BLOCKCHAIN: TEKNOLOGI DAN IMPLEMENTASINYA

Aprianti Nanda Sari [1], Trisna Gelar [2]
[1,2] Jurusan Teknik Komputer dan Informatika Politeknik Negeri Bandung
aprianti.nanda@polban.ac.id

ABSTRAK

Bitcoin merupakan mata uang digital atau yang lebih dikenal sebagai *cryptocurrency*. Bitcoin diciptakan pada tahun 2008 oleh Satoshi Nakamoto sebagai alat pembayaran elektronik secara *peer-to-peer*. Sebagai konsekuensinya, transaksi dengan menggunakan Bitcoin tidak memerlukan pihak ketiga seperti institusi keuangan atau pemerintah. Meskipun demikian, teknologi dibalik Bitcoin tidaklah baru. Pada dasarnya, Bitcoin menggunakan teknik-teknik dasar kriptografi dan jaringan komputer seperti fungsi *hash*, *blockchain*, jaringan komputer *peer-to-peer*, dan mekanisme konsensus. Sejak dibuatnya Bitcoin, aplikasi dari *blockchain* semakin meluas di berbagai bidang. Pada penelitian ini akan dibahas mengenai pengetahuan dasar mengenai *blockchain*. Selain itu, penelitian ini juga menganalisa implementasi *blockchain*, algoritma dasar yang digunakan, dan keterkaitannya dengan karakteristik *blockchain* di enam bidang berbeda yaitu ekonomi, kesehatan, pendidikan, pengarsipan dan kepemilikan, media, serta rantai pasok. Dari hasil analisis diketahui bahwa setiap bidang memiliki kebutuhan yang berbeda sehingga arsitektur *blockchain* yang dibangun juga berbeda.

Keyword : *Bitcoin, blockchain, fungsi hash, peer-to-peer, konsensus*

1. PENDAHULUAN

Popularitas *blockchain* semakin meningkat seiring implementasinya di bidang finansial yaitu Bitcoin. Berbeda dengan proses transaksi konvensional yang memerlukan pihak ketiga misalnya bank atau instansi pemerintahan, proses transaksi pada Bitcoin mengandalkan sistem buku besar terdesentralisasi (*decentralize ledger*) yang dikenal sebagai *blockchain* [1]. Pada dasarnya, *blockchain* merupakan kumpulan rekaman data yang terus terus bertambah dan didistribusikan serta dikonfirmasi oleh pihak-pihak yang berpartisipasi pada jaringan *blockchain* yang disebut dengan *node*. Dengan demikian, *blockchain* merupakan solusi dari transaksi konvensional dengan tidak bergantung pada pihak ketiga. Hal ini disebabkan karena sifat *blockchain* yang transparan dengan melakukan konfirmasi transaksi yang dilakukan oleh semua *node*.

Karena popularitasnya yang semakin meningkat, banyak peneliti yang menjadikan *blockchain* sebagai objek penelitian. Pada penelitian ini, akan dibahas mengenai teknologi yang mendasari *blockchain* seperti fungsi *hash*, penyimpanan terdistribusi, serta algoritma konsensus. Selain itu, pada penelitian ini juga membahas implementasi *blockchain* di berbagai bidang yaitu ekonomi, pendidikan, kesehatan, kearsipan, media, dan rantai pasok. Selain itu, pada penelitian ini juga menganalisa teknologi yang digunakan dan keterkaitannya dengan karakteristik *blockchain* di berbagai bidang tersebut.

Susunan dari artikel ilmiah ini adalah sebagai berikut. Bab 2 membahas tentang teori-teori yang mendasari tercetusnya *blockchain* yaitu fungsi *hash*, penyimpanan terdistribusi, algoritma konsensus, serta uraian singkat mengenai cara kerja *blockchain*. Bab 3 membahas mengenai metodologi penelitian. Bab 4 membahas tentang beberapa penerapan *blockchain* di enam bidang berbeda. Terakhir, pada Bab 5 memuat kesimpulan dan saran dari penelitian ini.

2. TINJAUAN PUSTAKA

Pada bagian ini akan dibahas mengenai teori-teori yang mendasari *blockchain* yaitu fungsi *hash*, jaringan *peer-to-peer*, serta algoritma konsensus.

2.1. Fungsi *Hash*

Fungsi *hash* disebut juga sebagai fungsi satu arah (*one-way function*) yang memetakan rangkaian bit (*bit string*) dengan panjang sembarang menjadi *bit string* dengan panjang tertentu. Fungsi *hash* memegang peranan penting di bidang kriptografi terutama dalam menjaga integritas data. Beberapa fungsi *hash* yang sering digunakan pada *blockchain* adalah MD5 dan SHA-256.

