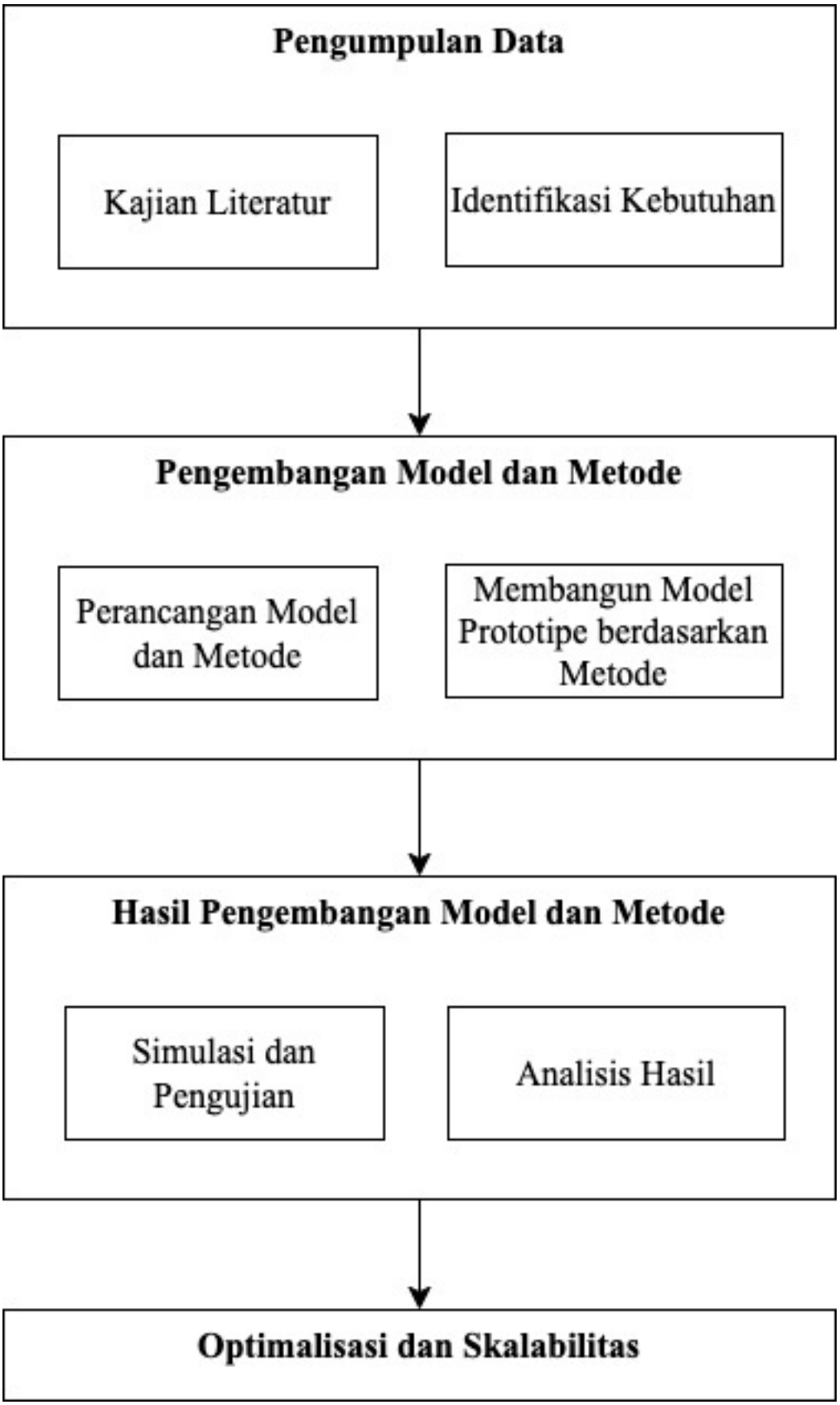
3.1 Motivasi

Kriptograsi adalah seni dan ilmu mengamankan komunikasi dan data. Ini adalah pondasi untuk berbagai aspek keamanan digital. Zero Knowledge Proof adalah metode dalam kriptografi yang memungkinkan satu pihak untuk membuktikan kepada pihak lain bahwa pernyataan tertentu benar tanpa mengungkapkan detail informasi sehingga dapat meningkatkan privasi. ZKP digunakan dalam berbagai aplikasi, seperti autentikasi, protokol blockchain dan lain sebagainya di mana privasi dan keamanan adalah perhatian utama. Karakteristik utama yang dimiliki teknologi blockchain yaitu desentralisa-

si, transparansi, kekekalan, keamanan, buku besar terdistribusi, tokenisasi, mekanisme konsensus dan smart contract. Hal ini membuat teknologi blockchain terus berkembang ke beragam aplikasi dan model binis berbasis platform yang inovatif. Pada penerapan e-certificate integrasi ZKP dan smart contract berbasis blockchain berhubungan erat dalam meningkatkan privasi, keamanan, keandalan dan efisiensi dalam transaksi dan aplikasi blockchain.

