Hasil Penelitian

Yang Tidak Dipublikasikan

# Interoperabilitas Arsitektur Cryptocurrency: Tinjauan Literatur Sistematis

Guson P. Kuntarto

Irwan Prasetya Gunawan

Berkah I. Santoso

Program Studi Informatika

Fakultas Teknik dan Ilmu Komputer

Universitas Bakrie

Jakarta

Genap 2021/2022

**LEMBAR PENGESAHAN HASIL PENELITIAN YANG TIDAK DIPUBLIKASIKAN**

| | | |
|---|---|---|
| 1. | Judul Penelitian | : Interoperabilitas Arsitektur Cryptocurrency: Tinjauan Literatur Sistematis |
| 2. | Peneliti Utama | |
| | a. Nama Lengkap | : Guson P. Kuntarto, S.T, M.Sc |
| | b. Jenis Kelamin | : Laki Laki |
| | c. Pangkat/Golongan/NIDN | : Lektor / III c / 0316067704 |
| | d. Bidang Keahlian | : Web Technology |
| | e. Program Studi | : Informatika |
| 3. | Tim Peneliti | : Irwan Prasetya Gunawan, Ph.D & Berkah I. Santoso, ST, MTI |
| 4. | Jangka waktu penelitian | : 31 Maret 2022 – 31 Agustus 2022 |

Jakarta, 12 Agustus 2022

Menyetujui,

| | |
|---|---|
| **Ketua Lembaga Penelitian dan Pengembangan** | **Peneliti Utama** |
| ( **Deffi Ayu Puspito Sari, Ph.D.** ) | ( **Guson P. Kuntarto, S.T, M.Sc**. ) |
| NIDN: 0308078203 | NIDN: 0316067704 |

# Abstrak

Meningkatnya penggunaan teknologi blockchain saat ini berdampak pada semakin pentingnya aspek pengelolaan, kelangsungsan hidup, dan keamanan sistem blockchain. Hal yang sama tentu akan berlaku pula pada sistem cryptocurrency. Dengan adanya berbagai macam sistem cryptocurrency yang berbeda-beda, maka interoperabilitas antar sistem yang berbeda ini menjadi hal yang penting. Laporan ini mencoba untuk membahas secara tinjauan literatur sistematis bagaimana dukungan arsitektur cryptocurrency yang berbeda-beda ini terhadap interoperabilitasnya. Sebagai contoh, akan dibandingkan dua sistem cryptocurrency yang berbeda, yaitu Bitcoin dan polkadot. Hasil penelusuran literatur mendapatkan bahwa meskipun secara umum penelitian dengan tema interoperabilitas cryptocurrency cukup banyak, namun interoperabilitas Bitcoin dan polkadot masih belum banyak mendapatkan perhatian. Dari persepektif arsitektur teknologi guna mendukung interoperabilitas, Bitcoin dan polkadot berbeda dalam proses penambangan serta algoritma konsensusnya.

# Daftar Isi

# Bab 1

# Pendahuluan

## 1.1 Latar Belakang

Penggunaan teknologi Blockchain untuk memberikan visibilitas yang lebih baik ke dalam informasi bersama di antara sejumlah peserta dan sistem yang diatur dalam topologi *peer-to-peer* (P2P). Namun, lebih perhatian perlu ditempatkan pada tantangan seputar aspek pengelolaan sistem Blockchain (*manageability*), kelangsungan hidup jaringan blockchain (*survivability*), dan keamanan siber dari sistem dan infrastruktur yang berpartisipasi dalam komunitas blockchain (*cybersecurity*). Penting untuk menjawab tantangan ini adalah kebutuhan untuk memahami aspek arsitektur Internet yang membuatnya terukur, tangguh, dan sukses secara komersial sebagai infrastruktur konektivitas global [1].

Arsitektur blockchain yang dapat dioperasikan adalah komposisi sistem blockchain yang dapat dibedakan, masing-masing mewakili buku besar data terdistribusi (*distributed data ledger*) yang unik, tempat pelaksanaan transaksi dapat menjangkau beberapa sistem Blockchain, dan di mana data direkam dalam satu Blockchain dapat dijangkau, diverifikasi, dan direferensikan oleh kemungkinan transaksi asing lainnya di acara yang kompatibel secara semantik. Teknik interoperabilitas memungkinkan akses tanpa batas (*seamless*) dan aman (*secure*) pelaksanaan kontrak pintar di antara berbagai taksonomi Blockchain public *permissionless, private*, atau *consortium permissioned* Blockchains. Hal ini biasanya diperiksa dari tiga tingkat yang luas, termasuk: (a) Fondasi, (b) Struktural, dan (c) Semantik. Pada dasarnya, data dapat ditransfer dengan lancar di antara yang berbeda sistem. Secara struktural, pertukaran yang disebutkan di atas membutuhkan tempat jika dan hanya jika ada format data yang terdefinisi dengan baik. Dan pada tingkat semantik, data transaksi lintas sistem adalah dapat ditafsirkan oleh pengguna akhir [2].

Teknik interoperabilitas yang diterapkan di dalam arsitektur blockchain tidak terlepas dari isu. Salah satunya adalah aspek *atomicity*. *Atomicity* sangat penting untuk sangat bermanfaat dan aman arsitektur Blockchain. Kuncinya adalah transaksi dijalankan dengan sukses dan lengkap, atau tidak diimplementasikan sama sekali. Dengan kata lain,

jika terjadi satu operasi di jaringan gagal, maka setiap operasi yang belum selesai akan sekaligus gagal [2]. Berangkat dari isu ini, maka dukungan arsitektur menjadi sangat krusial guna dapat memastikan bahwa transaksi lintas rantai memenuhi properti atomisitas (*atomicity*)?

## 1.2 Rumusan Masalah

Laporan ini mencoba membahas melalui tinjauan sistematis literatur mengenai bagaimanakah dukungan arsitektur *cryptocurrency* Bitcoin dan polkadot dalam aspek interoperabilitas guna memastikan bahwa transaksi lintas rantai memenuhi properti atomisitas (atomicity)?

## 1.3 Batasan Masalah

Ruang lingkup dari kajian ini adalah

1. Tinjauan sistematis literatur berbasis pendekatan PICOC dengan sumber literatur daring: *DTU Find-it*;
2. *Cryptocurrency* yang diteliti yaitu Bitcoin dan Polkadot;
3. Pembahasan fokus pada aspek interoperabilitas kedua *cryptocurrency* untuk memenuhi properti atomisitas.

## 1.4 Tujuan Penelitian

Melalui tinjauan sistematis literatur laporan ini mencoba mengidentifikasi bagaimanakah dukungan arsitektur *cryptocurrency* bitcoin dan polkadot dalam aspek interoperabilitas guna memastikan bahwa transaksi lintas rantai memenuhi properti atomisitas (atomicity).

## 1.5 Sistematika Penulisan

1. Bab 1 membahas latar belakang permasalahan dari munculnya beberapa jenis *cryptocurrency* dewasa ini seperti Bitcoin dan Polkadot yang memiliki pendekatan mekanisme atau teknik interoperabilitas. Setelah itu, masalah dirumuskan dan dibingkai dengan batasan masalah sehingga menjadi tujuan penelitian.
2. Bab 2 memaparkan *underlying concept* tentang Blockchain dan *cryptocurrency serta metode tinjauan sistematis literatur yang digunakan di dalam penelitian ini.*

3. Setelah tujuan penelitian dibahas serta didukung dengan paparan mengenai konsep, bab 3 membahas mengenai tahapan penelitian yang digunakan di dalam penelitian. Termasuk dibahas mengenai kriteria-kriteria yang digunakan guna mendukung penelitian.

4. Bab 4 Membahas secara komprehensif mengenai hasil serta diskusi dari tinjauan sistematis literatur serta hasil komparasi dua *cryptocurrency* yaitu Bitcoin dan Polkadot dalam aspek mekanisme interoperabilitas spesifik dalam menjamin properti atomisitas.

5. Bab 5 Memaparkan kesimpulan dari hasil penelitian mengenai tinjauan sistematis literatur serta komparasi dua *cryptocurrency* yaitu Bitcoin dan Polkadot dalam aspek mekanisme interoperabilitas spesifik dalam menjamin properti atomisitas.