Sebagai contoh, sebuah pesan yaitu ”Temui aku jam 8”. Pesan tersebut diubah menjadi bit string yaitu 01010100011001010111011010111010101101 00100100000011000010110101101110101001000 00011010100110000101101101001000000000111 000. Kemudian *bit string* tersebut dipetakan oleh fungsi *hash* dengan panjang 128 bit. Sebagai contoh, fungsi *hash* yang digunakan adalah MD5 (detail cara kerja algoritma MD5 dapat anda lihat di [2]). Nilai *hash* yang dihasilkan adalah 100100010001001111 01011000000000001111010010101101101111001 11110000111010101000111000001100000001011 01000110101101010001000001 atau jika dikonversi menjadi hexadesimal adalah 9113D6003D2B6F3E1D51C180B46B5441.
Perhatikan bahwa jika pesan diganti satu karakter saja, misalnya menjadi ”Temui aku jam 7”, maka nilai hash yang dihasilkan juga akan sangat jauh berbeda yaitu 814A816955B987B61469493821

3EEB97. Sehingga, fungsi *hash* sering digunakan untuk mengidentifikasi perubahan pada pesan dengan tujuan untuk menjaga integritasnya.

SHA-256 merupakan fungsi *hash* yang paling banyak digunakan pada *blockchain*. Fungsi ini merupakan keluarga dari SHA-2 yang dikembangkan oleh NIST (*National Institute of Standard* and *Technology*)[3]. Pesan akan diubah menjadi biner, kemudian akan diberi tambahan bit '1' di akhir pesan sedemikian hingga panjang bit menjadi kelipatan 512. Setelah itu, bit pesan akan dibagi menjadi n blok dan dioperasikan dengan *initial hash value*. Untuk lebih detail mengenai cara kerja SHA-256, lihat [3].

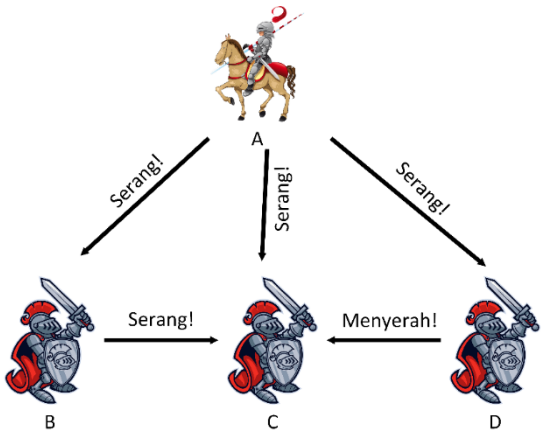
2.2. Jaringan *Peer-to-Peer*

Jaringan terdistribusi dapat disebut sebagai jaringan *Peer-to-Peer* (P2P) jika partisipan (*nodes*) pada jaringan tersebut dapat berbagi sumber daya seperti daya pemrosesan, penyimpanan, printer, dan lain sebagainya[4][5]. Selain itu, pada jaringan *Peer-to-Peer*, *nodes* juga dapat saling berbagi *file*.

2.3. Algoritma Konsensus

Algoritma konsensus atau persetujuan memungkinkan sekelompok mesin (komputer) untuk bekerja secara berkelompok dan terkoordinasi sedemikian hingga dapat bertahan walaupun ada sebagian anggota yang gagal [6]. Konsensus berawal dari *Byzantine Generals' Problem* yang diadaptasi sebagai solusi pada permasalahan sistem terdistribusi [7].

Misal, ada seorang jenderal dan prajurit yang sedang mengepung sebuah kastil. Jendral tersebut memerintahkan prajuritnya untuk menyerang atau menyerah. Kemudian, prajurit akan menyampaikan perintah dari jenderal ke prajurit lain yang berdekatan dengan mereka. Namun salah satu dari prajurit tersebut adalah pengkhianat yang selalu menyampaikan perintah yang bertentangan dengan perintah sebelumnya. Permasalahannya adalah mereka tidak tahu siapa penghianat tersebut. Sebagai ilustrasi, terdapat seorang jenderal A dan prajurit B, prajurit C, dan prajurit D. Jenderal A memerintahkan prajurit B, C, dan D untuk menyerang. Jenderal B dan D kemudian menyampaikan pesan tersebut ke jenderal yang berdekatan dengan mereka yaitu jenderal C. Sebagai contoh, pengkhianat di antara mereka adalah jenderal D, sehingga alih-alih memerintahkan untuk menyerang, ia memerintahkan jenderal C untuk menyerah. Ilustrasi kondisi ini dapat dilihat pada Gambar 1. Untuk memutuskan apakah menyerang atau menyerah, jenderal C mengambil perintah dengan suara terbanyak. Karena ada dua orang yang memerintahkan ia untuk menyerang dan hanya ada satu orang yang memerintahkan untuk menyerah, maka ia memutuskan untuk menyerang [7]. Mekanisme pengambilan keputusan inilah yang menjadi dasar dari algoritma konsensus.



