

## PENGARUH TEKNOLOGI BLOCKCHAIN TERHADAP TRANSFORMASI SISTEM PEMBAYARAN DIGITAL: TANTANGAN KEAMANAN DAN REGULASI

Kelvin<sup>1</sup>, Richard Raymond<sup>2</sup>, Fahrur Rozzi Nasution<sup>3</sup>, Andrew Law<sup>4</sup>, Philisya Salim<sup>5</sup>,  
Christin Christovany<sup>6</sup>

[211121305@students.mikroskil.ac.id](mailto:211121305@students.mikroskil.ac.id)<sup>1</sup>, [211120103@students.mikroskil.ac.id](mailto:211120103@students.mikroskil.ac.id)<sup>2</sup>,  
[211121363@students.mikroskil.ac.id](mailto:211121363@students.mikroskil.ac.id)<sup>3</sup>, [211121350@students.mikroskil.ac.id](mailto:211121350@students.mikroskil.ac.id)<sup>4</sup>,  
[211120486@students.mikroskil.ac.id](mailto:211120486@students.mikroskil.ac.id)<sup>5</sup>, [211120174@students.mikroskil.ac.id](mailto:211120174@students.mikroskil.ac.id)<sup>6</sup>

\*Corresponding Author: Joosten

[joosten.ng@mikroskil.ac.id](mailto:joosten.ng@mikroskil.ac.id)

Universitas Mikroskil

### ABSTRAK

Teknologi blockchain, dengan karakteristiknya yang terdesentralisasi, transparan, dan tahan terhadap perubahan, telah muncul sebagai solusi yang menjanjikan untuk mengatasi berbagai tantangan dalam sistem pembayaran tradisional. Mekanisme konsensus seperti proof of work (pow) atau proof of stake (pos) memastikan integritas data dan mencegah terjadinya double-spending. Kriptografi yang kuat digunakan untuk mengamankan transaksi dan melindungi identitas pengguna. Namun, implementasi blockchain dalam sistem pembayaran juga menghadapi sejumlah tantangan, seperti skalabilitas, konsumsi energi, dan regulasi. Selain itu, meskipun blockchain menawarkan tingkat privasi yang lebih tinggi dibandingkan sistem terpusat, masih terdapat kekhawatiran terkait dengan pelacakan alamat dan analisis on-chain.

**Kata Kunci:** Cryptocurrency, Desentralisasi, Keamanan Data, Kriptografi, Privasi, Sistem Pembayaran, Teknologi Blockchain, Transaksi, Keuangan.

### ABSTRACT

*Blockchain technology, with its decentralized, transparent and change-resistant characteristics, has emerged as a promising solution to overcome various challenges in traditional payment systems. Consensus mechanisms such as proof of work (pow) or proof of stake (pos) ensure data integrity and prevent double-spending. Strong cryptography is used to secure transactions and protect user identity. However, blockchain implementation in payment systems also faces a number of challenges, such as scalability, energy consumption, and regulation. Additionally, although blockchain offers a higher level of privacy than centralized systems, there are still concerns regarding address tracking and on-chain analysis.*

**Keywords:** Cryptocurrency, Decentralization, Data Security, Cryptography, Privacy, Payment Systems, Blockchain Technology, Transactions, Finance.

## PENDAHULUAN

Revolusi digital telah membawa transformasi signifikan dalam berbagai sektor, termasuk industri keuangan. Salah satu inovasi paling menonjol adalah teknologi blockchain, yang menawarkan paradigma baru dalam pengelolaan data dan transaksi. Menurut laporan grand view research, pasar global blockchain diproyeksikan mencapai usd 1,431.54 miliar pada tahun 2030, dengan tingkat pertumbuhan tahunan gabungan (cagr) sebesar 87.7% dari 2023 hingga 2030 [1], [2]. Konsep blockchain yang terdesentralisasi, transparan, dan tahan tamper telah menarik minat yang besar, terutama dalam konteks sistem pembayaran berbasis kriptografi.