# Bab 2

# Tinjauan Konsep

## 2.1 Blockchain

Biasanya, istilah "Blockchain" mengacu pada daftar atau catatan terdesentralisasi dari semua transaksi di jaringan *peer-to-peer*, yang disebut blok, yang berisi elemen data aktual. Arsitektur Blockchain, di sisi lain, terdiri dari jaringan yang disebut node, di mana setiap node menyimpan salinan Blockchain dan terus-menerus menukar salinannya dengan node lain. Dengan demikian, Blockchain harus *persistent*, yaitu entri harus tahan terhadap modifikasi. Untuk mencapai ini, node diharuskan mengikuti protokol tertentu yang terdiri dari beberapa, yang disebut, aturan konsensus [3].

Arsitektur Blockchain adalah turunan dari kelas arsitektur yang lebih umum yang disebut arsitektur dinamis. Dalam arsitektur seperti itu, komponen dapat bergabung atau meninggalkan arsitektur dan koneksi antar komponen dapat berubah seiring waktu. Dinamika ini membuat verifikasi arsitektur semacam itu menjadi tantangan, karena melibatkan penalaran tentang jumlah komponen yang tidak terbatas [3].

### 2.1.1 Karakteristik Blockchain

Terdapat beberapa karakteristik dari Blockchain, yaitu: desentralisasi, persistensi, *anonymity* dan *auditability*. Desentralisasi merupakan mekanisme yang memungkinkan penyelenggaraan transaksi pada jaringan Blockchain berlangsung antara 2 (dua) pasangan penyelenggara transaksi (Peer-to-Peer atau P2P) tanpa adanya otentikasi dari pihak lain secara terpusat. Pada mekanisme desentralisasi, Blockchain dapat mengurangi kekhawatiran terkait kepercayaan antar pengguna dengan penggunaan beberapa prosedur kesepakatan bersama atau konsensus. Persistensi merupakan salah satu karakteristik Blockchain yang menyediakan infrastruktur dengan kemampuan pengukuran tingkat kepercayaan dan mekanisme agar *producer* maupun *consumer* dapat membuktikan data mereka bersifat otentik serta tidak mengalami perubahan pada mekanisme komunikasi. Penggunaan mekanisme *anonymity* ditujukan agar pengguna dapat berinteraksi dengan jaringan

Blockchain menggunakan alamat yang dihasilkan secara acak untuk menghindarkan diri dari paparan terkait identitas pengguna yang bersangkutan. Pada karakteristik *auditability* memungkinkan semua transaksi yang terjadi pada jaringan Blockchain direkam secara digital pada buku jurnal yang terdistribusi dan dilakukan validasi oleh mekanisme *digital timestamp*. Hasil dari karakteristik *auditability* adalah kemampuan untuk dapat dilakukan audit dan penelusuran terhadap rekaman-rekaman yang terjadi sebelumnya dengan melakukan akses terhadap setiap *node* yang berada dalam jaringan Blockchain [4].

### 2.1.2 Taksonomi Blockchain

Terdapat 3 (tiga) tipe Blockchain, yaitu: publik, privat dan konsorsium. Ketiga tipe Blockchain tersebut dapat dibandingkan dengan menggunakan pendekatan cara pandang yang berbeda, seperti dijelaskan pada bagian berikut ini [4] :

1. Penentuan Konsensus
   Semua *node* dapat berpartisipasi pada proses konsensus dalam Blockchain publik seperti Bitcoin, dimana hanya sekumpulan *node* yang berjumlah sedikit bertanggung jawab untuk melakukan konfirmasi suatu blok dalam konsorsium Blockchain.

2. Izin Akses Pembacaan
   Blockchain yang masuk pada tipe publik memungkinkan izin akses pembacaan kepad pengguna, dimana Blockchain privat dan konsorsium dapat membuat akses yang ketat terhadap jurnal yang terdistribusi.

3. *Immutability*
   Pada jaringan Blockchain yang tidak tersentral, transaksi disimpan pada jurnal terdistribusi dan dilakukan validasi oleh semua peserta (peer). Mekanisme tersebut menjadikan ketidakmungkinan untuk melakukan modifikasi dalam jaringan Blockchain publik.

4. Efisiensi
   Pada Blockchain publik, setiap *node* dapat bergabung atau meninggalkan jaringan yang menjadikan mekanisme efisiensi dapat tercapai dengan baik serta memiliki kemampuan untuk bertambah besar serta bertambah banyak.

5. Sentralisasi
   Perbedaan penting diantara ketiga tipe Blockchain tersebut adalah kenyataan bahwa Blockchain publik bersifat terdesentralisasi, sedangkan konsorsium adalah sebagian tersentralisasi dan Blockchain private dikendalikan oleh pihak otoritas yang tersentral.

Berikut ini merupakan tabel komparasi antar infrastruktur Blockchain

Tabel 2.1: Tabel Komparasi Antar Infrastruktur Blockchain [4]

| Properti | Publik | Konsorsium | Privat |
|---|---|---|---|
| Sifat-sifat | Terbuka dan terdesentralisasi | Terkendali dan memiliki batasan | Terkendali dan memiliki batasan |
| Partisipan | *Anonymous* dan *Resilient* | Teridentifikasi dan terpercaya | Teridentifikasi dan terpercaya |
| Prosedur Konsensus | PoW, PoS, DPoS | PBFT | PBFT, RAFT |
| Hak Akses Pembacaan atau Penulisan | Tidak terdapat Hak Akses | Terdapat Hak Akses | Terdapat Hak Akses |
| *Immutability* | Tidak dapat dilakukan penyadapan | Dapat dilakukan penyadapan | Terkendali dan dapat dilakukan penyadapan |
| Efisiensi | Rendah | Tinggi | Tinggi |
| Skalabilitas | Tinggi | Rendah | Tinggi |
| Frekuensi Persetujuan Transaksi | Panjang atau lama (lebih dari 10 menit) | Pendek atau Cepat | Pendek atau Cepat |
| Konsumsi Energi | Tinggi | Rendah | Rendah |
| Transparansi | Rendah | Tinggi | Tinggi |
| Observasi | Disruptif terkait dengan disintermediasi | Efektif biaya terkait dengan penggunaan data kembar yang lebih sedikit dan waktu transaksi yang lebih tinggi | Efektif biaya terkait dengan penggunaan data kembar yang lebih sedikit dan waktu transaksi yang lebih tinggi |
| Contoh | Bitcoin, Ethereum, Litecoin, Factom, Blockstream, Dash | Ripple, R3, Hyperledger | Multichain, Blockstack, Bankchain |

### 2.1.3 Prosedur Konsensus pada Blockchain

Pada Blockchain, mekanisme untuk mendapatkan konsensus diantara *node* yang tidak dipercaya merupakan transformasi dari pemecahan masalah yang disebut Byzantine General (BG). Pada analogi pemecahan masalah BG, sekelompok jenderal memerintahkan sebagian tentara Byzantine untuk mengelilngi kota. Serangan yang dilancarkan akan mengalami kegagalan jika hanya sebagian jenderal yang menyerang kota tersebut. Para jenderal perlu melakukan komunikasi untuk mencapai persetujan apakah akan melakukan serangan atau tidak menyerang. Namun demikian dapat saja terdapat pengkhianat diantara kelompok jenderal tersebut. Pengkhianat dapat mengirimkan keputusan-keputusan yang berbeda untuk para jenderal yang berbeda. Pada jaringan Blockchain merupakan lingkungan yang tidak memiliki kepercayaan dan bersifat terdistribusi sehingga hal tersebut merupakan suatu tantangan untuk mencapai konsensus. Maka diperlukan adanya beberapa protocol untuk memastikan bahwa jurnal-jurnal pada *node* yang berbeda bersifat konsisten. Beberapa pendekatan umum akan disajikan dalam rangka membentuk konsensus pada Blockchain [4].