Gambar 1. Ilustrasi *Byzantine's Generals Problem*

Dalam kaitannya dengan *blockchain*, ada tiga algoritma konsensus yang paling sering digunakan yaitu *Proof-of-Work*, *Proof-of-Stake*, dan *Proof-of-Authority*.

2.3.1. *Proof-of-Work*

Proof-of-Work (PoW) merupakan algoritma konsensus yang diterapkan di Bitcoin [1] . Ide dasarnya adalah dengan mengadakan kompetisi antar *node*. Kompetisi tersebut adalah menebak teka-teki matematika berdasarkan informasi dari blok sebelumnya. *Node* yang berhasil memecahkan teka-teki tersebut akan diberikan hadiah berupa Bitcoin.

2.3.2. *Proof-of-Stake*

Proof-of-Stake (PoS) merupakan solusi dari PoW yang memiliki komputasi dan konsumsi energi yang tinggi [8][9]. Pada konsensus PoS, *node* dipilih secara acak untuk dapat membuat blok baru pada *blockchain*.

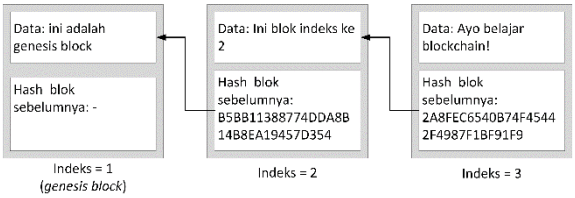
2.3.3. *Proof-of-Authority*

Proof-of-Authority (PoA) adalah algoritma konsensus yang sering digunakan pada *permissioned blockchain* (lihat bab 2.4 tentang jenis-jenis hak akses pada *blockchain*). Konsep PoA berdasar pada sebuah himpunan *N nodes* yang terpercaya yang disebut *authorities*. Setiap anggota *authorities* memiliki id yang unik dan dengan asumsi setidaknya $\frac{N}{2} + 1$ anggotanya jujur. Pada konsensus PoA, untuk dapat menambahkan blok pada *blockchain* (proses *mining*), setiap anggota *authorities* melakukannya secara bergantian [10].

2.4. *Blockchain*

Blockchain merupakan kumpulan blok (*block*) berisi data yang tersusun berurutan dan saling terhubung (*chain*) satu sama lain dengan menggunakan fungsi *hash* [11]. Secara umum sebuah blok terdiri dari data dan *hash* blok sebelumnya. Blok dengan indeks terkecil (indeks biasanya dimulai dari 1) disebut sebagai *genesis*

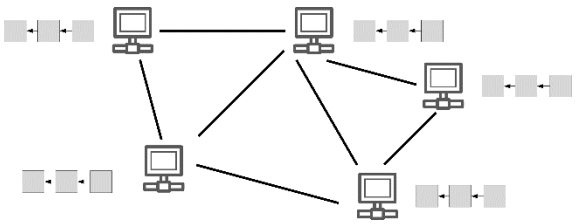
block. Pada *genesis block*, karena tidak ada blok sebelumnya maka hash dari *block* sebelumnya tidak diisi. Data pada *genesis block* kemudian diambil nilai hash-nya dan diisikan pada bagian hash blok sebelumnya untuk blok indeks ke-2. Begitu seterusnya hingga ilustrasi *blockhain* dapat dilihat pada Gambar 2



Gambar 2. Ilustrasi *blockchain*

Perhatikan bahwa jika ada pihak yang tidak bertanggung jawab yang berusaha mengganti data pada *genesis block*, maka nilai *hash genesis block* juga berubah. Akibatnya, hash blok sebelumnya pada blok di indeks ke-dua tidak lagi valid.

Selain diamankan dengan penggunaan fungsi *hash*, *blockchain* tersebut akan didistribusikan ke semua *node* yang terlibat pada jaringan seperti pada Gambar 3. Akibatnya, jika pihak yang tidak bertanggung jawab ingin mengganti sebuah blok pada blockchain, maka ia harus mengganti blok tersebut di semua *node*. Dengan demikian, hampir tidak mungkin untuk bisa memanipulasi data pada *blockchain*.



Gambar 3. Ilustrasi blockchain yang terdistribusi

Berdasarkan hak akses terhadap data, sistem *blockchain* terbagi menjadi empat [12] yaitu:

- *Unpermissioned*, atau biasa disebut *public blockchain* memungkinkan semua orang dapat menggunakan dan memelihara sistem *blockchain*. Contohnya adalah Bitcoin.
- *Permissioned public*, pada tipe *blockchain* ini semua orang dapat menggunakan sistem, namun hanya beberapa *node* terpercaya yang dapat memelihara sistem.
- *Permissioned private*, artinya hanya *node* terpercaya yang dapat menggunakan dan memelihara sistem *blockchain*.

