# BAB II

# TINJAUAN PUSTAKA

## 2.1 Verifikasi dan Validasi

Verifikasi merupakan langkah untuk menegaskan kebenaran, ketepatan, atau kevalidan suatu hal. Verifikasi juga dapat dijelaskan sebagai langkah untuk memastikan pemenuhan persyaratan atau mengidentifikasi perbedaan antara hasil yang diharapkan dan fakta yang ditemukan. Di sisi lain, validasi merupakan proses penilaian terhadap kesesuaian produk atau sistem yang telah dikembangkan dengan kebutuhan pengguna atau pelanggan, serta kemampuannya untuk beroperasi sesuai dengan harapan di lingkungan nyata. Kedua proses ini memiliki peran krusial dalam memastikan kualitas dan kelayakan suatu produk atau sistem (Aminullah et al., 2022).

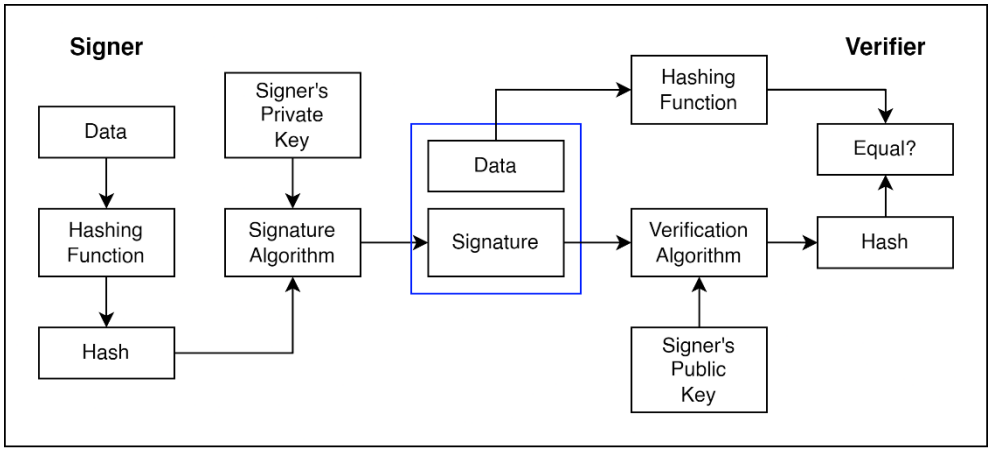
## 2.2 Sertifikat Digital

Sertifikat digital merupakan dokumen elektronik yang memuat tanda tangan elektronik dan informasi identitas, menunjukkan status hukum subjek hukum yang terlibat dalam transaksi elektronik yang diterbitkan oleh penyelenggara sertifikasi elektronik. Sertifikat digital ini memiliki signifikansi yang besar, mengingat bahwa sertifikat digital berfungsi sebagai bukti hak kepemilikan terhadap suatu produk dan dapat digunakan sebagai representasi keterampilan atau partisipasi dalam suatu kegiatan, yang kemudian diakui dengan pemberian sertifikat (Aminullah et al., 2022).

## 2.3 *Digital Signature* (Tanda Tangan Digital)

*Digital Signature* (tanda tangan digital) adalah primitif kunci publik dalam otentikasi pesan (Nadzifarin & Asmunin, 2022). Di dunia fisik, tanda tangan tangan adalah hal umum dalam pesan tertulis atau yang ditekan mesin ketik. Tanda tangan digunakan untuk mengaitkan pihak yang menandatanganinya dengan pesan yang disampaikan. *Digital signature* juga dapat diartikan sebagai

teknik yang mengaitkan individu/entitas dengan data digital. Kaitan ini dapat diverifikasi secara independen oleh penerima maupun pihak ketiga.




Gambar 2.1 Model *Digital Signature* (Sasi et al., 2023)

Penjelasan model *digital signature* dari Gambar 2.1 adalah sebagai tersebut:

1. Setiap individu yang mengadopsi skema ini memiliki sepasang kunci publik-privat.
2. Secara umum, sepasang kunci yang digunakan untuk enkripsi/dekripsi dan penandaan/verifikasi adalah berbeda. Kunci pribadi yang digunakan untuk penandaan disebut sebagai kunci tanda tangan dan kunci publik disebut sebagai kunci verifikasi.
3. Pengguna tanda tangan memasukkan data ke dalam fungsi hash dan menghasilkan hash dari data.
4. Nilai hash dan kunci tanda tangan kemudian dimasukkan ke dalam algoritma tanda tangan yang menghasilkan *digital signature* pada hash yang diberikan. Tanda tangan ditambahkan ke data dan keduanya dikirimkan kepada pihak yang memverifikasi.
5. Pihak yang memverifikasi memasukkan *digital signature* dan kunci verifikasi ke dalam algoritma verifikasi. Algoritma verifikasi memberikan suatu nilai sebagai keluaran.
6. Pihak yang memverifikasi juga menjalankan fungsi hash yang sama pada data yang diterima untuk menghasilkan nilai hash.