1. *Proof of Work* (PoW)
   Proof-of-Work (PoW) merupakan algoritma konsensus berbasiskan mekanisme pembuktian. Konsep dasar dari teknik konsensus adalah untuk melakukan identifikasi dan penentuan suatu *node* yang akan mendapatkan hak untuk menambahkan blok baru terhadap rantai koneksi yang sedang terbentuk dengan penyediaan bukti-bukti yang cukup atas usaha-usaha yang telah dilakukan. Prosedur konsensus ini telah lama digunakan pada jaringan Bitcoin.
   Pada konsensus ini terdapat masalah yang timbul akibat kebingungan antar node yang terjadi apabila setiap node mencoba untuk melakukan mekanisme *broadcast* berisi transaksi-transaksi yang telah diverifikasi secara sama. PoW mencoba memecahkan masalah yang timbul tersebut sebagai node yang membutuhkan pemecahan masalah dari potongan-potongan petunjuk yang sukar dengan penyesuaian tingkat kesulitan dalam rangka mendapatkan kesempatan untuk menambahkan blok baru pada rantai koneksi yang terjadi.
   *Node-node* yang akan bergabung pada proses tersebut disebut *miners*, sedangkan proses bergabungnya *node* disebut *mining*. *Miners* bertanggung jawab untuk melakukan pemilihan transaksi yang telah dilakukan verifikasi terpilih untuk membentuk suatu blok bersama-sama menyertakan informasi lainnya seperti *hash* sebelumnya dan *timestamp*. Selanjutnya fungsi *hash* 256 akan digunakan untuk mengubah semua informasi yang terkandung dalam *header block* untuk membuat nilai *hash* [4].

2. *Proof of Stake* (PoS)
   *Proof of Stake* (PoS) dapat menjadi suatu alternatif yang efisien pada pendekatan

prosedur konsensus pada Blockchain. Pada metode konsensus PoS, *miner* tidak perlu membuang sumber daya komputasi dengan jumlah besar untuk memecahkan masalah potongan-potongan petunjuk secara matematis. Selain itu, PoS tergantung pada pemenuhan acuan yang memadai pada sistem Blockchain agar *node-node* dapat berpartisipasi pada proses pembuatan blok. Kesempatan untuk melakukan validasi suatu blok seluruhnya tergantung pada acuan atau tingkat keberagaman atribut dari *node-node* yang berpartisipasi. Pada saat suatu validator dipilih berdasarkan acuan validator, maka validator tersebut akan memiliki blok pada jaringan Blockchain, dengan melakukan eliminasi kompetisi antar *peer*. Apabila blok tersebut disetujui, maka validator akan mengumpulkan bayaran dari transaksi pada blok tersebut, sehingga PoS menghemat lebih banyak energi komputasi agar dapat menyediakan latensi dan *throughput* yang lebih baik [4].

3. *Delegated Proof of Stake* (DPoS)
   *Delegated Proof of Stake* (DPoS) merupakan prosedur konsensus yang menggunakan mekanisme pemilihan dimana masing-masing *node* dengan acuan pada jaringan dapat mendelegasikan validasi transaksi kepada *node* yang lain dengan proses pemilihan. Mekanisme pemilihan tersebut merepresentasikan metode demokratis apabila dibandingkan dengan Proof of Stake (PoS) yang mengusung pendekatan demokratis langsung. Mekanisme delegasi tersebut dipilih oleh pihak yang berkepentingan untuk menghasilkan dan melakukan validasi suatu blok yang disebut sebagai saksi. *Node-node* yang terpilih selanjutnya akan membentuk sekumpulan blok yang diajukan dan melakukan validasi terhadap kondisi data. *Node-node* tersebut akan mengambil giliran melakukan pemilihan blok-blok sebagai perwakilan dari pihak-pihak yang berkepentingan dan *node-node* tersebut melakukan validasi terhadap mekanisme otentikasi blok-blok sebelumnya. Adapun keterbatasan utama dari mekanisme konsensus DPoS adalah kecenderungan terhadap sentralisasi, dimana partisipan yang memiliki acuan tinggi dapat melakukan pemilihan terhadap dirinya sendiri dan melakukan rekayasa partisipan lainnya untuk memilih sebagai validator. Bitshare merupakan contoh platform pada Blockchain yang menggunakan algoritma konsensus DPoS [4].

4. *Practical Byzantine Fault Tolerance* (PBFT)
   *Byzantine Fault Tolerance* (BFT) mengacu pada prosedur konsensus antara dua *node* yang berkomunikasi dengan aman melalui jaringan terdistribusi dihadapan *node-node* yang berbahaya dan menyesatkan. PBFT merupakan salah satu contoh penerapan BFT yang menggunakan algoritma replikasi yang dapat memberikan toleransi terhadap kesalahan-kesalahan pada Byzantine. PBFT mengasumsikan bahwa *node-node* tertentu tidak jujur atau memiliki kesalahan dan PBFT didesain untuk menjadi algoritma konsensus dengan kinerja tinggi. Algoritma konsensus tersebut

dapat mengandalkan sekumpulan *node-node* yang dipercaya pada jaringan. *Node-node* dalam PBFT diatur pada suatu antrian dimana satu node menjadi pemimpin antrian, sedangkan node yang lain bertindak sebagai *node* cadangan.
Ketika pemimpin *node* mendapatkan permintaan, maka pemimpin *node* tersebut akan memberitahukan permintaan kepada *node* cadangan dan melakukan proses atas permintaan tersebut. Pemimpin *node* menginformasikan hasil proses kepada pihak asal yang melakukan permintaan, sementara pemimpin node menunggu balasan dari *node-node* yang lain dengan hasil yang tepat sama. Hal ini memberikan makna bahwa proses pengambilan keputusan dilakukan melalui pemilihan mayoritas, dimana masing-masing *node* berkomunikasi dengan *node* lainnya dalam rangka pembuktian terhadap asal dari pesan yang telah diberi tanda secara digital untuk memastikan integritas pesan tersebut. Hyperledger fabric sebagai salah satu platform berbasis Blockchain telah menyediakan solusi terkait bisnis dengan meningkatkan pemanfaatan konsensus protokol PBFT [4].

5. *Tendermint*
   Tendermint merupakan salah satu prosedur konsensus yang berbasiskan pada algoritma konsensus Byzantine. Suatu blok baru ditentukan pada masing-masing putaran, sehingga semua *node* harus diketahui untuk pemilihan pihak yang mengajukan. Suatu blok dapat terbagi menjadi tiga tahapan, yaitu tahapan sebelum pemilihan, tahapan sebelum komitmen dan tahapan pembentukan komitmen.
   Pada tahapan sebelum pemilihan, para validator memilih apakah akan melakukan *broadcast* hasil sebelum pemilihan terhadap blok yang diajukan. Pada tahapan sebelum komitmen, apabila sebuah *node* telah menerima lebih dari 2/3 hasil sebelum pemilihan pada blok yang diajukan, maka *node* tersebut akan melakukan *broadcast* hasil sebelum komitmen untuk blok tersebut. Jika suatu node telah menerima lebih dari 2/3 hasil sebelum komitmen, maka node tersebut akan masuk pada tahapan pembentukan komitmen. *Node* tersebut melakukan validasi terhadap blok dan melakukan *broadcast* komitmen terhadap blok tersebut dalam tahap akhir. Jika suatu *node* telah menerima 2/3 komitmen, maka *node* akan menerima blok tersebut.
   Proses tersebut serupa dengan PBFT, akan tetapi *node-node* pada Tendermint harus melakukan penguncian koin-koin pada *node* untuk menjadi validator. Pada saat ditemukan suatu validator tidak jujur, maka validator tersebut akan diberikan hukuman atau sanksi oleh prosedur konsensus Tendermint [4].

## 2.2 *Cryptocurrency*

Blockchain adalah teknologi yang memungkinkan keberadaan *cryptocurrency* (antara lain). Bitcoin merupakan salah satu dari mata uang kripto (*cryptocurrency*) yang menggu-

nakan platform dasar teknologi blockchain. Sebagai mata uang digital terenkripsi, *cryptocurrency* dioperasikan dalam sistem yang tidak dapat terwujud, dan catatan komprehensif yang terstruktur dengan baik dari keseluruhan jaringan yang luar biasa memenuhi fitur 5 V Big Data (volume, variasi, kecepatan, kebenaran, dan nilai) [5].