3.2 Kerangka Penelitian

Tahapan penelitian yang dilakukan dapat dilihat pada Gambar 3.1. Penelitian ini dibagi menjadi empat tahap. Tahap pertama adalah pengumpulan data yang berisi kajian literatur dan identifikasi kebutuhan terkait alur bisnis e-certificate, pemangku kepetingan dan kesenjangan penelitian dan peluang pengembangan metode non-interactive ZKP dan smart contract berbasis blockchain pada e-certificate. Tahap kedua adalah Pengembangan model dan metode yang berisi perancangan arsitektur sistem e-certificate, perancangan model non-interactive ZKP dan smart contract berbasis blockchain dan membangun model prototipe non-interactive ZKP dan smart contract berbasis blockchain. Tahap ketiga adalah hasil pengembangan model dan metode yang berisi simulasi dan pengujian serta analisis hasil. Simulasi dan pengujian dilakukan pada jaringan testnet untuk mengumpulkan data kinerja dan pengujian ketahanan berupa pengujian beban dan serangan simulasi untuk menilai seberapa baik sistem bertahan terhadap upaya eksploitasi. Analisis yang dilakukan terdiri dari analisis statistik dan analisis keamanan. Analisis statistik dilakukan dengan membandingkan kinerja berbagai implementasi atau konfigurasi serta menentukan yang paling efisien dedangkan analisis keamanan dilakukan untuk menilai risiko keamanan, sepertin probabilitas kegagalan atau kerentanan. Tahap keempat adalah optimalisasi dan skalabilitas. Optimalisasi sumber daya dengan menganalisis penggunaan sumber daya komputasi untuk mengidentifikasi area yang dapat dioptimalkan dan evaluasi skalabilitas digunakan untuk mengukur bagaimana kinerja sistem saat transaksi meningkat.