7. Nilai hash dan keluaran dari algoritma verifikasi dibandingkan untuk memverifikasinya. Berdasarkan hasil perbandingan ini, pihak yang memverifikasi menentukan apakah *digital signature* tersebut valid.
8. Pengguna tanda tangan tidak dapat menyangkal penandatanganan data tersebut di masa depan karena digital signature dibuat oleh kunci 'pribadi' dari pengguna tanda tangan, dan tidak ada orang lain yang memiliki kunci tersebut.

## 2.4 Blockchain

### 2.4.1 Konsep Blockchain

*Blockchain* adalah sebuah teknologi yang memungkinkan penyimpanan data secara terdesentralisasi dan terdistribusi. Ini berfungsi sebagai buku besar digital yang mencatat transaksi-transaksi dalam bentuk blok yang saling terhubung dan aman dengan menggunakan kriptografi. Blok-blok dalam *blockchain* berisi informasi transaksi, *timestamp*, dan tautan ke blok sebelumnya. Data dalam *blockchain* disimpan di seluruh jaringan komputer yang terhubung dan setiap perubahan atau penambahan data memerlukan persetujuan dari mayoritas partisipan jaringan (Zheng et al., 2017).

### 2.4.2 Karakteristik Jaringan *Blockchain*

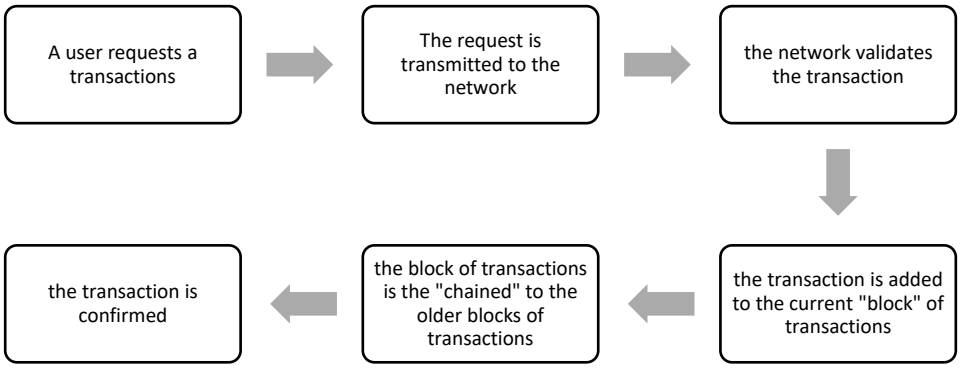
Karakteristik dari jaringan *blockchain* yaitu sebagai berikut (Zheng et al., 2017):

1. ***Decentralization***: Konteks sistem transaksi konvensional yang terpusat menunjukkan bahwa setiap transaksi harus melewati proses validasi oleh lembaga pusat yang dianggap sebagai otoritas yang sering kali menghasilkan biaya yang signifikan dan menghadapi kendala kinerja akibat beban pada server pusat. Sebaliknya, dalam penerapan teknologi *blockchain* tidak lagi diperlukan keterlibatan pihak ketiga sebagai otoritas pengesahan. Algoritma konsensus dalam *blockchain* berperan dalam menjaga konsistensi data di dalam jaringan yang terdistribusi tersebut.

2. ***Persistency***: Transaksi dapat divalidasi dengan cepat dan transaksi yang tidak valid tidak akan diterima oleh *miner*. Sangat sulit untuk menghapus atau membatalkan transaksi setelah mereka disertakan dalam *blockchain*. Blok yang berisi transaksi tidak valid dapat segera ditemukan.
3. ***Anonymity***: Setiap pengguna dapat berinteraksi dengan *blockchain* menggunakan alamat yang dihasilkan yang tidak mengungkapkan identitas sebenarnya pengguna. Perlu dicatat bahwa *blockchain* tidak dapat menjamin perlindungan privasi yang sempurna karena batasan intrinsik.
4. ***Auditability***: *Blockchain Bitcoin* menyimpan data tentang saldo pengguna berdasarkan model *Unspent Transaction Output (UTXO).* Setiap transaksi harus merujuk pada beberapa transaksi yang sebelumnya belum dihabiskan. Begitu transaksi saat ini dicatat ke dalam *blockchain*, status transaksi yang dirujuk tersebut beralih dari belum dihabiskan menjadi dihabiskan, sehingga transaksi dapat dengan mudah diverifikasi dan dilacak.

### 2.4.3 Cara Kerja *Blockchain*

Cara kerja *blockchain* menyerupai sebuah lembar kerja (*spreadsheet*) yang berisi catatan transaksi-transaksi yang kemudian direplikasi secara luas di seluruh jaringan komputer. Desain jaringan ini bertujuan untuk memperbarui lembar kerja secara berkala. Gambaran ini menunjukkan bahwa *blockchain* tidak memerlukan perantara, sehingga setiap individu dapat mencatat transaksinya sendiri dalam lembar kerja mereka masing-masing. Penggunaan algoritma internal dalam blockchain memungkinkan pencapaian konsensus dalam jaringan setiap kali ada entri baru yang ditambahkan (Laurence, 2023). Penjelasan lebih lanjut mengenai cara kerja *blockchain* disajikan pada Gambar 2.2.