Diatas aspek-aspek keamanan, *cryptocurrency* harus memastikan bahwa terdapat unsur-unsur uang, yaitu dapat dipertukarkan, dapat diukur atau dihitung dan dapat memiliki nilai. Sebagai tambahan, *cryptocurrency* memiliki keuntungan dengan menambahkan aspek-aspek seperti *pseudonymization* dengan cara menyembunyikan identitas asli dari pemangku kepentingan transaksi, *decentralization* dengan memungkinkan terjadinya verifikasi transaksi oleh banyak pihak, pengurangan biaya transaksi apabila dibandingkan dengan kanal-kanal pengiriman uang secara tradisional, pengiriman uang cepat dengan mengatasi batasan institusi dan teritorial, tidak memiliki kepercayaan terpusat, dengan cara menghilangkan validator yang biasa dipercaya secara terpusat.

Beberapa fasilitas lainnya adalah kemampuan untuk dapat diubah kepada platform *cryptocurrency* lainnya dan uang kertas, kemampuan tidak dapat dikembalikan kepada bentuk sebelumnya, dengan cara memastikan bahwa sekali transaksi *cryptocurrency* tersebut dilakukan maka tidak akan dapat dilakukan proses ke bentuk sebelumnya, fasilitas penempatan transaksi secara cepat dengan cara pertukaran nilai secara cepat antara pihak-pihak yang bertransaksi dan fasilitas pemenuhan *cryptocurrency* yang terkendali untuk meningkatkan titik *equilibrium* yang seimbang serta peningkatan nilai intrinsik yang baik [6].

*Cryptocurrency* mengelola identitas penggunanya menggunakan antrian acak panjang dari beberapa karakter, disebut sebagai kunci privat (kata kunci rahasia) dan kunci publik (nama pengguna secara publik). *Wallets* merupakan aplikasi yang digunakn untuk membuat, menyimpan kunci dan mengelola kunci serta untuk melakukan transaksi *cyrptocurrency*. Jenis-jenis *wallet* bervariasi sebagai bentuk dukungan atas tipe penyimpanan seperti *cold storage wallet* dan *hot storage wallet*. Pada *cold storage wallet* tetap berada pada mode *offline* dan *cold storage wallet* terhubung secara *online* hanya ketika pengguna membutuhkannya untuk melakukan transaksi. Tipe-tipe *wallet* tersebut mencakup *hardware wallet*, dimana perangkat lunak *wallet*, kunci privat dan kunci publik serta catatan keuangan *cryptocurrency* tersimpan pada perangkat fisik. Sedangkan pada *hot storage wallet* yang selalu terkoneksi secara *online* untuk menyimpan informasi. Bentuk dari *hot storage wallet* berupa aplikasi berbasis perangkat *mobile* dan aplikasi berbasis *desktop*, atau aplikasi *hot storage wallet* tersebut diletakkan pada web server dan cloud server. Beberapa tipe tambahan dari *wallet* adalah *multisignature wallet, simplified payment verification (SPV) wallet* dan *brain wallet* [6].

Mekanisme pertukaran secara *online* memungkinkan terjadinya transaksi lintas *platform* dan transaksi yang tidak berbatas antar *platform*. Mekanisme pertukaran diberi kategori sebagai layanan penghubung atau *brokerage services*, mekanisme pertukaran yang

bersifat *order booking* dan *platform* perdagangan.

Jaringan pembayaran juga merupakan salah satu aspek penting pada *cryptocurrency*. Perusahaan pembayaran beroperasi sebagai jaringan penghubung pihak ketiga antara berbagai *platform cryptocurrency* dengan pihak pelaksana perekonomian secara umum. Jaringan pembayaran dikategorikan sebagai jalur pembayaran yang memiliki fokus pada mata uang nasional dan pembayaran *cryptocurrency* yang memiliki fokus pada *cyrptocurrency*.

Teknologi Blockchain yang mengedepankan mekanisme terdistribusi dan terdesentralisasi teknologi jurnal yang tersebar melalui jaringan *peer to peer* dan memastikan aspek *immutability* menggunakan fungsi matematika yang rumit untuk menghasilkan kriptografi. Nilai intrinsik yang terdapat pada *cryptocurrency* adalah ditentukan oleh aspek-aspek dan fungsionalitas yang mendasari sistem Blockchain [6].

Sistem *mining* juga digunakan sebagai pembentuk *cryptocurrency*. Sebagai contoh Bitcoin memiliki protokol konsensus terdistribusi yang memiliki kemampuan untuk mengatur dirinya sendiri dalam rangka pengelolaan jurnal yang terdistribusi secara terdesentralisasi. Untuk memastikan pemenuhan kebutuhan atas koin-koin baru pada sistem, Bitcoin memperkenalkan konsep *mining* yang bekerja dimana para validator diminta untuk menemukan kunci-kunci *hash* secara acak dengan komponen-komponen khusus untuk melakukan verifikasi transaksi baru yang memasuki fase tunggu dan menambahkan transaksi tersebut pada blok selanjutnya. Para validator yang mendapatkan undian benar akan diberi penghargaan sejumlah nilai Bitcoin.

Terdapat beberapa pemangku kepentingan dari *cryptocurrency*, diantaranya adalah [6]:

- Pengguna, manusia, aplikasi atau sistem yang mengirimkan dan menerima koin.
- *Service enabler*, pengembang individual atau perusahaan yang menyediakan pengembangan dan platform perdagangan untuk *cryptocurrency*.
- Regulator, pimpinan perusahaan, perusahaan dan perwakilan perusahaan, konsorsium yang merumuskan desain kebijakan, kerangka kerja operasi berikut aturan terkait dan prosedur untuk penggunaan etika dan legalitas sistem *cryptocurrency*.
- Validator, seseorang atau perusahaan yang melakukan penambangan *cryptocurrency* dan melakukan validasi transaksi.

Terdapat beberapa masalah kepercayaan pada ekosistem *cryptocurrency*, yaitu: manipulasi harga dan volatilitas, *insider trading*, ekonomi bayangan dan ekonomi paralel, reputasi dari sistem, kurangnya transparansi, tumbuhnya aspek sentral, *token economy*, tata kelola dan aturan main, desain dan penggunaan, privasi dan keamanan.

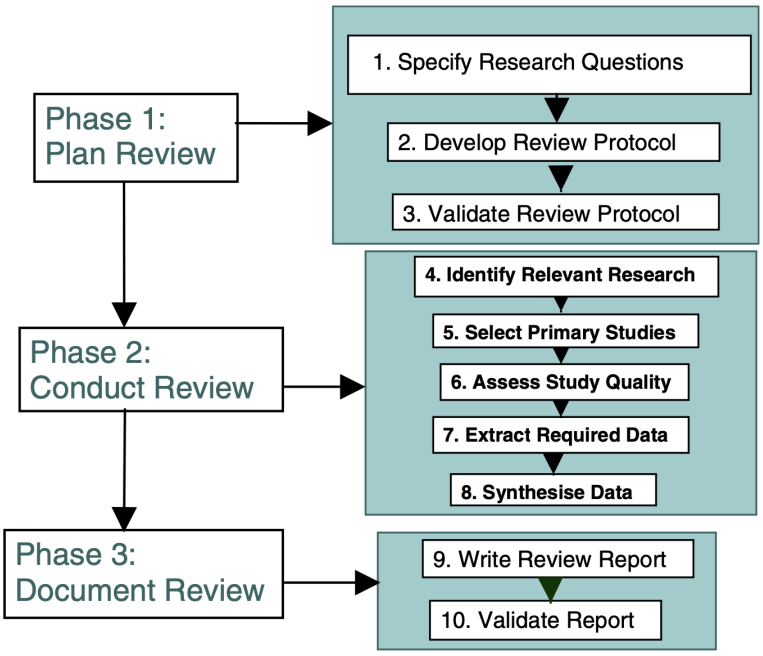
Hingga 2020, telah terdapat 10 (sepuluh) *cyrptocurrency* utama dengan karakteristiknya masing-masing, yaitu: Bitcoin, Ethereum, Ripple, Bitcoin Cash, EOS, Steller, Litecoin, Tether, Bitcoin SV, dan Tron [6].