Teknologi blockchain memiliki potensi besar untuk meningkatkan keamanan dan privasi dalam transaksi keuangan. Dengan menggunakan kriptografi yang kuat dan mekanisme konsensus yang terdistribusi, blockchain dapat meminimalkan risiko penipuan, mengurangi biaya intermediasi, serta melindungi data pengguna dari akses yang tidak sah. Studi yang dilakukan oleh deloitte menunjukkan bahwa implementasi blockchain dapat mengurangi biaya infrastruktur perbankan sebesar 30% dan meningkatkan kecepatan verifikasi transaksi hingga 100 kali lipat. [3], [4] beberapa kasus implementasi sukses telah ditunjukkan oleh jp morgan dengan platform onyx-nya yang telah memproses transaksi senilai lebih dari usd 300 miliar [5].

Namun, implementasi blockchain dalam sistem pembayaran juga menghadirkan tantangan unik. Jenis blockchain yang berbeda, seperti public blockchain dan private blockchain, memiliki karakteristik keamanan dan privasi yang berbeda pula. Algoritma konsensus yang digunakan, seperti proof of work (pow) dan proof of stake (pos), juga memiliki implikasi yang signifikan terhadap kinerja dan keamanan sistem. [4]. Selain itu, isu-isu terkait skalabilitas, interoperabilitas, dan regulasi masih perlu diatasi untuk memastikan adopsi blockchain yang lebih luas [5].

Penelitian ini bertujuan untuk menganalisis secara mendalam pengaruh teknologi blockchain terhadap keamanan dan privasi pada sistem pembayaran berbasis kriptografi. Fokus utama penelitian ini adalah pada:

- a. Jenis-jenis blockchain: membandingkan keamanan dan privasi yang ditawarkan oleh public blockchain, private blockchain, dan hybrid blockchain dalam konteks sistem pembayaran [6].
- b. Algoritma konsensus: menganalisis dampak berbagai algoritma konsensus, termasuk pow, pos, dan algoritma konsensus lainnya, terhadap keamanan dan efisiensi transaksi [6], [7].
- c. Mekanisme privasi: mengevaluasi penerapan teknik-teknik privasi seperti zero-knowledge proofs dan homomorphic encryption dalam meningkatkan kerahasiaan data pengguna. [6], [8].
- d. Kasus penggunaan: menjelajahi berbagai kasus penggunaan blockchain dalam sistem pembayaran, seperti pembayaran lintas batas, micropayments, dan pembayaran dalam rantai pasok [7].
- e. Dampak terhadap industri keuangan: menganalisis potensi perubahan pada peran lembaga keuangan, intermediasi, dan inklusi keuangan sebagai akibat dari adopsi blockchain [6], [7].

Dengan memahami secara komprehensif aspek-aspek di atas, penelitian ini diharapkan dapat memberikan kontribusi yang berharga bagi pengembangan sistem pembayaran yang lebih aman, efisien, dan inklusif. Penelitian ini menggunakan pendekatan kualitatif dengan dua metode utama, yaitu analisis literatur dan studi kasus, untuk mendapatkan pemahaman mendalam tentang pengaruh teknologi blockchain terhadap keamanan dan privasi dalam sistem pembayaran. Analisis literatur dilakukan