Gambar 2.2 Cara kerja *blockchain* (Singhal et al., 2018)

Penjelasan atau langkah-langkah berdasarkan Gambar 2.2 pada jaringan *blockchain* adalah sebagai berikut:

1. Proses dimulai ketika seorang pengguna mengajukan permintaan untuk melakukan transaksi. Transaksi ini bisa berupa pertukaran uang, properti, atau informasi lainnya.
2. Permintaan transaksi tersebut kemudian dikirimkan ke seluruh jaringan *blockchain*, memasukkan informasi ke dalam sistem terdistribusi.
3. Jaringan *blockchain* memvalidasi transaksi yang diajukan. Validasi ini melibatkan pemeriksaan apakah transaksi memenuhi syarat dan kriteria yang telah ditetapkan.
4. Transaksi yang telah divalidasi ditambahkan ke dalam blok transaksi saat ini. Sebuah blok adalah sekelompok transaksi yang dikumpulkan bersama untuk diolah.
5. Blok transaksi yang baru dibuat kemudian dihubungkan atau di-"*chained*" dengan blok-blok transaksi sebelumnya dalam blockchain. Inilah yang menciptakan struktur rantai blok.
6. Blok transaksi yang telah ditambahkan dan di-"*chained*" ke dalam blockchain menandakan selesainya dan pengkonfirmasian transaksi. Informasi transaksi ini menjadi bagian permanen dari *ledger blockchain*.

## 2.5 Smart Contract

*Smart contract* adalah program komputer yang dirancang untuk mengeksekusi, menegaskan, atau menyesuaikan perjanjian atau kontrak secara otomatis ketika kondisi yang telah ditentukan terpenuhi. Konsep ini pertama kali diperkenalkan oleh Nick Szabo pada tahun 1994. *Smart contract* berjalan di atas teknologi *blockchain*, seperti *Ethereum* yang menyediakan lingkungan eksekusi aman dan terdesentralisasi (W. Zou et al., 2021).

S*mart contract* pada jaringan *blockchain* merupakan kode komputer yang disematkan dalam suatu transaksi. Kode tersebut dapat berisi logika bisnis, syarat, atau aturan yang akan diterapkan secara otomatis ketika kondisi yang telah ditentukan tercapai. *Smart contract* memungkinkan pihak yang terlibat dalam suatu transaksi untuk menghilangkan kebutuhan akan perantara atau pihak kepercayaan karena eksekusi perjanjian dilakukan secara otomatis oleh *blockchain* (Mohanta et al., 2018).

## 2.6 Ethereum

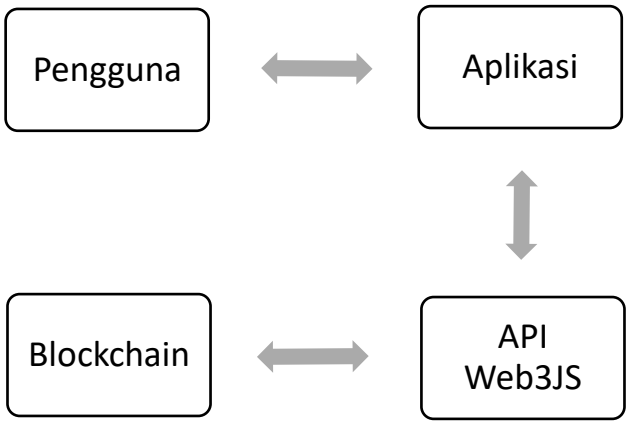
*Ethereum* adalah jaringan komputer di seluruh dunia yang mengikuti serangkaian aturan yang disebut protokol *Ethereum*. Jaringan *Ethereum* berfungsi sebagai dasar bagi komunitas, aplikasi, organisasi, dan aset digital yang dapat dibangun dan digunakan oleh siapa saja . *Ethereum* menyajikan jaringan *peer-to-peer* dari *node-node* yang saling tidak percaya, menjaga pandangan bersama atas keadaan secara global, dan menjalankan kode sesuai permintaan. Keadaan tersebut disimpan dalam *blockchain* yang dilindungi oleh mekanisme konsensus *proof-of-work*, serupa dengan *Bitcoin* (Tikhomirov, 2018).

*Ether* merupakan nama mata uang kripto yang digunakan dalam ekosistem *blockchain Ethereum*. *Ether* diperlukan sebagai alat untuk menjalankan kode di dalam jaringan *Ethereum*. Saat digunakan untuk mengeksekusi suatu kontrak di jaringan *Ethereum*, *Ether* disebut sebagai *gas* (Laurence, 2023). Istilah *Ethereum Gas* digunakan sebagai satuan untuk mengukur beban komputasi dalam pelaksanaan *smart contract*. Biaya *gas* merupakan nilai moneter yang harus

dikeluarkan oleh pengguna untuk melaksanakan *smart contract*. Semakin rumit transaksi tersebut, semakin besar *gas* yang dibutuhkan. *Gas Limit* menunjukkan batas maksimum biaya dalam satu transaksi, sementara *Gas Price* merupakan biaya yang dikenakan untuk memvalidasi transaksi. Semakin tinggi *Gas Price*, semakin cepat transaksi tersebut divalidasi oleh para penambang (Hewa et al., 2021).