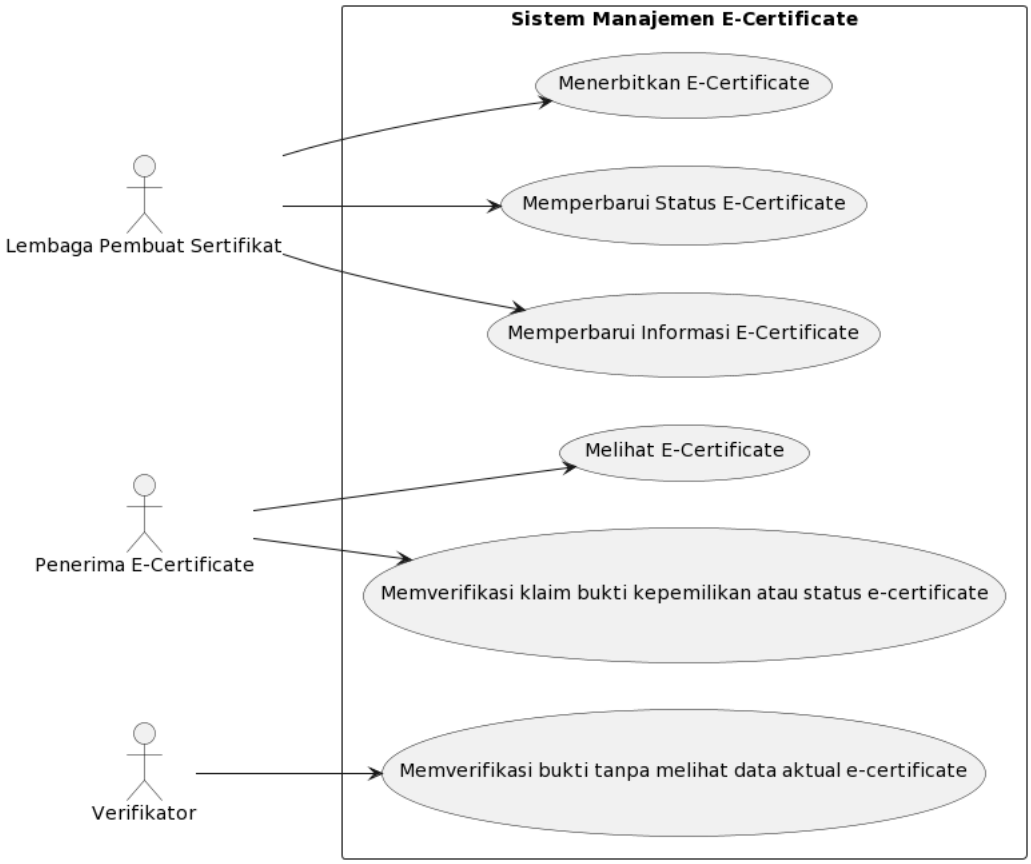
Gambar 3.1: Kerangka penelitian

3.3 Identifikasi Kebutuhan

Berdasarkan kajian literatur yang sudah dilakukan, identifikasi pengguna atau pemangku kepentingan adalah pihak yang terlibat di dalam jaringan terdesentralisasi. Pengguna dan pemangku kepentingan meliputi lembaga pembuat sertifikat, pihak penerima sertifikat dan pihak verifikator. Lembaga pembuat sertifikat akan membuat e-certificate dengan data yang telah divalidasi dan ditanda tangani secara digital serta merekam e-certificate pada blockchain. Lembaga pembuat sertifikat akan menghasilkan pasangan kunci publik/privat yang unik untuk setiap e-certificate. Kunci privat akan diberikan kepada penerima e-certificate secara aman untuk digunakan dalam proses Non-Interactive ZKP. Kunci publik disimpan atau dibagikan dengan cara yang aman dan dapat diakses oleh verifikator untuk memverifikasi klaim tanpa mengungkapkan detail informasi dari pemilik e-certificate. Smart contract digunakan untuk mengeksekusi tindakan secara otomatis seperti penerbitan, verifikasi, memperbarui status e-certificate dan memperbarui informasi. Smart contract baru dilakukan ketika memverifikasi dan merekam bukti Non-Interactive ZKP serta memperbarui status e-certificate. Smart contract akan ditempatkan ke dalam jaringan blockchain dan semua data dan transaksi akan disimpan di dalam buku besar terdistribusi.

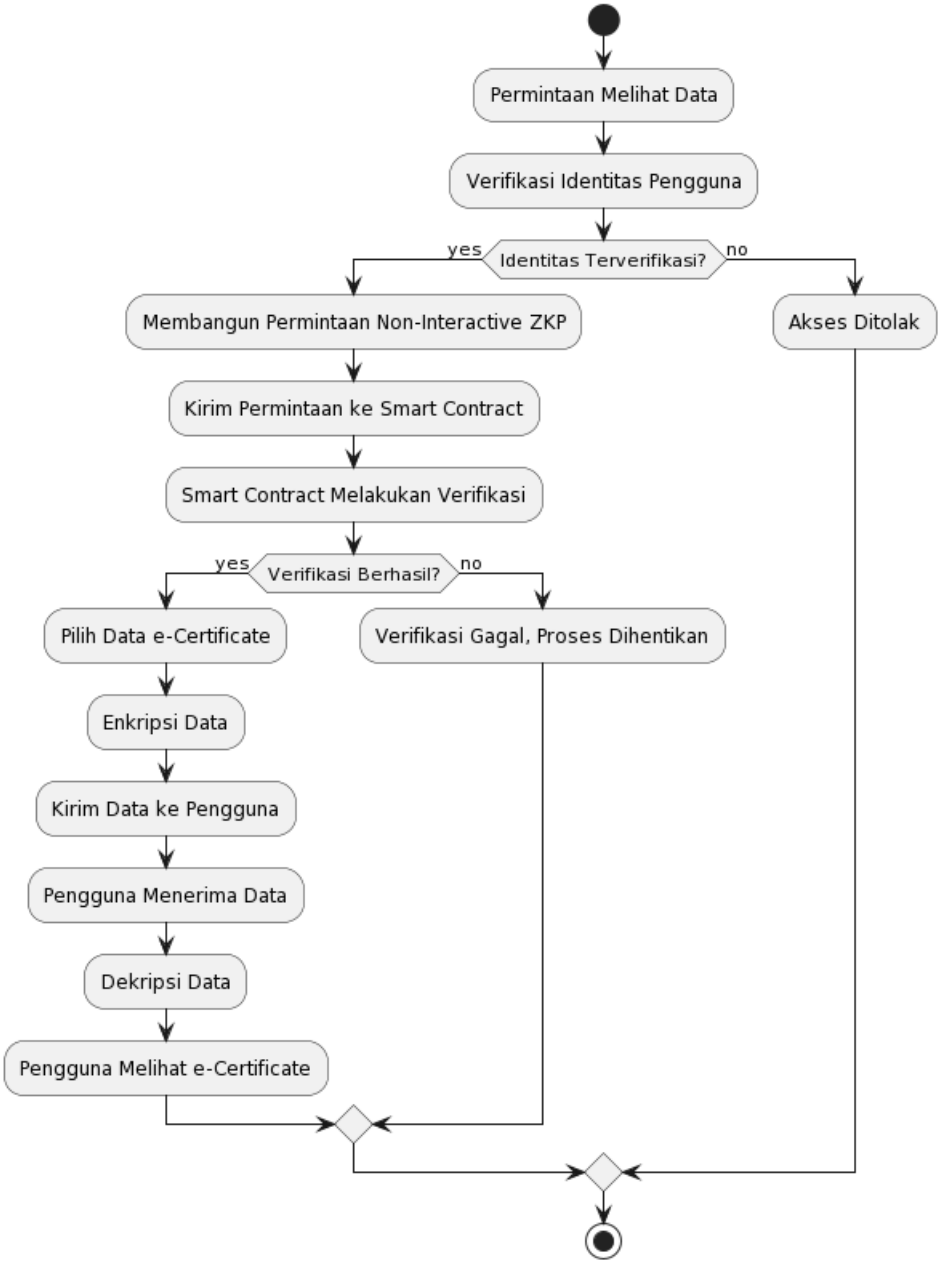
Gambar 3.2 menunjukkan interaksi para pemangku kepentingan di dalam sistem e-certificate dengan mengembangkan metode non-interactive ZKP dan smart contract berbasis blockchain. Aktor lembaga pembuat sertifikat bertanggung jawab terkait pembuatan dan pengelolaan e-certificate, penerima e-certificate adalah individu atau entitas yang e-certificate dikelola dalam sistem dan verifikator adalah pihak yang bertugas memverifikasi informasi e-certificate. Lembaga pembuat sertifikat dapat menerbitkan e-certificate, memperbarui status e-certificate seperti validasi, pembaruan atau pencabutan serta memperbarui informasi e-certificate. Penerima e-certificate dapat melihat e-certificate dan memverifikasi klaim bukti kepemilikan atau status e-certificate. Verifikator dapat memverifikasi bukti tanpa melihat data aktual e-certificate.