dengan mengumpulkan dan mengkaji berbagai sumber akademis dan laporan industri yang relevan mengenai teknologi blockchain, keamanan data, privasi, dan implementasi sistem pembayaran. Dimana chain, dan hybrid blockchain dalam konteks sistem pembayaran, menganalisis dampak berbagai algoritma konsensus, termasuk pow, pos, dan algoritma konsensus lainnya, terhadap keamanan dan efisiensi transaksi, serta mengevaluasi penerapan teknik-teknik privasi seperti zero-knowledge proofs dan homomorphic encryption dalam meningkatkan kerahasiaan data pengguna. Studi kasus diterapkan untuk menganalisis implementasi blockchain dalam sistem pembayaran di dunia nyata. Beberapa kasus yang dipilih mencakup aplikasi blockchain dalam pembayaran lintas batas, micropayments, dan sistem pembayaran dalam rantai pasok. Serta menganalisis potensi perubahan pada peran lembaga keuangan, intermediasi, dan inklusi keuangan sebagai akibat dari adopsi blockchain. Data dari studi kasus akan dianalisis secara deskriptif untuk memahami bagaimana blockchain diterapkan dan bagaimana teknologi ini memengaruhi keamanan dan privasi pengguna dalam sistem pembayaran. Dengan menggunakan kedua metode ini, penelitian diharapkan dapat memberikan pandangan komprehensif tentang manfaat dan tantangan implementasi blockchain dalam sistem pembayaran serta dampaknya terhadap keamanan dan privasi transaksi.

Dengan semakin populernya pasar kripto, banyaknya mata uang kripto yang tidak diatur (beberapa ratus), perhatian yang lebih besar sekarang diberikan oleh pemerintah dan pemangku kepentingan lainnya keliling dunia. Ilustrasinya adalah bahwa total kapitalisasi pasar dari 100 cryptocurrency terbesar dilaporkan melebihi setara dengan eur 330 miliar secara global pada awal 2018. Total pasar kapitalisasi semua mata uang kripto bersama-sama pada periode itu memuncak pada usd 728 yang lebih tinggi miliar, turun hanya tiga minggu kemudian menjadi sekitar usd 360 miliar.<sup>2</sup> regulator sedang melihat apakah — dan bagaimana — mengatur cryptocurrency. Sampai saat ini tidak ada pandangan yang jelas tentang bagaimana caranya lakukan itu. Bagaimanapun, ada alasan kuat mengapa cryptocurrency harus berada di bawah pengawasan yang lebih ketat oleh regulator dan pengawas. Ancaman volatilitas harga, perdagangan spekulatif, serangan peretasan, pencucian uang dan pendanaan teroris semuanya menyerukan regulasi yang lebih ketat.[9].

Penelitian ini menyelami masalah terakhir secara mendalam. Menurut banyak orang, selain dari ketidakstabilan harga cryptocurrency, cryptocurrency ini harus memiliki pengawasan peraturan yang lebih besar untuk mencegah aktivitas ilegal dan penggunaan yang tidak sah. Selain ketidakstabilan harga cryptocurrency, regulator mengkhawatirkan penjahat yang semakin banyak menggunakan cryptocurrency untuk kegiatan (berdagang jauh dari saluran resmi) seperti penipuan dan manipulasi, penghindaran pajak, peretasan, uang pencucian dan pendanaan untuk kegiatan teroris. Masalahnya adalah masalah yang signifikan: meskipun skala penyalahgunaan mata uang virtual tidak diketahui, nilai pasarnya telah dilaporkan melebihi eur 7 miliar di seluruh dunia [10].

## **METODE PENELITIAN**

Penelitian ini menggunakan pendekatan kualitatif dengan dua metode utama:

### **1. Analisis literatur**

Penelitian ini dikumpulkan dan dipelajari dengan penelitian akademik, laporan industri, dan artikel tentang teknologi blockchain, keamanan data, privasi, dan penerapan sistem pembayaran berbasis kriptografi. Analisis literatur mencakup perbandingan antara keamanan dan privasi yang ditawarkan oleh public blockchain, private blockchain, dan hybrid blockchain, serta evaluasi pengaruh berbagai algoritma konsensus, seperti proof of work (pow) dan proof of stake (pos), terhadap keamanan dan efisiensi transaksi. Analisis

juga membahas teknik privasi seperti bukti kurang pengetahuan dan enkripsi homomorfik yang dapat mempertahankan privasi data pengguna.