## 2.7 API Web3JS

*Web3JS* adalah *library JavaScript* yang menyediakan *Application Programming Interface (API)* untuk berinteraksi dengan *node Ethereum*. *Library* ini memungkinkan pengembang untuk membuat aplikasi terdesentralisasi *(dApps)* yang dapat berkomunikasi dengan jaringan *Ethereum*. Pengembang dapat mengakses berbagai fungsi *blockchain*, termasuk membaca dan menulis data ke dalam *smart contract*, mengirim transaksi, dan berinteraksi dengan *node Ethereum* dengan menggunakan *Web3JS*.




Gambar 2.3 Cara kerja *API Web3JS*

Berikut ini alur dari cara kerja dari *API Web3JS* berdasarkan Gambar 2.3:

1. Pengguna memberikan input atau permintaan melalui antarmuka aplikasi.
2. Aplikasi menerima input dari pengguna dan memprosesnya sesuai dengan logika bisnis atau fungsionalitas yang diimplementasikan. Ketika diperlukan interaksi dengan *blockchain*, aplikasi menggunakan *API Web3JS* untuk berkomunikasi dengan jaringan *blockchain*.

3. Aplikasi menggunakan *API Web3JS* untuk mengirim permintaan atau transaksi ke *blockchain*.
4. *Blockchain* memproses transaksi sesuai dengan aturan yang diatur dalam *smart contract* atau protokol *Ethereum* setelah menerima permintaan dari *API Web3JS*. Hasil transaksi seperti pembaruan status *smart contract* atau transfer aset digital dicatat dan disimpan di dalam blok baru.
5. *API Web3JS* akan menampilkan berhasil atau tidaknya pada aplikasi pengguna setelah proses selesai.

## 2.8 Algoritma *Keccak256*

*Keccak256* merupakan sebuah fungsi kriptografi dan bagian dari *Solidity* (Keluarga *SHA-3*). Fungsi ini menghitung *hash* dari suatu input menjadi output berukuran tetap yang menghasilkan hash tunggal *32byte* dari berbagai input. Fungsi hash kriptografi ini hanya dapat digunakan dalam satu arah dan tidak dapat dibalik.

Cara kerja dari algoritma *Keccak256* yaitu diberikan sebuah string sebagai input, seperti "Namaste Duniya" kemudian dikirim melalui fungsi hash menggunakan *keccak256*, maka akan menghasilkan:

```
Namaste Duniya -> keccak-256(fungsi hash) ->
8a0fe4fd16bb35fbecde2e774008fb7f92a8568a680f3fa93d0948bcfbf68dc3
```

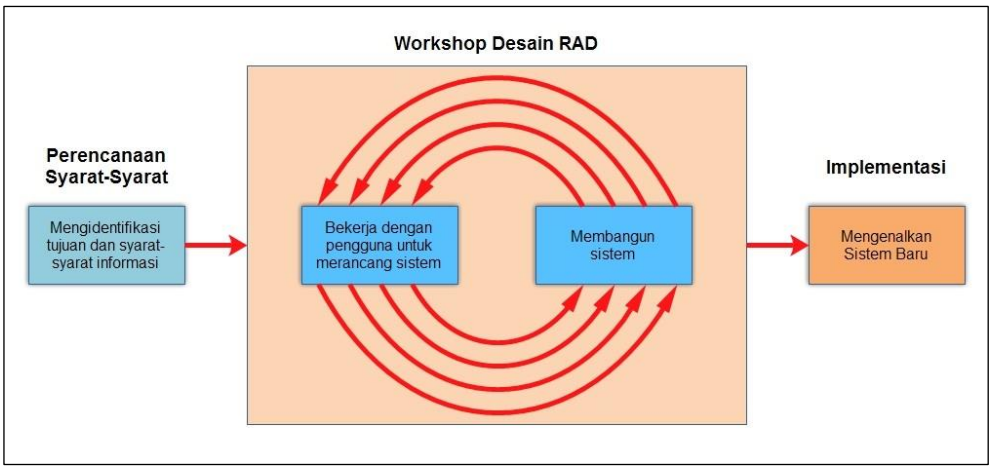
*String* "Namaste Duniya" tidak sama dengan "namaste duniya". Jika dilakukan hash pada *string* "namaste duniya", maka akan mendapatkan hasil yang benar-benar berbeda.

```
namaste duniya -> keccak-256(fungsi hash) ->
544ff8f09d34fdfbfa5a8dcb9d7d57deb6c862026cb8b655cfd7bf9c192e4d21
```

Bahkan perubahan atau modifikasi terkecil pada *string* memiliki dampak signifikan pada hash *digest*. Meskipun banyak input yang diberikan, hasilnya akan selalu sama.