Gambar 3.3 menunjukkan alur kerja atau aktivitas dari suatu proses atau sistem. Alur kerja di mulai saat pengguna memulai permintaan untuk melihat data e-certificate. Sistem akan memverifikasi identitas pengguna untuk memastikan bahwa pengguna berwenang untuk mengakses data. Sistem



Gambar 3.2: Use case sistem e-certificate

atau pengguna membangun permintaan menggunakan Non-Interactive ZKP untuk membuktikan bahwa pengguna memiliki hak untuk melihat data tanpa mengungkapkan informasi identitas atau detail informasi yang sebenarnya. Kemudian permintaan Non-Interactive ZKP dikirim ke smart contract yang berjalan di blockchain. Smart contract melakukan verifikasi bukti Non-interactive tanpa memerlukan interaksi tambahan dengan pengguna, memastikan privasi dan keamanan. Jika verifikasi berhasil, smart contract akan memproses permintaan dan memilih data e-certificate yang relevan. Data e-certificate yang dipilih dienkripsi dan dikirim kembali ke pengguna untuk menjaga keamanan saat transmisi. Pengguna menerima data, mendekripsinya, dan akhirnya dapat melihat informasi e-certificate.



Gambar 3.3: Activity diagram sistem e-certificate

3.4 Perancangan Model dan Metode

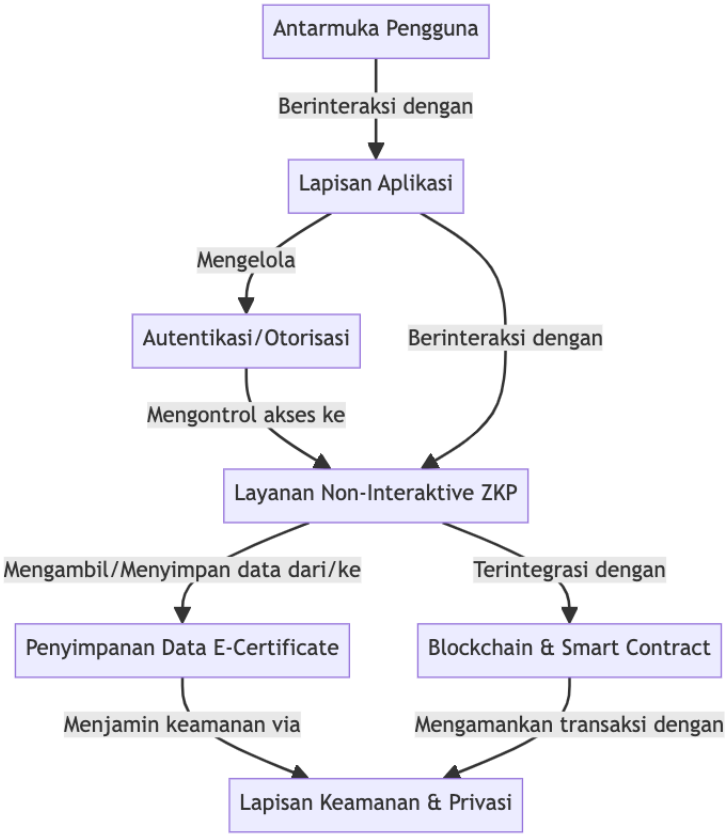
Pada tahap ini terdiri dari perancangan model arsitektur sistem e-certificate, perancangan metode non-interactive ZKP, perancangan metode smart contract berbasis blockchain dan integrasi metode Non-Interactive ZKP dan smart contract berbasis blockchain.

3.4.1 Perancangan Model Arsitektur Sistem E-certificate

Gambar 3.4 menunjukkan perancangan model arsitektur sistem e-certificate dengan mengembangkan non-interactive ZKP dan smart contract berbasis blockchain. Proses di mulai dengan antarmuka pengguna, tempat pengguna berinteraksi dengan sistem. Hal ini berupa aplikasi web atau mobile yang digunakan oleh pengguna yang terlibat di dalam sistem e-certificate. Setelah pengguna melakukan interaksi, permintaan diteruskan ke lapisan aplikasi. Lapisan ini bertindak sebagai penghubung antara pengguna dan sistem, mengelola logika aplikasi dan mengarahkan alur kerja ke layanan yang sesuai. Sebelum pengguna dapat mengakses informasi atau melakukan operasi kritis maka harus melalui autentikasi/otorisasi. Identitas pengguna akan diverifikasi dan sistem memastikan bahwa pengguna memiliki izin yang tepat untuk melanjutkan. Layanan Non-Interactive ZKP digunakan untuk memverifikasi hak akses pengguna atas data e-certificate tanpa mengungkap detail informasi. Hal ini membantu dalam menjaga privasi pengguna dambil memastikan keamanan dan integrasi transaksi. Blockchain dan smart contract bekerja bersama untuk merekam, memverifikasi, dan mengamankan setiap transaksi atau perubahan data. Smart contract secara otomatis mengeksekusi aturan bisnis yang telah ditetapkan, blockchain dapat menjamin transaksi dijalankan di jaringan terdesentralisasi. Penyimpanan data e-certificate dapat dilakukan di buku besar terdistribusi. Lapisan keamanan dan privasi memastikan bahwa semua data dan transaksi dilindungi.