## **2. Studi kasus**

Selain itu, penelitian ini menyelidiki penerapan blockchain dalam sistem pembayaran nyata, dengan penekanan pada penggunaan blockchain dalam micropayments, pembayaran lintas batas, dan sistem pembayaran rantai pasok. Tujuan dari studi kasus ini adalah untuk memahami bagaimana blockchain diterapkan dalam sistem pembayaran dan bagaimana teknologi tersebut berdampak pada keamanan dan privasi pengguna.

Metode ini diharapkan dapat memberikan pemahaman yang komprehensif tentang bagaimana teknologi blockchain mempengaruhi keamanan dan privasi sistem pembayaran berbasis kriptografi, serta peluang dan masalah yang muncul dari penerapan teknologi tersebut di industri keuangan.

Pertama, penelitian ini terbatas pada cryptocurrency dan blockchain. Artinya, jenis aset lainnya daripada cryptocurrency, seperti token atau sekuritas kripto, tidak termasuk dalam lingkup penelitian ini. Kami akan menjelaskan bagaimana aset ini berbeda dari cryptocurrency lebih lanjut. Kami juga tidak akan menguraikan derivatif cryptocurrency, yang pada dasarnya adalah instrumen investasi. Blockchain akan menjadi diteliti sejauh cryptocurrency berjalan pada teknologi ini. Oleh karena itu, teknologi blockchain tidak akan dilihat di luar konteks cryptocurrency, seperti digunakan sebagai teknik untuk menghilangkan perantara di sektor keuangan, publik atau lainnya. Ini akan mengarah jauh dan melebihi ruang lingkup penelitian ini. Kedua, penelitian ini berkaitan dengan konteks hukum cryptocurrency dan blockchain. Fokusnya adalah, karenanya, yang legal. Ini berarti bahwa kami tidak akan menguraikan semua aspek teknis – dan ada banyak – yang berkaitan dengan cryptocurrency dan blockchain. Kami hanya akan menyinggung mereka sejauh ini diperlukan untuk memahami konteks hukum. Kami juga tidak akan mengambil ekonomi, kriminologis atau apa pun pendekatan lain selain pendekatan hukum. Kami fokus pada konteks hukum UE. Oleh karena itu, kami tidak akan menguraikan pada konteks internasional atau nasional, kecuali relevan untuk lebih memahami Eropa konteks. Ketiga, konteks hukum dibahas sehubungan dengan implikasi kejahatan keuangan, uang pencucian dan penghindaran pajak. Oleh karena itu, kami hanya akan meneliti konteks hukum cryptocurrency dan blockchain sejauh yang relevan sehubungan dengan kejahatan keuangan, pencucian uang, dan pajak penghindaran. Kami akan melakukan ini dengan menilai apa sebenarnya cryptocurrency dan blockchain itu, yang tantangan yang mereka bawa dari perspektif memerangi kejahatan keuangan, pencucian uang, dan pajak penghindaran, sejauh mana mereka tertangkap oleh undang-undang di tingkat Eropa dan apa yang bisa dilakukan meningkatkan kerangka hukum [12]. Kami tidak akan menyelami lebih dalam pertanyaan hukum lain selain yang terkait dengan pencucian uang, pendanaan teroris, dan penghindaran pajak, seperti kualifikasi cryptocurrency di bawah undang-undang perpajakan atau perlindungan investor dalam cryptocurrency (baik konsumen atau tidak) di bawah undang-undang jasa keuangan. Meski sangat menarik, pertanyaan-pertanyaan ini melampaui ruang lingkup penelitian ini. Terakhir, penelitian ini berkaitan dengan kejahatan keuangan, pencucian uang, dan penggelapan pajak. Kejahatan keuangan tidak ada istilah seni. Secara umum, ini digunakan sebagai istilah umum untuk menunjuk semua jenis kejahatan yang berkaitan penggunaan keuangan, seperti penipuan, pencurian, penghindaran pajak, penyusutan, pencucian uang, pendanaan teroris, dll. Dalam konteks UE, kejahatan keuangan antara lain termasuk kejahatan terhadap integritas keuangan sektor, seperti pencucian uang dan transaksi orang dalam, dan kejahatan terhadap kepentingan finansial serikat pekerja, seperti penipuan. Dalam penelitian ini kami tidak akan menguraikan semua kejahatan keuangan yang bisa dibayangkan. Pada sebaliknya,