## 2.9 Metode RAD (Rapid Application Development)

Metode *RAD (Rapid Application Development)* adalah pendekatan pengembangan perangkat lunak yang bertujuan untuk mempercepat proses pengembangan dengan menggunakan iterasi, prototipe, dan input-input dari pengguna.




Gambar 2.4 Metode *Rapid Application Development* (Kendall, 2010)

Berdasarkan Gambar 2.4, Model RAD terbagi menjadi 3 tahap, yaitu sebagai berikut:

1. *Requirement Planning* (Perencanaan syarat-syarat)

Kolaborasi antara pengguna dan analis dilakukan pada fase ini untuk mengidentifikasi tujuan sistem dan persyaratan informasi yang dibutuhkan. Fokus utama pada langkah ini adalah menyelesaikan permasalahan yang dihadapi oleh perusahaan (Susilo et al., 2023).

2. Workshop Design

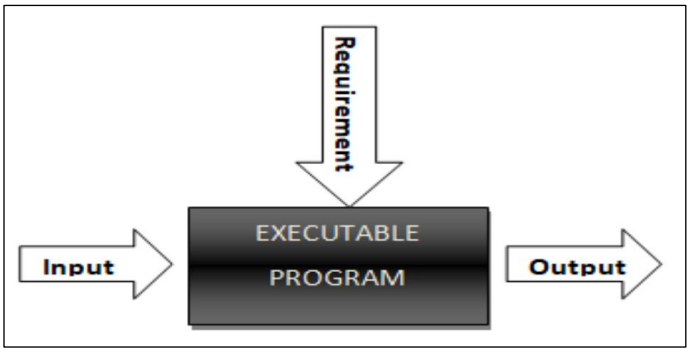
Fase ini dapat dianggap sebagai *workshop desain* di mana analis dan pemrogram bekerja sama untuk membangun dan membuat representasi visual desain serta pola kerja untuk pengguna. Selama fase ini, pengguna memberikan tanggapan terhadap prototipe yang ada dan analis melakukan perbaikan pada modul yang telah dirancang berdasarkan respons pengguna (Susilo et al., 2023).

3. *Implementation* (Implementasi)

Tahap ini merupakan langkah pembangunan dan penyempurnaan sistem sesuai dengan aspek-aspek yang telah disetujui pada tahap desain *workshop*. Sistem kemudian diuji coba dan diperkenalkan kepada organisasi. Proses pada tahap ini terdiri dari pengkodean sistem dan pengujian sistem menggunakan metode *black box testing* untuk menilai apakah terdapat kesalahan pada sistem atau tidak (Pramulia & Anggorojati, 2020).

## 2.10 Black Box Testing

*Black box testing* adalah teknik pengujian perangkat lunak yang digunakan untuk menentukan fungsionalitas aplikasi. Fokus utama dari *black box testing* adalah input yang tersedia untuk suatu aplikasi dan keluaran yang diharapkan untuk setiap nilai input. Metode pengujian ini didasarkan pada persyaratan dan spesifikasi perangkat lunak. Metode ini merupakan teknik pengujian perangkat lunak di mana cara kerja internal dari item yang diuji tidak diketahui oleh penguji (Verma et al., 2017), seperti ditunjukan pada Gambar 2.5.




Gambar 2.5 *Black Box Testing* (Verma et al., 2017)

## 2.11 Penelitian Terkait *(State of The Art)*

Tabel 2.1 Penelitian Terkait *(State of The Art)*

| No | Nama dan Tahun Penelitian | Judul | Media | Metode | Hasil |
|---|---|---|---|---|---|
| 1 | (Lorien & Wellem, 2021) | Implementasi Sistem Otentikasi Dokumen Berbasis Quick Response (QR) Code dan Digital Signature | Dokumen | Menggunakan fungsi *hash SHA256* dan algoritma *Rivest-Shamir-Adleman (RSA)* pada *digital signature* | Pengujian dilakukan dengan 30 sertifikat, dimana 15 sertifikat menggunakan metode tersebut dan 15 tanpa metode tersebut. Hasil pengujian menunjukkan bahwa implementasi sistem otentikasi dokumen berbasis *QR code* dan *digital signature* dapat memastikan keaslian dan integritas dokumen, mencegah pemalsuan, dengan kemampuan mengidentifikasi dokumen palsu yang mencantumkan *QR code* yang tidak dihasilkan oleh sistem ini. |
| 2 | (Saputra & Nasution, 2019) | Analisa Algoritma SHA-256 Untuk Mendeteksi Orisinalitas Citra Digital | Citra Digital | *Secure Hash Algorithm 256 (SHA256)* | Dilakukan pengujian objek ijazah dan transkrip nilai yaitu mengubah resolusi, mengubah nilai 1 *pixel*, mengubah *brightness* dan *contrast*, dan mengubah nilai atau huruf. Algoritma *SHA-256* dapat digunakan untuk mendeteksi orisinalitas citra hasil pemindaian ijazah dan transkrip nilai, mengidentifikasi perubahan bahkan jika hanya terjadi pada satu piksel, dan menghasilkan perbedaan nilai *hash* yang signifikan. |