3.4.2 Perancangan Metode Non-Interactive ZKP

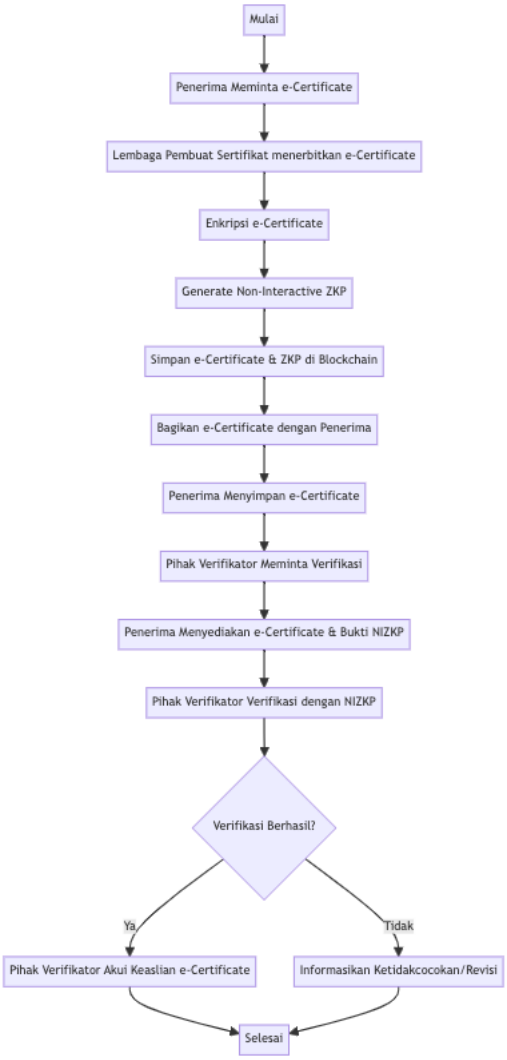
Gambar 3.5 menunjukkan perancangan metode non-interactive ZKP. Penerima meminta e-certificate kepada lembaga pembuat sertifikat. Lembaga pembuat sertifikat menerbitkan e-certificate. Untuk menjaga keamanan dan



Gambar 3.4: Perancangan model arsitektur sistem e-certificate

privasi, e-certificate dienkripsi. Ini memastikan bahwa hanya pihak yang berwenang yang dapat mengakses dan membaca. Untuk memungkinkan verifikasi tanpa mengungkapkan detail pribadi atau isi e-Certificate, sistem menghasilkan bukti Non-Interactive ZKP. E-Certificate dan bukti Non-Interactive ZKP kemudian disimpan di blockchain. Ini menjamin bahwa data tidak dapat diubah dan keasliannya dapat diverifikasi. E-certificate dibagikan dengan penerima, yang kemudian dapat menyimpannya secara pribadi atau membagikannya dengan pihak ketiga untuk verifikasi. Penerima menyimpan e-Certificate di tempat yang aman, siap untuk digunakan kapan saja diperlukan. pihak verifikator, seperti calon pemberi kerja atau institusi pendidikan, meminta verifikasi keaslian e-certificate. Penerima kemudian menyediakan e-certificate dan bukti Non-Interactive ZKP kepada pihak verifikator. Ini memungkinkan pihak verifikator untuk melakukan verifikasi tanpa melihat data sensitif. Pihak verifikator menggunakan bukti Non-Interactive ZKP untuk memverifikasi keaslian e-Certificate. Mereka melakukan ini dengan membandingkan bukti dengan data yang tersimpan di blockchain. Pihak

verifikator menilai apakah e-certificate asli dan valid. Ya: Jika verifikasi berhasil, pihak verifikator mengakui keaslian e-certificate dan proses verifikasi selesai. Tidak: Jika terdapat ketidakcocokan atau masalah, pihak verifikator akan menginformasikan kebutuhan untuk perbaikan atau revisi.