Menurut Luca, et al., ada enam karakteristik utama dari *blockchain*, yaitu sebagai berikut [13]:

- *Decentralization*, artinya sistem *blockchain* dapat diakses dan dipelihara oleh semua *nodes* sehingga transaksi (pertukaran data) yang terjadi dapat divalidasi oleh semua pihak tanpa ada intervensi.
- *Immutability*, artinya data pada *blockchain* tidak dapat diubah karena setiap blok saling terhubung dengan blok sebelumnya. Dengan demikian, sedikit saja perubahan pada satu blok dapat mengakibatkan tidak validnya blok lain secara keseluruhan.
- *Traceability*, pengguna dapat melakukan verifikasi dan melihat riwayat data yang disimpan pada *blockchain*.
- *Non-repudiation*, transaksi yang sudah ditandatangani secara digital oleh seorang pengguna dan disimpan di *blockchain* tidak dapat disangkal. Hal ini dapat terjadi karena proses tanda tangan digital harus menggunakan kunci privat yang hanya diketahui dan dimiliki oleh pengguna tersebut.
- *Transparency*, setiap pengguna dapat mengakses dan berinteraksi dengan sistem *blockchain* sesuai dengan hak aksesnya.
- *Pseudonymity and anonymity*, sistem *blockchain* memiliki kemampuan untuk mempertahankan anonimitas pada tingkat tertentu.

3. METODE PENELITIAN

Tujuan dari penelitian ini adalah mengeksplorasi teknologi yang digunakan pada *blockchain* dan aplikasinya berdasarkan karya-karya yang diterbitkan pada jurnal akademik, prosiding konferensi, laporan teknis, dan lain sebagainya. Dari sumber-sumber tersebut, kemudian dikelompokkan berdasarkan bidang aplikasi. Setelah itu dianalisa teknologi yang mendasari aplikasi *blockchain* tersebut dan keterkaitannya dengan karakteristik *blockchain*.

4. HASIL DAN PEMBAHASAN

Pada bagian ini akan dijelaskan aplikasi *blockchain* di bidang ekonomi, kesehatan, pendidikan, pengarsipan dan kepemilikan, media, serta rantai pasok. Selain itu, pada bagian ini juga dijelaskan mengenai teknologi-teknologi yang digunakan pada aplikasi *blockchain* tersebut.

4.1. Ekonomi

Setelah Satoshi Nakamoto memperkenalkan Bitcoin, aplikasi *blockchain* di bidang ekonomi didominasi oleh penggunaan mata uang kripto (*cryptocurrency*). Transaksi pada Bitcoin memiliki tujuh tahap yang dijelaskan sebagai berikut.

Misal Alice dan Bob masing-masing memiliki *wallet* di Bitcoin. Alice membeli sebuah barang dari Bob dan ia ingin membayarnya dengan Bitcoin. Maka tahapan yang dilakukan adalah [14][1]:

- Pembuatan alamat. Bob sebagai penerima *cryptocurrency* secara acak akan membuat alamat pembayaran untuk Alice.
- Pengajuan pembayaran. Alice mengirimkan sejumlah Bitcoin kepada Bob berdasarkan

alamat yang ia terima dengan menggunakan perangkat lunak *wallet* yang ia miliki.

- Tanda tangan. Isi transaksi pembayaran kemudian diubah menjadi nilai *hash*. Alice kemudian menandatangani nilai *hash* transaksi tersebut secara digital dengan menggunakan kunci privat yang ia miliki. Tujuannya untuk menjaga integritas dan *non-repudiation* dari transaksi yang ia lakukan.
- Penyebaran dan validasi. Transaksi yang telah ditandatangani kemudian disebarkan melalui jaringan sehingga *nodes* dapat mengecek dan melakukan validasi terhadap transaksi tersebut dan menyebarkan transaksi ke *nodes* lain untuk melakukan hal yang sama.
- Menambahkan transaksi ke *blockchain*. Jika jumlah minimal *nodes* yang sudah melakukan pengecekan dan validasi terpenuhi, maka *miners* akan menambahkan transaksi tersebut pada blok baru.
- *Proof-of-Work*. Semua *miners* kemudian berlomba untuk menebak sebuah angka acak bernama *nonce* untuk menyelesaikan teka-teki nilai *hash*. Algoritma *Proof-of-Work* dapat dilihat sebagai berikut.

Algoritma proof-of-work
input: nilai hash dari blok sebelumnya *previous_hash*,
nilai hash dari block baru *mining_hash*,
nilai acak *nonce*,
target kerumitan *target*,
boolean *status*
output: nilai *nonce* yang lebih kecil dari *target*
prosedur:
nonce = 0
status = False
while *status* = False do
mining_hash = SHA256(*previous_hash*, *nonce*)
if *mining_hash*[0:*target*] = '0'**target* then
status = True
else
nonce = *nonce* + 1
end if
end while

- Konfirmasi. Setelah teka-teki dapat diselesaikan oleh seorang *miner*, maka ia berhak untuk menambahkan transaksi pada blok baru dan mendapatkan hadiah. Setelah itu, Alice akan mendapatkan konfirmasi bahwa transaksinya sudah berhasil.