| No | Nama dan Tahun Penelitian | Judul | Media | Metode | Hasil |
|---|---|---|---|---|---|
| 3 | (Jabbar et al., 2020) | Adopting formal verification and model-based testing techniques for validating a blockchain-based healthcare records sharing system | Aplikasi | *Formal Verification Methodologies* dan *Model Based Testing* | Melakukan pengujian dengan metode tersebut pada *Healthcare Records Sharing System* berbasis *blockchain*. Hasil dari penelitian ini yaitu BiiMED, sebuah kerangka kerja *Blockchain* untuk Meningkatkan Interoperabilitas dan Integritas Data terkait aplikasi *Electronic Health Records (EHR)* |
| 4 | (Gayathiri et al., 2020) | Certificate validation using blockchain | Dokumen (sertifikat) | *Chaotic algorithm* dan *Blockchain* | Membuat suatu aplikasi untuk melakukan validasi pada sertifikat akademik berbasis *blockchain*. |
| 5 | (Nagasubramanian et al., 2020) | Securing e-health records using keyless signature infrastructure blockchain technology in the cloud | Dokumen medis | *Keyless Signature Infrastructure (KSI), Timestamped algorithm, Merkle tree, Blockchain* | Penggunaan metode *Keyless Signature Infrastructure (KSI), Timestamped algorithm, Merkle tree,* dan *Blockchain* menunjukkan bahwa waktu respons sistem yang diusulkan dengan teknologi *blockchain* hampir 50% lebih singkat dibandingkan dengan teknik konvensional. Penelitian ini juga menyatakan bahwa biaya penyimpanan sekitar 20% lebih rendah untuk sistem dengan *blockchain* dibandingkan dengan teknik yang ada. |

| No | Nama dan Tahun Penelitian | Judul | Media | Metode | Hasil |
|---|---|---|---|---|---|
| 6 | (Rakhmansyah et al., 2021) | Smart Digital Signature berbasis Blockchain pada Pendidikan Tinggi menggunakan Metode SWOT | Dokumen | *Algoritma RSA, algoritma SHA256, digital signature* berbasis *blockchain* | Penelitian ini menunjukkan bahwa sistem smart digital signature memperoleh skor SUS sebesar 87.5, yang menempatkannya dalam kategori "Acceptable". Smart digital signature juga diklasifikasikan sebagai Net Promoter karena skor SUS yang melebihi 82, menunjukkan potensi sebagai penggerak penggunaan yang terus meningkat. Meskipun dapat menyebabkan penurunan signifikan, kategori detractor tidak berlaku untuk smart digital signature karena skornya melebihi 67. |
| 7 | (Durand et al., 2020) | Decentralized LPWAN infrastructure using blockchain and digital signatures | Jaringan | *Digital signature* dan *blockchain* | Penelitian ini mengimplementasikan jaringan *blockchain* pada *LoRaWAN network* yang berada pada *physical layer*. Dilakukan percobaan mengirimkan data dan hasilnya LoRaWAN 5+/MB, ECDSA-160 41+/MB, ECDSA-192 49+/MB, ECDSA-256 65+/MB, dan Guib 17+/MB. Hasil dari penelitian ini menjelaskan tentang *LoRaWAN* yang menggunakan jaringan *blockchain* bisa memperkecil biaya pengiriman data, tetapi penelitian ini hanya dilakukan pada jaringan *blockchain* lokal saja, belum dilakukan percobaan untuk public *blockchain*. |

| No | Nama dan Tahun Penelitian | Judul | Media | Metode | Hasil |
|---|---|---|---|---|---|
| 8 | (Sowmiya et al., 2021) | Linear elliptical curve digital signature (LECDS) with blockchain approach for enhanced security on cloud server | Dokumen | *Linear Elliptical Curve Digital Signature (LECDS), Algoritma RSA, Modified Spider Optimization Search Algorithm (MSOA),* berbasis *blockchain* | Penelitian ini melakukan beberapa pengujian yaitu keamanan, waktu eksekusi, *Comparison of throughput, Misclassification performance,* dan *Average latency*. Pengujian dilakukan pada *LECDS, MHT, AuthPrivacyChain*, dan *SDS*. Berdasarkan tabel pada penelitian, nilai rata-rata dari *LECDS* lebih tinggi dibanding yang lain. |
| 9 | (Jayabalasamy & Koppu, 2022) | High-performance Edwards curve aggregate signature (HECAS) for nonrepudiation in IoT-based applications built on the blockchain ecosystem | IoT | *High-performance Edwards curve aggregate signature (HECAS), digital signature* berbasis *blockchain* | Pendekatan yang dikembangkan dalam penelitian ini menyelesaikan tugas penandatanganan dan verifikasi dengan waktu pemrosesan yang 10% dan 13% lebih singkat, masing-masing, dibandingkan dengan skema *digital signature* konvensional. Pengadopsian *High-performance Edwards curve aggregate signature (HECAS)* dalam ekosistem *blockchain* dapat memberikan peningkatan 10% pada aliran transaksi, peningkatan 10% pada validasi blok, dan penurunan 40% dalam biaya penyimpanan relatif terhadap sistem yang sama yang diimplementasikan tanpa *HECAS*. |