Gambar 3.5: Perancangan metode Non-Interactive ZKP

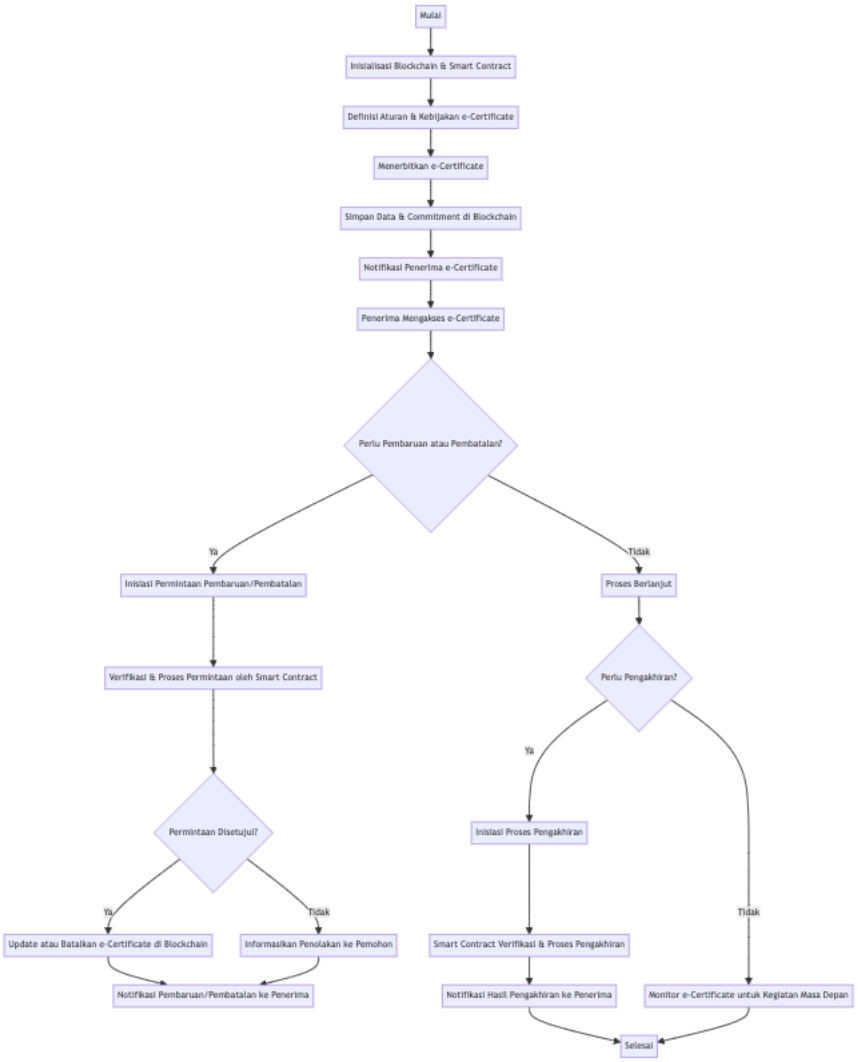
3.4.3 Perancangan Metode Smart Contract berbasis Blockchain

Gambar 3.6 menunjukkan perancangan metode smart contract berbasis blockchain. Di mulai dengan inisialisasi blockchain dan smart contract. Definisi aturan dan kebijakan e-certificate yaitu terkait penerbitan, pembaruan

dan pembatalan e-certificate. Menerbitkan e-certificate. Data e-certificate dan commitment yang terkait disimpan di blockchain, memastikan keaslian dan integritas sertifikat serta memudahkan verifikasi di masa depan. Penerima diberitahu bahwa e-certificate telah diterbitkan dan tersedia. Mereka mungkin juga diberikan instruksi tentang cara mengakses atau menggunakan sertifikat. Penerima mengakses e-certificate, yang mungkin diperlukan untuk tujuan verifikasi, aplikasi pekerjaan, atau pendidikan lanjutan. Apakah ada kebutuhan untuk memperbarui atau membatalkan e-certificate, mungkin karena perubahan informasi atau status penerima. Jika ada maka inisiasi permintaan pembaruan atau pembatalan. Smart contract memverifikasi dan memproses permintaan pembaruan atau pembatalan. Ini memastikan bahwa permintaan tersebut sah dan sesuai dengan kebijakan yang telah ditetapkan. Jika permintaan disetujui maka e-certificate diperbarui atau dibatalkan di blockchain. Jika tidak pemohon diberitahu tentang penolakan dan alasannya.

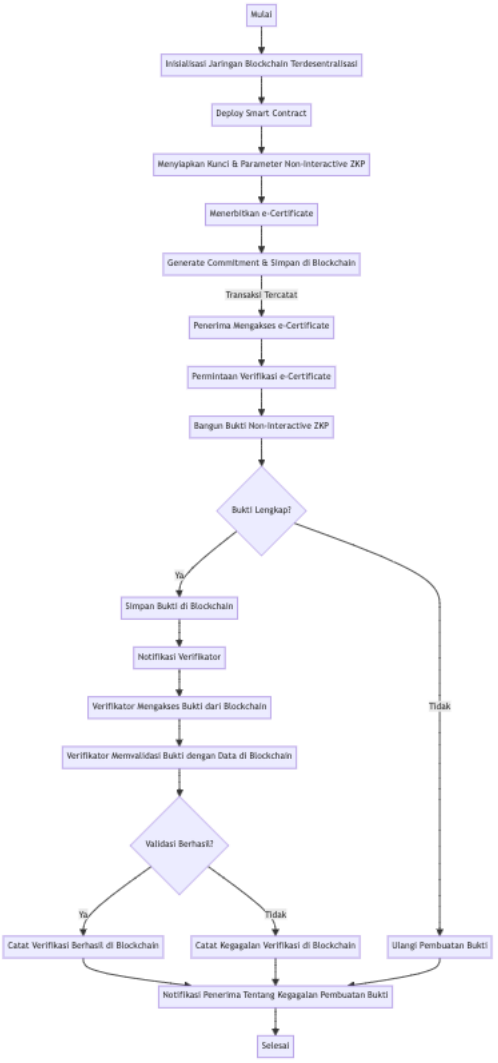
3.4.4 Integrasi Metode Non-Interactive ZKP dan Smart Contract berbasis Blockchain