## 2.3 Tinjauan Literatur Sistematis

Tujuan utama laporan penelitian kali ini adalah untuk mempelajari metode serta teknik interoperabilitas antar sistem cryptocurrency yang sudah diteliti dan dilakukan selama ini. Oleh karena itu, kami menggunakan metode tinjauan literatur sistematis (*systematic literature review*, SLR) sebagai sarana untuk mencapai tujuan tersebut. Ini kami lakukan karena SLR dapat mengevaluasi dan menafsirkan semua penelitian yang tersedia yang relevan dengan permasalahan penelitian atau topik tertentu. Penelitian dengan metode SLR dapat digolongkan ke dalam penelitian sekunder, sementara literatur atau hasil-hasil penelitian yang dipelajari dengan menggunakan SLR adalah penelitian primer. Hasil penelitian sekunder sebagaimana yang dilakukan melalui metode SLR diharapkan dapat memberikan informasi yang berharga mengenai topik tertentu yang kemudian bisa diklarifikasi lebih lanjut melalui penelitian primer.

Proses SLR dapat dilakukan dalam beberapa tahapan seperti yang dijelaskan pada Gambar 2.3. Secara garis besar, tahapan SLR terdiri atas tiga fase: perencanaan (*plan*), pelaksanaan (*conduct*), dan penulisan (*conduct*).

Di tahap perencanaan, permasalahan yang akan dijawab oleh penelitian diformulasikan dalam bentuk *research question* (RQ). Perumusan ini penting karena dapat menjaga agar pencarian literatur yang dilakukan tidak meluas kepada hal-hal yang kurang relevan dengan tujuan penelitian. RQ digunakan sebagai panduan untuk memilih kata kunci pencarian dalam pencarian otomatis literatur serta untuk untuk menentukan data yang




Gambar 2.1: Tahapan-tahapan *systematic literature review* (SLR) [7]

perlu diekstrak dari setiap literatur primer yang didapat. Formulasi permasalahan yang dirumuskan dalam RQ dibentuk dengan kerangka PICOC [8, 9]:

- *Population*: objek yang akan ditelaah atau diteliti (*who* atau *what*)
- *Intervention*: metode, teknik, atau teknologi yang diterapkan pada populasi (*how*)
- *Comparison*: perbandingan antar metode intervensi yang satu terhadap yang lain
- *Outcomes*: hasil yang diinginkan
- *Context*: lingkungan tempat studi yang dilakukan bisa diterapkan dan menerima manfaat dari studi yang dilakukan, misalnya apakah akademis, industri, atau subset dari ranah industri, dan sebagainya.

Selain itu, komponen penting lainnya dalam tahapan perencanaan ini adalah penyusunan protokol untuk penelitian. Dalam hal ini, protokol memberikan rincian rencana untuk melakukan tinjauan literatur yang akan dilakukan, termasuk, misalnya, menentukan proses yang harus diikuti dan kondisi untuk diterapkan ketika memilih studi utama dan menentukan metrik kualitas yang akan diterapkan pada studi utama.

Di tahapan pelaksanaan, dilakukan proses pencarian literatur sesuai dengan RQ dan protokol yang sudah disepakati. Strategi pencarian literaturnya dilakukan dengan pendekatan yang dijelaskan dalam [7]:

- Pertanyaan penelitian didekomposisi menjadi elemen individu yang terkait dengan teknologi, arsitektur, dan interoperabilitas dari system cryptocurrency
- Kata-kata kunci yang diperoleh dari studi-studi utama yang diketahui dinilai untuk istilah-istilah utama lainnya.
- Sinonim untuk istilah utama diidentifikasi.
- String pencarian dibangun menggunakan Boolean ”AND” untuk menggabungkan istilah utama dan ”OR” untuk memasukkan sinonim.

Sebagaimana dijelaskan dalam [7], layanan index literatur yang bisa digunakan dalam pencarian literatur untuk SLR ini adalah:

- IEEExplore
- ACM Digital library
- Google scholar (<scholar.google.com>)
- Citeseer library (<citeseer.ist.psu.edu>)
- Keele University’s electronic library (<opac.keele.ac.uk>)
- Inspec (<www.iee.org/publish/inspec/>)
- ScienceDirect (<www.sciencedirect.com>)

- EI Compendex (<www.engineeringvillage2.org/control-ler/servlet/athensservice>)

Sebagai alternatif dari layanan index individual seperti di atas, bisa juga digunakan layanan index terpadu seperti yang disediakan oleh *DTU Find-it* (https://findit.dtu.dk/).

Penggunaan database yang berbeda pada pencarian bukan tidak menimbulkan masalah, sebagaimana dilaporkan dalam [7]. Permasalahan timbul karena layanan pencarian pada database elektronik dibangun dengan model yang unik, sehingga pencarian kata kunci utama pada satu database mungkin tidak bisa digunakan secara serta merta pada layanan database lainnya. Kemudian, [7] juga melaporkan bahwa hasil evaluasi string pencarian secara Boolean tergantung dari urut-urutan kata kuncinya. Oleh karena itu, [7] menggunakan kumpulan kata kunci yang berbeda untuk masing-masing database elektronik dalam proses pencariannya.

Permasalahan yang dihadapi oleh [7] dalam pencarian literatur sepertinya bisa diatasi dengan menggunakan layanan terpadu seperti yang dilaporkan oleh [10]. Layanan searching database *DTU Find-it* yang digunakan dalam [10] menggali sumber-sumber literatur dari *ACM*, *IEEE*, *Scopus*, *Citeseer*, *arXiv*, dan beberapa sumber database jurnal lainnya yang banyak digunakan.

# Bab 3

# Metode

Di bagian ini kami akan memaparkan metode yang kami gunakan untuk mendapatkan literatur yang relevan dengan permasalahan yang kami ajukan. Kami menggunakan metode yang biasa digunakan dalam proses penulisan review literatur sistematis (atau *systematic literatur review*) seperti yang dijelaskan dalam [8].

Kami berangkat dari pengertian bahwa interoperabilitas sistem cryptocurrency memungkinkan akses tanpa batas (*seamless*) dan aman di antara berbagai taksonomi blockchain yang berbeda, dengan berdasarkan prinsip atomicity.

Formulasi permasalahan kami rumuskan dalam *Research Question* (RQ) yang dibentuk dengan kerangka PICOC [8] sebagai berikut:

- *Population*: sistem cryptocurrency
- *Intervention*: teknik yang digunakan untuk mendukung interoperabilitas antara sistem cryptocurrency yang berbeda-beda
- *Comparison*: perbandingan beberapa arsitektur cryptocurrency yang berbeda dan permasalahan interoperabilitasnya dari aspek konsensus algoritmanya
- *Outcomes*: paparan mengenai arsitektur serta teknik interoperabilitas dari beberapa sistem cryptocurrency yang berbeda
- *Context*: perbandingan dilakukan dalam ranah penelitian akademis dengan menganalisis protokol-protokol yang ada

Berdasarkan metode di atas, kami menyusun RQ sebagaimana diberikan di Section 2.3, yaitu: "bagaimanakah dukungan arsitektur cryptocurrency Bitcoin dan polkadot dalam aspek interoperabilitas guna memastikan bahwa transaksi lintas rantai memenuhi properti atomisitas?"

Dari RQ yang sudah ditetapkan ini, kami turunkan kandidat kata kunci yang digunakan dalam pencarian literatur sebagai berikut: *cryptocurrency architecture* (KS1), *blockchain architecture* (KS2), *cryptocurrency interoperability* (KS3), *blockchain interoperability* (KS4), *atomicity* (KS5), *bitcoin* (KS6), dan *polkadot* (KS7).

Tidak semua kandidat kata kunci ini memberikan informasi yang diinginkan untuk tujuan penelitian kali ini, karena ada beberapa kata kunci yang memiliki jangkauan yang luas ketika diberikan sebagai masukan dari mesin pencari yang digunakan. Oleh karena itu, hanya sebagian dari kandidat kata kunci ini yang digunakan dalam proses pencarian literatur; dari beberapa kata kunci yang digunakan, pengerucutan pencarian dilakukan dengan menggabungkan dua kandidat kata kunci yang berbeda.