| No | Nama dan Tahun Penelitian | Judul | Media | Metode | Hasil |
|---|---|---|---|---|---|
| 10 | (Roopak & Sumathi, 2020) | Electronic voting based on virtual id of aadhar using blockchain technology | Citra (sidik jari) | *Algoritma RSA*, Fitur Ekstrasi, *digital signature* berbasis *blockchain* | Penelitian ini menghasilkan sistem *e-voting* yang aman menggunakan *blockchain*, integrasi *Aadhar*, dan *digital signature*, dengan peningkatan keamanan melalui penggunaan data sidik jari serta penekanan pada panjang kunci dalam proses enkripsi dan dekripsi. |
| 11 | (Shankar et al., 2023) | Improved Multisignature Scheme for Authenticity of Digital Document in Digital Forensics Using Edward-Curve Digital Signature Algorithm | Dokumen | *Edwards-curve Digital Signature Algorithm (EdDSA), Ed25519, algoritma RSA, digital signature* berbasis *blockchain* | Melakukan pengujian analisis pada *RSA, ECDSA*, dan *EdDSA*. Parameter yang diuji yaitu dari keamanan dan waktu dari tiap metode. Hasilnya performa *EdDSA* lebih cepat dibanding yang lainnya, tetapi popularitas nya kalah dari *RSA* karena masih baru. |
| 12 | (Andi et al., 2022) | Securing Medical Records of COVID-19 Patients Using Elliptic Curve Digital Signature Algorithm (ECDSA) in Blockchain | Dokumen medis | *EllipticCurve Digital Signature Algorithm (ECDSA), Blockchain Technology* | Berdasarkan hasil penelitian, teknologi *blockchain* adalah solusi yang tepat dalam mengamankan rekam medis pasien. Penerapan algoritma *ECDSA* cocok untuk melindungi rekam medis pasien *COVID-19* sehingga hanya pihak-pihak yang berkepentingan yang dapat mengaksesnya. |

| No | Nama dan Tahun Penelitian | Judul | Media | Metode | Hasil |
|---|---|---|---|---|---|
| 13 | (X. Zou & Zeng, 2023) | A new digital signature primitive and its application in blockchain | Dokumen | *Expander signature, blockchain* | Penelitian ini bertujuan untuk mengusulkan *digital signature primitive* yang baru, disebut dengan *expander signature.* Hasil dari penelitian ini yaitu suatu metode baru yaitu *expander signature*, dimana metode ini melakukan banyak tanda tangan sekaligus pada satu waktu menggunakan spesifikasi komputer yang tinggi. |

## 2.12 Matriks Penelitian

Tabel 2.2 Matriks Penelitian

| No | Judul, Penulis, dan Tahun | Ruang Lingkup Penelitian | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Objek yang diteliti | | | | Metode | | | | | | | | | | |
| | | | | | | *Hash function* | | *Digital Signature* | | | *Cryptography dan Security* | | *Verification dan Validation* | | | |
| | | **Dokumen** | **Citra** | **Aplikasi** | **Jaringan** | ***SHA256*** | ***Keccak256*** | ***Digital Signature*** | ***ECDSA*** | ***HECAS*** | ***Chaotic Algorithm*** | ***Keyless Signature Insfrastructure*** | ***Expander Signature*** | ***FVM*** | ***Model-Based Testing*** | ***Blockchain*** |
| 1 | Implementasi Sistem Otentikasi Dokumen Berbasis Quick Response (QR) Code dan Digital Signature, (Lorien & Wellem, 2021) | ✓ | - | - | - | ✓ | - | ✓ | - | - | - | - | - | - | - | - |
| 2 | Analisa Algoritma SHA-256 Untuk Mendeteksi Orisinalitas Citra Digital, (Saputra & Nasution, 2019) | - | ✓ | - | - | ✓ | - | - | - | - | - | - | - | - | - | - |
| 3 | Adopting formal verification and model-based testing techniques for validating a blockchain-based healthcare records sharing system, (Jabbar et al., 2020) | - | - | ✓ | - | - | - | - | - | - | - | - | - | ✓ | ✓ | ✓ |