kami akan fokus pada pencucian uang, pendanaan teroris, dan penghindaran pajak sebagai subtype dari kejahatan keuangan. Fokus ini dapat dibenarkan karena sejumlah alasan. Pertama, pencucian uang, teroris pembiayaan dan penghindaran pajak berada di garis depan upaya uni eropa dalam memerangi kejahatan keuangan. Selain itu, ue jelas mengambil pendekatan untuk mengatasi masalah cryptocurrency melalui anti-uang undang-undang pencucian dan penanggulangan pendanaan terorisme. Penelitian ini mengakui pendekatan itu dan mengambil yang sama. Kedua, mengesampingkan pencurian, pencucian uang, pendanaan teroris dan pajak penghindaran mungkin adalah tiga jenis kejahatan keuangan yang kemungkinan paling terkait dengan cryptocurrency dan blockchain, yaitu ketika orang melakukan kejahatan yang berkaitan dengan cryptocurrency dan blockchain, kemungkinan kejahatan itu adalah pencucian uang, pendanaan teroris dan/atau pajak penghindaran tinggi [10]. Cryptocurrency dianggap sangat cocok untuk pencucian uang, teroris tujuan pembiayaan dan penghindaran pajak karena anonimitasnya, sifat lintas batas dan cepat kemampuan transfer. Ketiga, beberapa kejahatan tidak dapat dilakukan pada tahap ini melalui cryptocurrency. Kejahatan keuangan seperti penyalahgunaan pasar dan transaksi orang dalam misalnya tidak relevan untuk mata uang kripto. Aturan penyalahgunaan pasar terkait dengan instrumen keuangan yang diperdagangkan di pasar yang diatur, multilateral trading facility ("mtf") atau organised trading facility ("otf"). Untuk aplikasi untuk mata uang kripto ini menimbulkan dua masalah: mata uang kripto bukanlah instrumen keuangan dan mereka tidak diperdagangkan di pasar yang diatur, mtf atau otf.

Penelitian dimulai dengan definisi cryptocurrency dan blockchain. Setelah itu, taksonomi cryptocurrency akan diberikan berdasarkan analisis 10 cryptocurrency dengan kapitalisasi pasar. Taksonomi ini akan berfungsi sebagai tolok ukur selama penelitian ini dan akan memungkinkan untuk memverifikasi kecukupan kerangka hukum yang ada dan yang akan datang. Untuk mengungkap anonimitas [13], [14], [15], [16], [17], [18], [19], [20], [21], [22] pengguna cryptocurrency, ue harus mempertimbangkan sistem pendaftaran wajib pengguna dan tanggal yang telah ditentukan sebelumnya yang berlaku daripada sistem pendaftaran sukarela pengguna. Ue juga harus berpikir untuk memperluas daftar "entitas wajib" di bawah aml5 dengan para pemain yang diidentifikasi dalam penelitian ini sebagai titik lemah atau memiliki potensi besar menjadi titik lemah, termasuk penambang, pertukaran cryptocurrency murni yang tidak juga penyedia dompet kustodian, penyedia dompet perangkat lunak dan perangkat keras, platform perdagangan dan pemberi koin. Selain itu, ue harus berpikir untuk memberlakukan larangan khusus pada aspek-aspek seputar tersebut. Mata uang kripto yang ditujukan untuk membuatnya tidak mungkin untuk memverifikasi penggunaannya (misalnya pencampuran) dan memberikan sanksi pidana terhadap aspek-aspek ini. Selain itu, ue dapat mempertimbangkan untuk memperluas cakupan peraturan transfer dana menjadi pastikan bahwa semua informasi relevan yang menyertai transaksi cryptocurrency ada di sana, memungkinkan pemeriksaan pencucian uang dan pendanaan teroris yang memadai. Entitas yang harus memenuhi persyaratan dapat menjadi perantara di mana transaksi berjalan [23].