Untuk mesin pencari yang digunakan dalam penelusuran literatur, kami putuskan untuk menggunakan *DTU Find-it* sebagai alat utama pencarian kami dengan pertimbangan seperti yang dijelaskan dalam [10] bahwa mesin pencari tersebut menjangkau sumber-sumber yang terdiri dari berbagai macam sumber indeks literatur lainnya. Hal ini tentunya diharapkan bisa menghindari proses pencarian dari permasalahan yang serupa dengan yang dihadapi oleh [7] serta menyederhanakan proses pencarian itu sendiri namun tetap dengan memberikan hasil yang lebih baik.

Selanjutnya kami menerapkan kriteria-kriteria tertentu untuk memilah-milah lebih lanjut literatur yang sudah didapatkan melalui proses pencarian ini. Kriteria tersebut dinyatakan dalam beberapa IC (*inclusion criteria*) dan EC (*exclusion criteria*) sebagai berikut:

- IC1: literatur ditulis dalam Bahasa Inggris
- IC2: literatur ditulis dalam Bahasa Indonesia
- IC3: literatur membahas tentang arsitektur sistem *cryptocurrency*
- IC4: literatur membahas tentang interoperabilitas sistem *currency*
- EC1: literatur tidak ditulis dalam Bahasa Inggris atau Bahasa Indonesia

Dalam penelitian kali ini, kami tidak membatasi jenis literatur yang didapat dalam proses pencarian ke dalam jenis artikel/makalah yang diterbitkan dalam jurnal melalui proses review (*peer reviewed article*). Kami beralasan bahwa satu dari sistem cryptocurrency yang menjadi fokus penelitian kali ini, yaitu *polkadot*, merupakan sistem yang cukup baru sehingga akan cukup sulit untuk mendapatkan literatur dalam topik ini di penerbitan jurnal konvensional.

# Bab 4

# Hasil dan Diskusi

## 4.1 Hasil

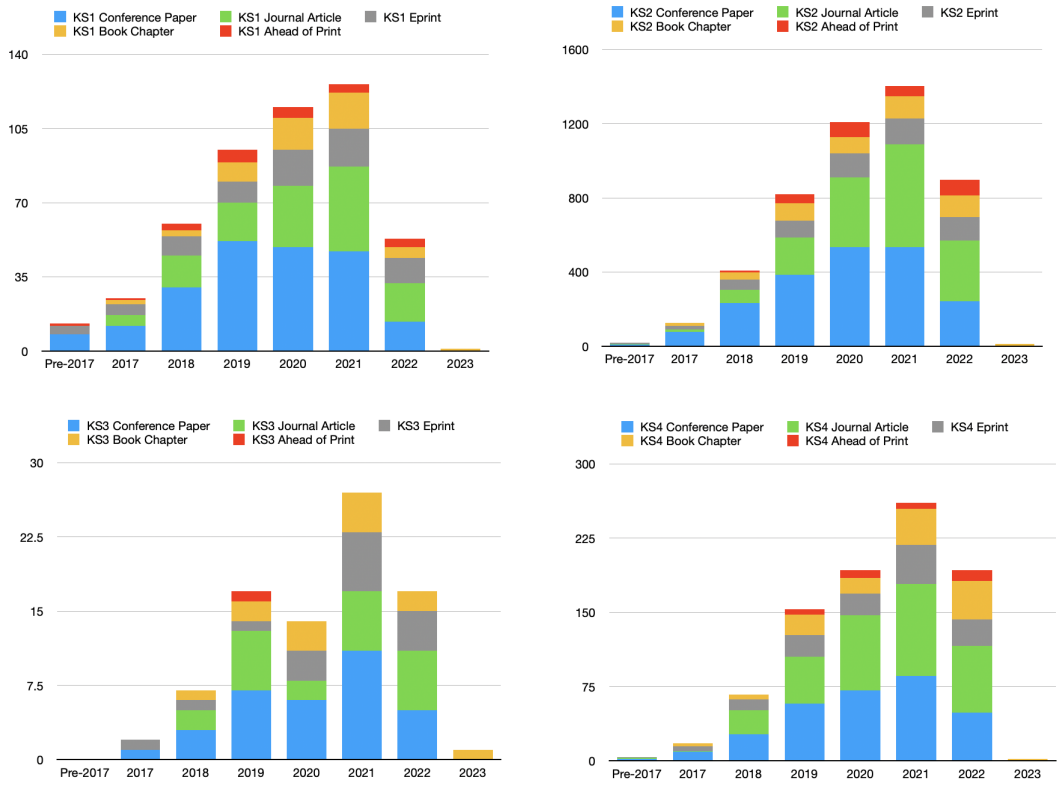
Pada sub bab ini dipaparkan hasil tinjauan sistematis literatur serta arsitektural komparasi BitCoin dan Polkadot dalam aspek interoperabilitas.

### 4.1.1 Tinjauan Literatur Sistematis

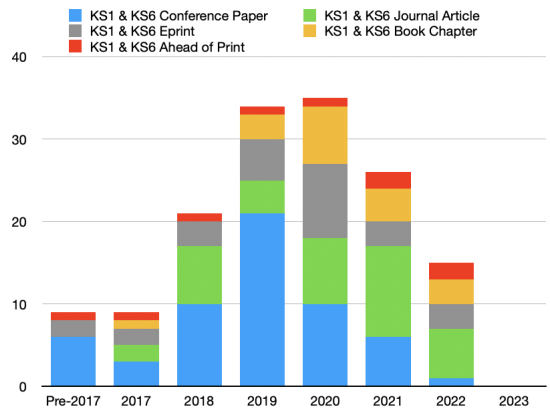
Pencarian dengan kata kunci **KS1** - **KS4** bisa dilihat di Gambar 4.1. Literatur dengan tema blockchain terlihat lebih unggul dari segi jumlah daripada literatur dengan tema cryptocurrency, baik dari sisi aspek arsitektur maupun interoperabilitasnya. Hal ini masuk akal, karena blockchain bersifat lebih umum daripada cryptocurrency.

Hasil pencarian dengan kata kunci kombinasi **KS1 & KS7** (*cryptocurrency architecture polkadot*) pada mesin pencari yang digunakan tidak memberikan hasil. Mungkin bisa dipahami karena arsitektur polkadot tergolong masih baru (muncul pertama kali di tahun 2020). Ini sangat kontras dengan pencarian menggunakan kombinasi **KS1 & KS6** (*cryptocurrency architecture bitcoin*) yang memberikan hasil cukup signifikan seperti terlihat pada Gambar 4.2.

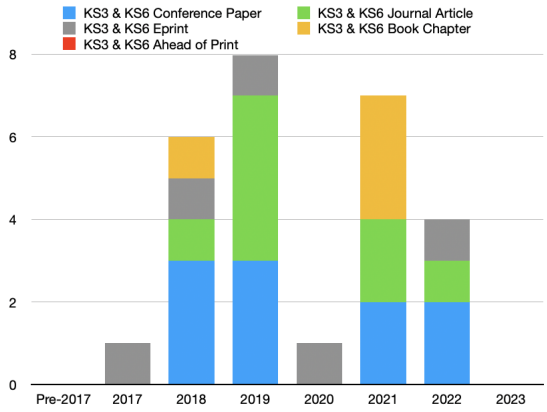
Sementara itu, pencarian dengan kata kunci kombinasi **KS3 & KS6** (*cryptocurrency interoperability bitcoin*) memberikan hasil yang bisa diringkas dalam Gambar 4.3. Dari sisi jumlah, terlihat sangat sedikit apabila dibandingkan dengan hasil pencarian menggunakan kata kunci **KS1 & KS6** dan kata kunci **KS3**. Dari 85 literatur yang membahas cryptocurrency interoperabilitas secara umum, hanya 27 literatur atau sekitar 31.76% saja yang membahas interoperabilitas bitcoin ini. Jumlah yang lebih sedikit lagi didapatkan untuk literatur yang membahas sifat interoperabilitas polkadot; dari pencarian yang dilakukan dengan kata kunci **KS3 & KS7**, hanya 1 literatur yang memenuhi persyaratan pencarian.