| No | Judul, Penulis, dan Tahun | Ruang Lingkup Penelitian | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Objek yang diteliti | | | | Metode | | | | | | | | | | |
| | | | | | | *Hash function* | | *Digital Signature* | | | *Cryptography dan Security* | | *Verification dan Validation* | | | |
| | | **Dokumen** | **Citra** | **Aplikasi** | **Jaringan** | ***SHA256*** | ***Keccak256*** | ***Digital Signature*** | ***ECDSA*** | ***HECAS*** | ***Chaotic Algorithm*** | ***Keyless Signature Insfrastructure*** | ***Expander Signature*** | ***FVM*** | ***Model-Based Testing*** | ***Blockchain*** |
| 4 | Certificate validation using blockchain, (Gayathiri et al., 2020) | ✓ | - | - | - | - | - | - | - | - | ✓ | - | - | - | - | ✓ |
| 5 | Securing e-health records using keyless signature infrastructure blockchain technology in the cloud, (Nagasubramanian et al., 2020) | ✓ | - | - | - | - | - | - | - | - | - | ✓ | - | - | - | ✓ |
| 6 | Smart Digital Signature berbasis Blockchain pada Pendidikan Tinggi menggunakan Metode SWOT, (Rakhmansyah et al., 2021) | ✓ | - | - | - | ✓ | - | ✓ | - | - | - | - | - | - | - | ✓ |
| 7 | Decentralized LPWAN infrastructure using blockchain and digital signatures, (Durand et al., 2020) | - | - | - | ✓ | - | - | ✓ | - | - | - | - | - | - | - | ✓ |

| No | Judul, Penulis, dan Tahun | Ruang Lingkup Penelitian | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Objek yang diteliti | | | | Metode | | | | | | | | | | |
| | | | | | | *Hash function* | | *Digital Signature* | | | *Cryptography dan Security* | | *Verification dan Validation* | | | |
| | | **Dokumen** | **Citra** | **Aplikasi** | **Jaringan** | ***SHA256*** | ***Keccak256*** | ***Digital Signature*** | ***ECDSA*** | ***HECAS*** | ***Chaotic Algorithm*** | ***Keyless Signature Insfrastructure*** | ***Expander Signature*** | ***FVM*** | ***Model-Based Testing*** | ***Blockchain*** |
| 8 | Linear elliptical curve digital signature (LECDS) with blockchain approach for enhanced security on cloud server, (Sowmiya et al., 2021) | ✓ | - | - | - | - | - | - | ✓ | - | - | - | - | - | - | ✓ |
| 9 | High-performance Edwards curve aggregate signature (HECAS) for nonrepudiation in IoT-based applications built on the blockchain ecosystem, (Jayabalasamy & Koppu, 2022) | - | - | ✓ | - | - | - | ✓ | - | - | - | - | - | - | - | ✓ |
| 10 | Electronic voting based on virtual id of aadhar using blockchain technology, (Roopak & Sumathi, 2020) | - | ✓ | - | - | - | - | ✓ | - | - | - | - | - | - | - | ✓ |
| 11 | Improved Multisignature Scheme for | ✓ | - | - | - | - | - | ✓ | ✓ | - | - | - | - | - | - | ✓ |

| No | Judul, Penulis, dan Tahun | Ruang Lingkup Penelitian | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Objek yang diteliti | | | | Metode | | | | | | | | | | |
| | | | | | | *Hash function* | | *Digital Signature* | | | *Cryptography dan Security* | | *Verification dan Validation* | | | |
| | | **Dokumen** | **Citra** | **Aplikasi** | **Jaringan** | ***SHA256*** | ***Keccak256*** | ***Digital Signature*** | ***ECDSA*** | ***HECAS*** | ***Chaotic Algorithm*** | ***Keyless Signature Insfrastructure*** | ***Expander Signature*** | ***FVM*** | ***Model-Based Testing*** | ***Blockchain*** |
| | Authenticity of Digital Document in Digital Forensics Using Edward-Curve Digital Signature Algorithm, (Shankar et al., 2023) | | | | | | | | | | | | | | | |
| 12 | Securing Medical Records of COVID-19 Patients Using Elliptic Curve Digital Signature Algorithm (ECDSA) in Blockchain, (Andi et al., 2022) | ✓ | - | - | - | - | - | - | ✓ | - | - | - | - | - | - | ✓ |
| 13 | A new digital signature primitive and its application in blockchain, (X. Zou & Zeng, 2023) | ✓ | - | - | - | - | - | - | - | - | - | - | ✓ | - | - | ✓ |
| 14 | Aplikasi Sertifikat Digital Dengan Algoritma Keccak256 Berbasis Blockchain, (Maulana, Firman, 2024) | ✓ | - | - | - | - | ✓ | ✓ | - | - | - | - | - | - | - | ✓ |

Berdasarkan matriks penelitian yang tercantum dalam Tabel 2.2, beberapa penelitian telah membahas penggunaan teknologi *blockchain* untuk keamanan dokumen dan sertifikat digital, namun masih ada beberapa gap atau kekurangan yang harus diatasi. Salah satu contohnya penggunaan *blockchain* tetapi tanpa ada tambahan algoritma *hash*. Penelitian ini berkontribusi dalam bidang verifikasi dan validasi sertifikat digital berbasis *blockchain*. Adapun kebaruan dari penelitian ini adalah:

1. Penggunaan kombinasi digital signature, teknologi blockchain, dan algoritma hash Keccak256 untuk mendeteksi perubahan pada sertifikat digital.
2. Melakukan pengujian khusus pada berbagai bentuk modifikasi sertifikat digital untuk memastikan integritas dan keamanan data.