Tahapan-tahapan tersebut kemudian diadaptasi pada cryptocurrency lain dengan penerapan fungsi *hash* dan algoritma konsensus yang berbeda. Pada Tabel 1 merupakan ringkasan jenis-jenis *cryptocurrency* beserta fungsi *hash* dan algoritma konsensus yang digunakan.

Tabel 1. Jenis-jenis *cryptocurrency*

Cryptocurrency	Fungsi Hash	Konsensus
Bitcoin [1]	SHA-256	PoW
Etherum [15]	SHA-256	PoS
Litecoin [16]	Scrypt	PoW
Dogecoin [16]	Scrypt	PoW
Cardano [16]	Tidak disebutkan	PoS
Solana [17]	SHA-256	Proof-of-History
TRON [16]	Tidak disebutkan	Tidak disebutkan
Toncoin [18]	SHA-256	Byzantine Fault Tolerant
Peercoin [19]	SHA-256	PoW dan PoS

4.2. Kesehatan

Di bidang kesehatan, *blockchain* digunakan untuk menyimpan informasi medis penting yang rawan dimanipulasi seperti rekam medis dan sertifikat vaksin. Ringkasan implementasi *blockchain* di bidang kesehatan dapat dilihat pada Tabel 2.

Tabel 2. Implementasi *blockchain* di bidang kesehatan

Penulis & Ringkasan	Fungsi *Hash*	Konsensus
Ahram, et al. [20]. Implementasi *blockchain* dapat digunakan sebagai media penyimpanan rekam medis. Aplikasi ini diberi nama HealthChain	Tidak disebutkan	Practical Byzantine Fault Tolerance (lihat [21])
Azaria, et al. [21]. Hampir sama dengan yang diaplikasikan pada Health Chain, Azaria dkk menawarkan aplikasi bernama MedRec yang memungkinkan pemangku kepentingan dapat menyimpan rekam medis pasien.	Tidak disebutkan	Proof-of-Work
Abid et al. [22]. Saat pandemi COVID-19 berlangsung, mobilitas masyarakat menjadi terbatas. Beberapa fasilitas umum seperti rumah sakit, bandara, terminal, dan lain sebagainya hanya dapat diakses oleh masyarakat yang sudah diberi vaksin COVID-19. Untuk mencegah pemalsuan sertifikat vaksin COVID-19, peneliti mengajukan aplikasi bernama Novi Chain yang berbasis *blockchain* yang merekam riwayat vaksin COVID-19.	Tidak disebutkan	Tidak disebutkan

4.3. Pendidikan

Sama seperti di bidang kesehatan, *blockchain* digunakan untuk menyimpan data penting dan riwayat aktivitas akademik baik siswa maupun dosen seperti pada Tabel 3.

Tabel 3. Implementasi *blockchain* di bidang pendidikan

Penulis & Ringkasan	Fungsi *Hash*	Konsensus
Han, et al. [23]. Pada penelitian tersebut, penulis menggunakan teknologi *blockchain* sebagai media untuk menyimpan ijazah. Sehingga untuk membuktikan kelulusan, seorang alumni tidak lagi menggunakan salinan ijazah pada saat mencari pekerjaan.	SHA-256	Dengan asumsi bahwa hanya pihak-pihak terpercaya yang hanya terlibat, sehingga data yang disimpan di *blockchain* memang valid
Farah, et al. [24]. Aplikasi *blockchain* digunakan untuk menyimpan riwayat aktivitas belajar siswa.	Tidak disebutkan	*Proof-of-Work*
Xidong [25]. Selain menjaga integritas data terkait aktivitas dan kelulusan siswa, *blockchain* juga dapat dimanfaatkan untuk merekam transaksi peminjaman buku di perpustakaan.	Tidak menggunakan hash	Tidak disebutkan
Yusup, et al. [26]. Sebagai syarat seorang dosen mendapatkan sertifikat profesional adalah dengan mengumpulkan portofolio. Pada tulisan ini, penulis merancang program *e-certificate* yang memungkinkan dosen dapat menyimpan aset-aset yang dibutuhkan untuk portfolio yang keamanannya terjamin.	SHA	Tidak disebutkan

4.4. Pengarsipan dan kepemilikan

Selain untuk menyimpan informasi kepemilikan agar tidak mudah dimanipulasi, *blockchain* juga dapat digunakan untuk mengarsipkan dokumen di pemerintahan sehingga mudah untuk diaudit seperti yang dirangkum pada Tabel 4.