Gambar 4.1: Hasil pencarian dengan kata kunci KS1 - KS4




Gambar 4.2: Hasil pencarian dengan kata kunci kombinasi **KS1 & KS6**




Gambar 4.3: Hasil pencarian dengan kata kunci kombinasi **KS3 & KS6**

### 4.1.2 Arsitektural Komparasi BitCoin dan Polkadot dalam Aspek Interoperabilitas

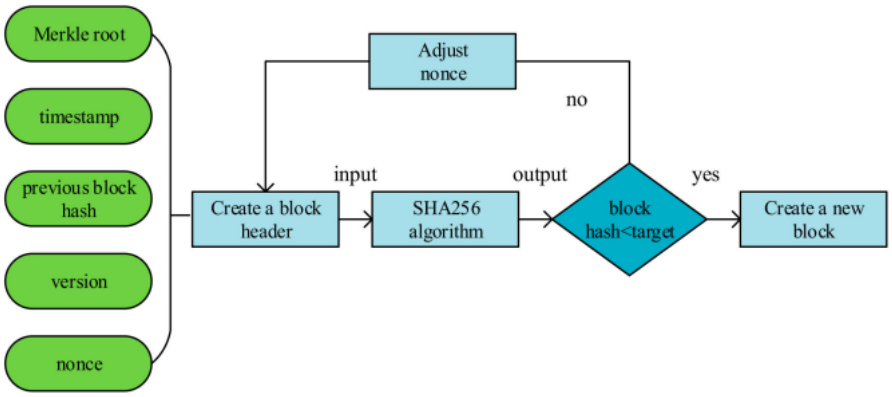
Secara arsitektural, penambangan Bitcoin melibatkan menebak angka acak (yang disebut *nonce*), menambahkannya ke blok kandidat dan memeriksa apakah hash yang sesuai menunjukkan bentuk tertentu (dimulai dengan sejumlah nol). Hal ini membuat penambangan blok baru menjadi mahal secara komputasi, karena biasanya membutuhkan banyak tebakan (dan *hashing* berikutnya) untuk menemukan nomor yang menghasilkan *hash* yang tepat. Di sisi lain, memastikan bahwa blok tertentu memang berhasil ditambang tetap murah secara komputasi (hanya membutuhkan satu *hashing*). Dari sisi algoritma konsensus, arsitektur Blockchain menyimpan salinan lokal setiap *node* dari Blockchain yang ditukar. Karena sifatnya yang terdistribusi, mungkin saja dua blok berbeda ditambahkan secara bersamaan, menghasilkan dua versi berbeda dari Blockchain yang tersedia di jaringan. Untuk mencapai konsensus tentang versi mana yang benar, arsitektur Blockchain biasanya dilengkapi dengan strategi bagaimana memilih versi yang tepat dari serangkaian blockchain yang bersaing. Aturan ini diterapkan oleh setiap node jaringan yang dapat dipercaya dan harus menjamin bahwa *node* sehingga pada akhirnya mencapai konsensus. Ada beberapa jenis strategi konsensus yang digunakan di dalam Bitcoin, seperti *proof-of-work* [3].

Dalam jaringan *proof-of-work*, setiap CPU mendapat satu suara dan keputusan mayoritas biasanya hanya dapat dimanipulasi jika satu entitas memiliki lebih dari 50% daya komputasi jaringan. Namun, hal ini mungkin tidak benar untuk blok yang baru saja ditambahkan ke dalam Blockchain. Satu *node* mungkin hanya beruntung dan menebak yang benar dengan cepat, tanpa menginvestasikan banyak daya komputasi. Untuk mengatasi tebakan keberuntungan seperti itu, diperlukan blok konfirmasi di dalam Bitcoin. Sebagai contoh, disarankan untuk menunggu setidaknya enam blok konfirmasi untuk menerima

transaksi sampai dengan selesai [3].

Selain Bitcoin, pada tahun 2020 diperkenalkan jenis lain dari *cryptocurrency* yaitu Polkadot. Polkadot adalah Blockchain dengan desain yang sepenuhnya terpecah berbasis teknik *a multi-chain (sharded)* pemisahan basis data yang memungkinkan beberapa rantai memproses transaksi secara paralel. Setiap pecahan Blockchain disebut *parachain* yang menghubungkan ke Rantai Relay. Rantai Relay secara efektif merupakan jantung dari Blockchain yang bertindak sebagai *hub* utama dari sistem. Selanjutnya, Polkadot berfungsi sebagai *platform* interoperabilitas yang memungkinkan komunikasi silang antara heterogen Blockchain termasuk yang eksternal, seperti Bitcoin dan Ethereum. Sementara *Relay Chain* mengatur dan memastikan berfungsi dapat berfungsi di seluruh jaringan secara benar. *Parachain* dapat disesuaikan sesuai kebutuhan, termasuk untuk meng-*host* kontrak cerdas dan kasus penggunaan lainnya. Pada dasarnya, Polkadot dikembangkan dengan tujuan untuk mengatasi beberapa kekurangan yang terdapat didalam teknologi Blockchain, yaitu, skalabilitas, interoperabilitas, dan mencapai jaminan keamanan standar diberbagai model kepercayaan [11].

Polkadot mengadopsi konsensus *Proof of Stake* (PoS) dengan variasi yang dikenal dengan istilah *Nominated Proof of Stake* (NPoS). Skema ini disebut sebagai dinominasikan karena *validator* (pengelola *Relay Chain* yaitu *node* bertanggung jawab untuk membuat dan memverifikasi blok baru) didukung oleh *nominator* yang mengunci DOT mata uang asli Polkadot sebagai jaminan dengan imbalan mempertaruhkan *reward*. Namun, jika *validator* berperilaku buruk, maka *nominator* yang sesuai juga dipotong (pengurangan DOT dari akun). Sementara *validator* yang memelihara *Relay Chain*, *collator* adalah *node* yang bertanggung jawab untuk memelihara *parachain* [11, 13]. Mekanisme konsensus yang diterapkan di dalam Polkadot adalah teknik hibrida yang menerapkan dua blok: produksi dan finalitas yang terisolasi secara proses. Algoritma yang bertanggung jawab untuk menangani produksi blok disebut *Blind Assignment for Blockchain Extension* (BABE) dan gadget terakhirnya adalah *GHOST-based Recursive ANcestor Deriving Pre-*




Gambar 4.4: Mekanisme konsensus Bitcoin [12]

*fix Agreement* (GRANDPA) yang memungkinkan satu set node untuk menyetujui rantai kanonik dari banyak kemungkinan garpu. Ini bekerja di bawah asumsi dari sistem Toleransi Patahan Bizantium: sebagian sinkron jaringan dengan paling banyak sepertiga node Bizantium (tidak jujur atau tidak responsif). Di satu sisi, implementasi produksi blok (BABE) dimaksudkan agar menjaga keamanan secara probabilistik (mampu terus-menerus menghasilkan blok baru dengan jaminan probabilitas bahwa blok yang dihasilkan akan diselesaikan setelah beberapa waktu) [11, 13].

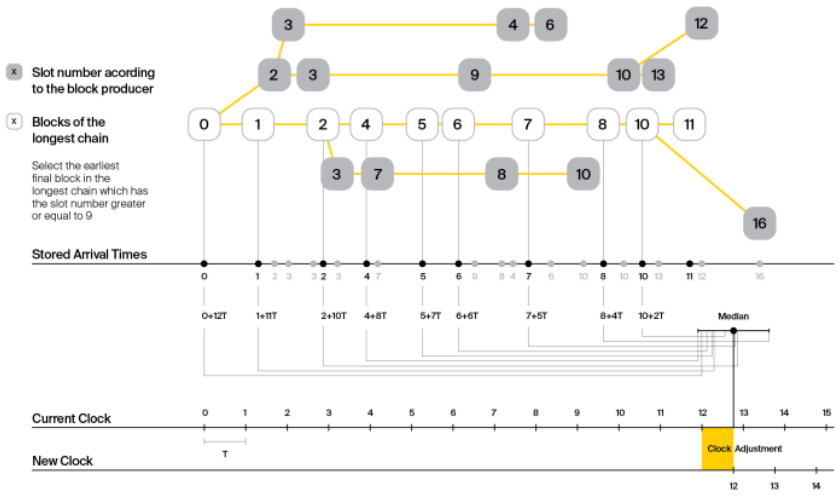
## 4.2 Diskusi

Pada sub bab ini dipaparkan ikhtisar tinjauan sistematis literatur serta pro dan kontra arsitektural BitCoin dan Polkadot dalam aspek interoperabilitas.