Gambar 3.7 menunjukkan integrasi metode Non-Interactive ZKP dan smart contract berbasis blockchain. Di mulai dengan inisialisasi jaringan blockchain terdesentralisasi. Smart contract dijalankan di jaringan blockchain untuk otomatisasi proses, penanganan e-certificate dan logika verifikasi. Kunci dan parameter untuk Non-Interactive Zero-Knowledge Proof disiapkan untuk memastikan bahwa proses verifikasi dapat dilakukan tanpa mengungkapkan detail informasi. E-certificate diterbitkan kepada penerima setifikat setelah verifikasi kredensial. Generate commitment dari e-Certificate dihasilkan dan disimpan di blockchain. Ini bertindak sebagai bukti yang tidak dapat diubah dari e-Certificate dan memudahkan verifikasi di masa depan. Penerima e-Certificate dapat mengaksesnya setelah berhasil direkam di blockchain. Permintaan verifikasi e-certificate dapat dilakukan oleh penerima sertifikat atau verifikator. Bukti Non-Interactive ZKP dibangun untuk menanggapi permintaan verifikasi, memungkinkan verifikasi keaslian tanpa mengungkapkan informasi pribadi atau rahasia. Kemudian dilakukan pemeriksaan terkait bukti NIZKP apakah telah lengkap dan akurat, Jika ya, maka proses dilanjutkan dengan menyimpan bukti di blockchain. Jika tidak, proses bukti akan diu-



Gambar 3.6: Perancangan metode Smart Contract berbasis Blockchain

langi. Bukti yang lengkap dan akurat disimpan di blockchain, memastikan integritas dan kemudahan akses di masa depan. Verifikator mengakses bukti yang tersimpan di blockchain untuk memulai proses validasi. Verifikator memvalidasi bukti dengan membandingkannya dengan data commitment yang tersimpan di blockchain. Kemudian dilakukan pemeriksaan terkait validasi. Jika ya, maka velidasi berhasil dan verifikasi akan dicatat di blockchain. Jika validasi gagal, kegagalan verifikasi dicatat di blockchain. Penerima diberitahu tentang hasil verifikasi, apakah e-Certificate mereka telah berhasil diverifikasi atau ada masalah yang perlu ditangani.



Gambar 3.7: Integrasi Non-Interactive ZKP dan Smart Contract berbasis Blockchain

Bibliografi

[1] A. Moutaz, A. Salah, W. Albara, and B. Ayman. Blockchain technology in supply chain management: an empirical study of the factors affecting user adoption/acceptance. *Cluster Computing*, 2020.

[2] A. Perdana, A. Robb, V. Balachandran, and F Rohde. Distributed ledger technology: its evolutionary path and the road ahead. *Information and Management*, 58(3), 2021.

[3] AWS. Blockchain on aws, 2023. URL `https://aws.amazon.com/blockchain/`.

[4] B. Scott, J. Loonam, and Kumar V. Exploring the rise of blockchain technology: Towards distributed collaborative organizations. *Strategic Change*, 26:423–428, 2017.

[5] N. Upadhyay. Demystifying blockchain: a critical analysis of challenges, applications and opportunities. *International Journal of Information Management*, Oktober 2020.

[6] SE. Chang, Y-C. Chen, and Lu M-F. Supply chain re-engineering using blockchain technology: a case of smart contract-based tracking process. *Technol Forecast Soc Change 144*, 2019.

[7] C. Natalia and M.Y. Muhammad. Consensus algorithms in blockchain: Comparative analysis, challenges and opportunities. *International Conference on Open Source Systems and Technologies (ICOSST)*, 2018.

[8] Y. Wang, J. Han, and P. Beynon. Understanding the blockchain technology for future supply chains: a systematic literature review and research agenda. *Supply Chain Management: An International Journal*, 24(1):62–84, 2019.

[9] K. Lei, M.Y. Du, J.Y. Huang, and T. Jin. Groupchain: towards a scalable public blockchain in fog computing of iot services computing. *IEEE Transactions on Services Computing*, 13(2):pp. 252–262, 2020.

[10] D.P. Claudia, A. Marcel, C. Tudor, A. Ionut, and S. Ioan. Blockchain and demand response: Zero-knowledge proofs for energy transactions privacy. *MDPI Sensors 2020, 20, 5678*, 2020.

[11] S. Swagatika, M. Arnab, and Halder. Raju. A unified blockchain-based platform for global e-waste management. *International Journal of Web Information Systems*, 17(5):pp. 449–479, 2021.

[12] Qiu. Zhuoliang, Xie. Zhijun, Jiang. Xianliang, Ran. Chuan, and Chen. Kewei. Novel blockchain and zero-knowledge proof technology-driven car insurance. *MDPI Electronics 2023, 12, 3869*, 2023.