Tabel 4. Implementasi blockchain di bidang pengarsipan dan kepemilikan

Penulis & Ringkasan	Fungsi *Hash*	Konsensus
Permatasari, et al. [27]. Implementasi *blockchain* pada penelitian tersebut berfokus pada sistem pengarsipan dokumen elektronik di Kota Cilegon. Pengguna dari sistem tersebut sebanyak 130 petugas arsip yang tersebar di 32 unit Kota Cilegon. Dengan teknologi *blockchain*, pengarsipan yang awalnya tersentralisasi menjadi terdesentralisasi. Selain keamanannya yang semakin terjamin, arsip yang terdesentralisasi memudahkan Badan Pemeriksa Keuangan melakukan audit terhadap dokumen di pemerintahan Kota Cilegon.	Tidak disebutkan	Tidak disebutkan
Pada karya ilmiah ini, Galiev dan kawan-kawan [28] mengusulkan metode baru untuk menyimpan dokumen pada pemerintah Republic of Tatarstan (Russia). Terdapat tiga aktor pengguna yang terlibat yaitu *Administrator*, *Participant*, dan *Expert*. Administrator adalah juru arsip yang bertugas menandatangani arsip secara digital ketika informasi arsip akan disimpan di *blockchain*. *Expert* adalah seseorang yang ditunjuk oleh *Administrator* untuk mengecek arsip yang masuk. Sedangkan *Participant* adalah pihak atau unit atau organisasi pada pemerintahan yang menandatangani arsip secara digital Ketika sudah disetujui oleh *Expert*.	GOST R (lihat [29])	Tidak menggunakan algoritma konsensus dengan asumsi system *blockchain* yang digunakan adalah *permissioned blockchain*
Krishnapriya, et al. [30]. Untuk menjaga keamanan data kepemilikan lahan, penulis menawarkan solusi berbasis *blockchain* yang memungkinkan pengguna untuk bertransaksi jual beli lahan. Selain itu, penggunaan *blockchain* juga mengurangi kemungkinan *double spending* lahan. Artinya lahan yang sama tidak dapat diperjualbelikan berkali-kali dalam waktu yang bersamaan.	SHA-256	*Proof-of-Work*

4.5. Media

Kebenaran dari sebuah berita juga dapat dilacak melalui *blockchain* dengan memanfaatkan aspek *anonymity* pada *blockchain* seperti yang tersaji pada Tabel 5.

Tabel 5. Implementasi *blockchain* di bidang media

Penulis & Ringkasan	Fungsi *Hash*	Konsensus
Chen, et al. [31]. Dengan masifnya teknologi informasi, kebenaran dari sebuah berita yang beredar di komunitas sosial menjadi masalah serius. Dengan teknologi *blockchain*, penulis menawarkan solusi untuk pencegahan meluasnya berita palsu. Berita yang akan diterbitkan atau disiarkan, akan divalidasi kebenarannya oleh *validator nodes*. Untuk dapat menjadi *validator nodes*, organisasi media seperti CNN dipilih berdasarkan skor kredibilitasnya.	Tidak disebutkan	*Proof-of-Authority*
Berbeda dengan penelitian yang dilakukan Chen, et al [31] yang berfokus pada pencegahan meluasnya berita palsu, penelitian yang dilakukan Paul, et al [32] lebih mengutamakan pendeteksian berita palsu yang beredar di media sosial. Caranya, dengan memanfaatkan aspek anonim pada pengguna sosial media yang terlibat sebagai *validator*. Berita yang masuk (berdasarkan kriteria viralitas tertentu) kemudian akan dibagikan kepada semua *validator*. Setelah *validator* memberikan ulasan terhadap berita tersebut, maka berita sekaligus *rating*-nya disimpan dan di *blockchain*.	Tidak disebutkan	Tidak disebutkan

4.6. Rantai pasok

Masalah transparansi dan ketertelusuran menjadi hal yang sangat penting di bidang rantai pasok. Konsumen ingin mengetahui di mana bahan-bahan produk yang mereka konsumsi dibeli dan diproses, serta siapa saja yang terlibat. Pada Tabel 6 memuat beberapa contoh aplikasi *blockchain* di bidang rantai pasok.