Dari uraian pembahasan sebelumnya, maka dapat dianalisis perbedaan teknik interoperabilitas yang digunakan pada Bitcoin dan Polkadot. Adapun parameter yang digunakan sebagai pembanding adalah algoritma konsensus, *ledger* dan *incentive*. Tabel 4.1 menunjukkan hasil komprasi dari dua *cryptocurrency* dalam aspek interoperabilitas.

Secara umum, Polkadot dan Bitcoin memiliki tujuan dan fungsi yang berbeda. Bitcoin fokus untuk menjadi jaringan terdesentralisasi secara global pertama yang dapat digunakan sebagai alat pembayaran inovatif. Di sisi lain, Polkadot mengambil peran untuk tumbuh sebagai *platform* multi-rantai yang memungkinkan interoperabilitas antara Blockchain dapat dilakukan. Contoh, sebagai sarana pertukaran token, data dan komunikasi.

Dari perspektif arsitektur teknologi, perbedaan utama dari Bitcoin dan Polkadot adalah dalam proses penambangan serta algoritma konsensus guna mendukung aspek intero-




Gambar 4.5: Mekanisme konsensus Polkadot [13]

Tabel 4.1: Tabel Komparasi Arsitektural cryptocurrency: Bitcoin dan Polkadot dari sisi interoperabilitas

| No | Parameter | Bitcoin | Polkadot |
|---|---|---|---|
| 1 | Tahun Rilis | 2009 | 2020 |
| 3 | *Founder* | Satoshi Nakamoto | Gavin Wood |
| 4 | Algoritma Konsensus | *Proof of Work (SHA-256)* | *Proof of Stake (PoS)/ Nominated Proof of Stake (NPoS).* |
| 5 | *Ledger* | *Blockchain* | *Blockchain shards called parachains* |
| 6 | *Incentive* | *MinedBlock* | *Shared Incentive* |
| 7 | *Fees* | *Per transaction* | *Per transaction* |

perabilitas. Bitcoin menggunakan *proof-of-work*, sementara Polkadot mengadopsi teknik *proof-of-stake* atau dikenal dengan istilah *Nominated proof-of-stake* yang menerapkan teknik hibrida yang dua blok: produksi dan finalitas yang terisolasi secara proses yaitu BABE dan GRANDPA. Meskipun kedua *cryptocurrency* ini menggunakan sistem *fees* yang sama yaitu *per transaction* namun pengelolaan *ledger* keduanya memiliki perbedaan. Bitcoin menerapkan teknik *Blockchain* sedangkan Polkadot menerapkan sistem *shards Blockchain* yang dikenal dengan istilah *parachains*. Dari pembagian insentif, Bitcoin menerapkan teknik *MinedBlock* sedangkan Polkadot menerapkan sistem *shared incentive*.

# Bab 5

# Kesimpulan

Diakhir pembahasan dapat disimpulkan dua poin penting dari hasil tinjauan sistematis literatur dari dua *cryptocurrency* yaitu Bitcoin dan Polkadot dalam dukungan aristektur terkait isu atau aspek interoperabilitas, yaitu sebagai berikut:

1. Metode SLR dalam penelusuran literatur untuk mengidentifikasi gap dalam sebuah area permasalahan tertentu cukup membantu kami dalam menuntun proses penelusuran literatur dalam penelitian kali ini. Jumlah keywords yang digunakan untuk mendapatkan literatur membantu mempertajam tujuan serta substansi penelitian.

   Dari hasil penelusuran literatur, meskipun secara umum penelitian dengan tema interoperabilitas blockchain atau cryptocurrency cukup banyak, namun ternyata tidak demikian halnya untuk tema interoperabilitas bitcoin dan polkadot. Bitcoin, yang merupakan salah satu dari sistem cryptocurrency yang sudah beredar cukup lama, belum mendapatkan perhatian yang signifikan dari sisi properti interoperabilitasnya jika dilihat dari hasil pencarian yang dilakukan. Hasil yang sama terjadi pada tema interoperabilitas polkadot. Ini barangkali merupakan gap yang nantinya bisa dijawab dengan melakukan penelitian primer selanjutnya.

2. *Cryptocurrency* Polkadot dan Bitcoin memiliki tujuan dan fungsi yang berbeda. Bitcoin fokus untuk menjadi jaringan terdesentralisasi secara global pertama yang dapat digunakan sebagai alat pembayaran inovatif. Di sisi lain, Polkadot mengambil peran untuk tumbuh sebagai *platform* multi-rantai yang memungkinkan interoperabilitas antara Blockchain dapat dilakukan secara *atomic*. Dari perspektif arsitektur teknologi, perbedaan utama dari Bitcoin dan Polkadot adalah dalam proses penambangan serta algoritma konsensus guna mendukung aspek interoperabilitas. Bitcoin menggunakan *proof-of-work*, sementara Polkadot mengadopsi teknik *proof-of-stake* atau dikenal dengan istilah *Nominated proof-of-stake* yang menerapkan teknik hibrida yang dua blok: produksi dan finalitas yang terisolasi secara proses yaitu BABE dan GRANDPA.

# Bibliografi


[1] T. Hardjono, A. Lipton, and A. Pentland, "Toward an interoperability architecture for blockchain autonomous systems," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1298–1309, 2020. 1

[2] Y. Pang, "A new consensus protocol for blockchain interoperability architecture," *IEEE Access*, vol. 8, pp. 153 719–153 730, 2020. 1, 2

[3] D. Marmsoler, "Towards Verified Blockchain Architectures: A Case Study on Interactive Architecture Verification," in *39th International Conference on Formal Techniques for Distributed Objects, Components, and Systems (FORTE)*, ser. Formal Techniques for Distributed Objects, Components, and Systems, J. A. Pérez and N. Yoshida, Eds., vol. LNCS-11535. Copenhagen, Denmark: Springer International Publishing, Jun. 2019, pp. 204–223, part 1: Full Papers. [Online]. Available: https://hal.inria.fr/hal-02313742 4, 19, 20

[4] A. A. Monrat, O. Schelen, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117 134–117 151, 2019. 5, 6, 7, 8, 9

[5] H. Hassani, X. Huang, and E. Silva, "Big-crypto: Big data, blockchain and cryptocurrency," *Big Data and Cognitive Computing*, vol. 2, pp. 34–, 10 2018. 10

[6] M. H. u. Rehman, K. Salah, E. Damiani, and D. Svetinovic, "Trust in blockchain cryptocurrency ecosystem," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1196–1212, 2020. 10, 11

[7] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *Journal of Systems and Software*, vol. 80, no. 4, pp. 571–583, 2007, software Performance. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S016412120600197X 12, 13, 14, 16

[8] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," University of Keele and University of Durham, UK, Tech. Rep. EBSE-2007-01, 2007. 13, 15

[9] C. Wohlin, P. Runeson, M. Höst, M. C. Ohlsson, B. Regnell, and A. Wesslén, *Experimentation in Software Engineering*. Springer, 2012. 13

[10] L. Herskind, P. Katsikouli, and N. Dragoni, "Privacy and cryptocurrencies – a systematic literature review," *IEEE Access*, vol. 8, pp. 54 044–54 059, 2020. 14, 16

[11] H. Abbas, M. Caprolu, and R. Di Pietro, "Analysis of polkadot: Architecture, internals, and contradictions," in *2022 IEEE International Conference on Blockchain (Blockchain)*, 2022. 20, 21

[12] H. Xiong, M. Chen, C. Wu, Y. Zhao, and W. Yi, "Research on progress of blockchain consensus algorithm: A review on recent progress of blockchain consensus algorithms," *Future Internet*, vol. 14, no. 2, 2022. [Online]. Available: https://www.mdpi.com/1999-5903/14/2/47 20

[13] J. Burdges, A. Cevallos, P. Czaban, R. Habermeier, S. Hosseini, F. Lama, H. K. Alper, X. Luo, F. Shirazi, A. Stewart, and G. Wood, "Overview of polkadot and its design considerations," *CoRR*, vol. abs/2005.13456, 2020. [Online]. Available: https://arxiv.org/abs/2005.13456 20, 21