[13] Tsai. Ya-Che, Tso. Raylin, Liu. Zi-Yuan, and Chen. Kung. An improved non-interactive zero-knowledg. *IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON)*, 2019.

[14] Ra. etc. Gyeongjin. Vaim: Verifiable anonymous identity management for human-centric security and privacy in the internet of things. *IEEE Access*, 2021.

[15] O. Patric, F. Brendan, U. Hiroshi, and O Hiroaki. Managing lifelong learning records through blockchain. *Research and Practice in Technology Enhanced Learning*, 14(4):1–19, 2019.

[16] Kim. Seong-Kyu. Blockchain smart contract to prevent forgery of degree certificates: Artificial intelligence consensus algorithm. *MDPI Electronics 2023, 11, 2112*, 2022.

[17] K.P. etc. Manjula. Performance analysis of e-certificate generation and verification using blockchain and ipfs. *International Conference on Inventive Computation Technologies (ICICT)*, 2022.

[18] Dib. Omar, B. Kei-Leo, and D. Antoine. Consortium blockchains: Overview, applications and challenges. *International Journal on Advances in Telecommunications*, 11, 2018.

[19] Baliga. Arati. Performance characterization of hyperledger fabric. *In the First Crypto Valley Conference on Blockchain Technology (CVCBT 2018)*, 2018.

[20] K. Ioannis, P. Maria, and A.B. Nedaa. Design of the blockchain smart contract: A use case for real estate. *Journal of Information Security*, pages 177–190, 2018.

[21] Namecoin. Namecoin, 2018.

[22] F. Md-Sadek, J. Mohammad, A.H. Mohammad, and C. Alan. Blockchain consensus algorithm: A survey. *Distributed, Parallel, and Cluster Computer (cs.DC) arXiv:2001.07091*, 2020.

[23] K. Rukshanda and K. Nasreen. Blockchain technology development and implementation for global logistics operations: a reference model perspective. *Journal of Global Operations and Strategic Sourcing*, 2021.

[24] M.J.M. Chowdhury, M.S. Ferdous, K. Biswas, and P Waters. A comparative analysis of distributed ledger technology platforms. *IEEE Access*, 7:167930–167943, 2019.

[25] A. Baliga. Understanding blockchain consensus models, 2017.

[26] C. Cachin and M. Vukoli. Blockchains consensus protocols in the wild. *arXiv preprint arXiv:1707.01873*, 2017.

[27] S. Kudva, S. Badsha, S. Sengupta, I. Khalil, and A. Zomaya. Towards secure and practical consensus for blockchain based vanet. *Information Sciences*, 545:pp. 170–187, 2021.

[28] H.Y. Song, N.F. Zhu, R.X. Xue, J.S. He, K. Zhang, and J.Y. Wang. Proof-of-contribution consensus mechanism for blockchain and its application in intellectual property protection. *Information Processing and Management*, 58(3), 2021.

[29] Y. Sompolinsky and A. Zohar. Secure high-rate transaction processing in bitcoi. *Financial Cryptography and Data Security. FC 2015. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg*, 8975, 2015.

[30] I. Eyal, A.E. Gencer, E.G. Sirer, and Renesse R. Bitcoin-ng: a scalable blockchain protocol. *Proceedings of the 13th USENIX Conference on Networked Systems Design and Implementation*, pages pp. 45–59, 2016.

[31] Xie Mingyue and Liu. Jun. A survey on blockchain consensus mechanism: research overview, current advances and future directions. *International Journal of Intelligent Computing and Cybernetics*, 16(2):pp. 314–340, 2022.

[32] B. David, P. Gazi, A. Kiayias, and A. Russell. Ouroboros praos: an adaptively-secure, semisynchronous proof-of-stake blockchain. *Proceedings of International Association for Cryptologic Research,*, pages pp. 66–98, 2018.

[33] C.L. Li, J. Zhang, and X.M. Yang. Scalable blockchain storage mechanism based on two-layer structure and improved distributed consensus. *The Journal of Supercomputing*, 78(4):pp. 4850–4881., 2022.

[34] L. Wang, Y. Bai, Q. Jiang, V.C.M. Leung, W. Cai, and Li X.X. Beh-raftchain: a behaviorbased fast blockchain protocol for complex networks. *IEEE Transactions on Network Science and Engineering*, 8(2):pp. 1154–1166, 2021.

[35] He. Benyuan. An empirical study of online shopping using blockchain technology. *Department of Distribution Management, Takming University of Science and Technology, Taiwan, R.O.C*, 2017.

[36] Chen. Jiin-Chiou, Lee. Narn-Yih, and Chen. Chien, Chi.and Yi-Hua. Blockchain and smart contract for digital certificate. *IEEE International Conference on Applied System Invention (ICASI)*, 2018.

[37] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems. in providing sound foundations for cryptography: On the work of shafi goldwasser and silvio micali. *ACM: New York*, pages pp. 203–225., 2019.

[38] C. Andrea and G. Jeans. Efficient zero-knowledge proofs and their applications. *CORE UCL Discovery*, 2019.