Tabel 6. Implementasi *blockchain* di bidang rantai pasok

Penulis & Ringkasan	Fungsi *Hash*	Konsensus
Cao, et al. [33]. Pada artikel ilmiah ini, penulis memberikan solusi untuk transparansi di bidang rantai pasok industri daging sapi di Australia. Setiap hewan ternak dicatat keberadaannya mulai dari peternakan, tempat penggemukan, tempat penyembelihan, tempat pemotongan, hingga layanan makanan.	Tidak disebutkan	*Proof-of-Authority*
Yanovich, et al. [34]. Maraknya pemalsuan perangko di Rusia, membuat penulis menawarkan solusi berbasis *blockchain*. *Client* membeli perangko dari Kantor Pos secara *offline*. Di saat yang bersamaan, Kantor Pos memberikan *token* kepada *client* melalui *blockchain*. Saat *client* ingin mengirim surat ke *client* lain, ia harus mengirimkan sejumlah *token* seharga perangko yang berlaku. Jika surat sudah diterima, maka *token* tersebut akan hangus.	Tidak disebutkan	Tidak disebutkan
Bubba Cook [35]. Dampak *blockchain* juga terasa di bidang rantai pasok hidangan laut. Untuk memberantas produksi hidangan laut yang ilegal dan tidak etis. Hidangan laut seperti ikan tuna yang didapat dari laut kemudian diberi tag dan sensor RFID. Setiap proses dan pihak-pihak yang terlibat pada pemrosesan ikan tuna akan dicatat di *blockchain*. Daging ikan tuna dipasarkan akan dilengkapi QR Code berisi tautan untuk memungkinkan pembeli dapat mengecek riwayat pemrosesan daging ikan tuna yang mereka konsumsi.	Tidak disebutkan	Tidak disebutkan

5. KESIMPULAN DAN SARAN

Pada studi ini telah dilakukan analisis terhadap aplikasi *blockchain* beserta teknologi yang mendasarinya. Dari hasil analisa ditemukan bahwa karakteristik *blockchain* dapat berbeda dan bergantung pada kebutuhan di setiap bidang. Di bidang ekonomi, *blockchain* menjadi dasar mata uang kriptografi yang mementingkan semua karakteristik *blockchain*. Berbeda halnya di bidang kesehatan, pendidikan, pengarsipan dan kepemilikan yang lebih mementingkan *immutability*, *traceability*, dan *transparency*. Sehingga *blockchain* digunakan untuk menyimpan data penting dan sensitif seperti sertifikat, ijazah, rekam medis, dan bukti kegiatan jual beli. Di bidang media, karakteristik *blockchain* yang dominan adalah *anonymity*. Pengguna dapat memberikan rating secara anonim pada berita-berita yang tersebar tanpa intervensi dari siapapun. Sedangkan di bidang rantai pasok, *blockchain* berguna untuk *traceability* sebuah produk. Konsumen dapat mengetahui bahan-bahan, proses produksi, dan pihak-pihak yang terlibat sehingga dapat meningkatkan kepercayaan konsumen terhadap produk yang dikonsumsi.

DAFTAR PUSTAKA

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Bus. Rev.*, p. 21260, 2008.

[2] R. Rivest, "The MD5 message-digest algorithm," 1992.

[3] NIST, "FIPS 180-4 Secure Hash Standard (SHS)," *Gaithersburg, Montgomery County, Maryl. Natl. Inst. Stand. Technol. doi http//dx. doi. org/10.6028/NIST. FIPS*, pp. 180–184, 2015.

[4] W. Kellerer, "Dienstarchitekturen in der

Telekommunikation-Evolution, methoden und vergleich," *Tech. Rep. TUM-LKN-TR-9801. 1998*, 1998.

[5] R. Schollmeier, "A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications," *Proc. - 1st Int. Conf. Peer-to-Peer Comput. P2P 2001*, no. September, pp. 101–102, 2001, doi: 10.1109/P2P.2001.990434.

[6] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," in *2014 {USENIX} Annual Technical Conference ({USENIX}{ATC} 14)*, 2014, pp. 305–319.

[7] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, 1982, doi: 10.1145/357172.357176.

[8] W. Kin Chan, R. Zhang, and W. K. Chan, "Evaluation of Energy Consumption in Block-Chains with Proof of Work and Proof of Stake," *J. Phys. Conf. Ser.*, vol. 1584, no. 1, 2020, doi: 10.1088/1742-6596/1584/1/012023.

[9] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," *self-published Pap. August*, vol. 19, no. 1, 2012.

[10] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain," *CEUR Workshop Proc.*, vol. 2058, pp. 1–11, 2018.

[11] A. Bahga and V. K. Madisetti, "Blockchain Platform for Industrial Internet of Things," *J. Softw. Eng. Appl.*, vol. 09, no. 10, pp. 533–546, 2016, doi: 10.4236/jsea.2016.910036.

[12] H. Okada, S. Yamasaki, and V. Bracamonte, "Proposed classification of blockchains based on authority and incentive dimensions," *Int. Conf. Adv. Commun. Technol. ICACT*, pp. 593–597, 2017, doi: 10.23919/ICACT.2017.7890159.

[13] L. Turchet and C. N. Ngo, "Blockchain-based Internet of Musical Things," *Blockchain Res. Appl.*, vol. 3, no. 3, p. 100083, 2022, doi: 10.1016/j.bcra.2022.100083.

[14] C. Brennan and W. Lunn, "Blockchain: the trust disrupter," *Credit Suisse Secur. Ltd. London, UK*, 2016.

[15] V. Buterin, "A next-generation smart contract and decentralized application platform," *white Pap.*, vol. 3, no. 37, pp. 1–2, 2014.

[16] Anonymous, "Today's Cryptocurrency Prices by Market Cap." https://coinmarketcap.com/ (accessed Jun. 30, 2023).

[17] A. Yakovenko, *Solana : A new architecture for a high*. 2019.

[18] N. Durov, "The Open Network," pp. 1–126, 2021, [Online]. Available: https://ton.org/whitepaper.pdf.

[19] S. King and S. Nadal, "Peercoin–secure & sustainable cryptocoin," *Aug-2012 [Online]. Available: https://peercoin. net/whitepaper ()*, 2012.

[20] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, "Blockchain Technology Innovations," *2017 IEEE Technol. Eng. Manag. Soc. Conf. TEMSCON 2017*, no. 2016, pp. 137–141, 2017.

[21] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," *Proc. - 2016 2nd Int. Conf. Open Big Data, OBD 2016*, pp. 25–30, 2016, doi: 10.1109/OBD.2016.11.

[22] A. Abid, S. Cheikhrouhou, S. Kallel, and M. Jmaiel, "NovidChain: Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates," *Softw. - Pract. Exp.*, vol. 52, no. 4, pp. 841–867, 2022, doi: 10.1002/spe.2983.

[23] M. Han, D. Wu, Z. Li, Y. Xie, J. S. He, and A. Baba, "A novel blockchain-based education records verification solution," *SIGITE 2018 - Proc. 19th Annu. SIG Conf. Inf. Technol. Educ.*, no. September, pp. 178–183, 2018, doi: 10.1145/3241815.3241870.

[24] J. C. Farah, A. Vozniuk, M. J. Rodriguez-Triana, and D. Gillet, "A blueprint for a blockchain-based architecture to power a distributed network of tamper-evident learning trace repositories," *Proc. - IEEE 18th Int. Conf. Adv. Learn. Technol. ICALT 2018*, pp. 218–222, 2018, doi: 10.1109/ICALT.2018.00059.

[25] X. Liu, "A smart book management system based on Blockchain platform," in *2019 International Conference on Communications, Information System and Computer Engineering (CISCE)*, 2019, pp. 120–123.

[26] M. Yusup, Q. Aini, D. Apriani, and P. Nursaputri, "Pemanfaatan Teknologi Blockchain Pada Program Sertifikasi Dosen," *SENSITIf Semin. Nas. Sist. Inf. dan Teknol. Inf.*, pp. 365–371, 2019.

[27] I. Permatasari, M. Essaid, H. Kim, and H. Ju, "Blockchain implementation to verify archives integrity on cilegon E-archive," *Appl. Sci.*, vol. 10, no. 7, 2020, doi: 10.3390/app10072621.

[28] A. Galiev, N. Prokopyev, S. Ishmukhametov, E. Stolov, R. Latypov, and I. Vlasov, "Archain: A Novel Blockchain Based Archival System," *Proc. 2nd World Conf. Smart Trends Syst. Secur. Sustain. WorldS4 2018*, pp. 308–312, 2019, doi: 10.1109/WorldS4.2018.8611607.

[29] V. Dolmatov and A. Degtyarev, "GOST R 34.11-2012: hash function," 2013.

[30] S. Krishnapriya and G. Sarath, "Securing Land Registration using Blockchain," *Procedia Comput. Sci.*, vol. 171, no. 2019, pp. 1708–1715, 2020, doi: 10.1016/j.procs.2020.04.183.

[31] Q. Chen, G. Srivastava, R. M. Parizi, M.

Aloqaily, and I. Al Ridhawi, "An incentive-aware blockchain-based solution for internet of fake media things," *Inf. Process. Manag.*, vol. 57, no. 6, p. 102370, 2020, doi: 10.1016/j.ipm.2020.102370.

[32] S. Paul, J. I. Joy, S. Sarker, S. Ahmed, and A. K. Das, "Fake news detection in social media using blockchain," in *2019 7th International Conference on Smart Computing & Communications (ICSCC)*, 2019, pp. 1–5.

[33] S. Cao, M. Foth, W. Powell, T. Miller, and M. Li, "A blockchain-based multisignature approach for supply chain governance: A use case from the Australian beef industry," *Blockchain Res. Appl.*, vol. 3, no. 4, p. 100091, 2022, doi: 10.1016/j.bcra.2022.100091.

[34] Y. Yanovich, I. Shiyanov, T. Myaldzin, I. Prokhorov, D. Korepanova, and S. Vorobyov, "Blockchain-based supply chain for postage stamps," *Informatics*, vol. 5, no. 4, pp. 1–9, 2018, doi: 10.3390/informatics5040042.

[35] B. Cook and W. N. Zealand, "Blockchain: Transforming the seafood supply chain," *World Wide Fund Nat.*, 2018.