Dalam jangka panjang, ue harus mempertimbangkan untuk mengembangkan kerangka kerja untuk cryptocurrency, dan menetapkan standar ue untuk cryptocurrency sejalan dengan saran dan rekomendasi yang dibuat oleh eba, termasuk persyaratan lisensi untuk penyedia layanan cryptocurrency. Bagian dari kerangka kerja tersebut dapat membuat atau memaksakan "perantara", di mana penggunaan blockchain atau teknologi buku besar terdistribusi lainnya telah terputus perantara seperti itu, karena ini akan memungkinkan regulator untuk melampirkan peraturan kepada orang yang dapat diidentifikasi, sehingga berkontribusi pada peningkatan kepatuhan dan penegakan yang

efektif. Dengan maksud untuk mencapai regulasi terpadu cryptocurrency di tingkat g20, itu adalah merekomendasikan agar ue memimpin inisiatif lebih lanjut dengan memberi contoh.

Uni eropa harus meninggalkan blockchain dari pencucian uang, pendanaan teroris dan pajak penghindaran dan fokus pada kasus penggunaan terlarang cryptocurrency. Blockchain hanya teknologi dan dapat memiliki efek menguntungkan di beragam sektor. Perkembangannya seperti itu tidak boleh berkecil hati.

### **Cryptocurrency**

Cryptocurrency adalah mata uang digital di mana transaksinya dapat dilakukan dalam jaringan (online). Tidak seperti halnya mata uang kertas yang dicetak, cryptocurrency di desain dengan memecahkan soal-soal matematika berdasarkan kriptografi. Mata uang ini dibentuk berdasarkan teknologi kriptografi agar tidak mudah digandakan atau berpindah terhadap pihak lain yang bukan pemiliknya dan tidak memiliki akses pada mata uang ini. [24]. Satoshi nakamoto mengumumkan rilis pertama bitcoin, sistem uang elektronik baru yang menggunakan jaringan peer-to-peer untuk mencegah pengeluaran ganda. Ini benar benar terdesentralisasi tanpa server atau otoritas pusat. Untuk mewujudkan uang digital anda memerlukan jaringan pembayaran dengan akun, saldo, dan transaksi. Satu masalah utama yang harus diselesaikan oleh jaringan pembayaran adalah dengan mencegah apa yang disebut pengeluaran ganda untuk mencegah bahwa satu entitas menghabiskan jumlah yang sama sebanyak dua kali. Biasanya, ini dilakukan oleh server pusat yang menyimpan catatan tentang saldo. Dalam jaringan terdesentralisasi, anda tidak memiliki server ini. Jadi anda perlu setiap entitas jaringan untuk melakukan pekerjaan ini. Setiap rekan dalam jaringan harus memiliki daftar dengan semua transaksi untuk memeriksa apakah transaksi masa depan valid atau upaya untuk melipatgandakan pembelanjaan. Peer-to-peer, menghubungkan ke pengguna, membiarkan mereka untuk berbagi file dan sumber daya komputer tanpa server umum. Memfokuskan untuk membantu individu membuat informasi yang tersedia untuk penggunaan seseorang dengan menghubungkan para pemakai pada web. Contoh sintus p2p adalah napster.com dan mymp3.com. Teknologi kedua-duanya digunakan dengan mengizinkan konsumen untuk berbagi file dan jasa. Kriptografi adalah sebuah cabang ilmu komputer yang mempelajari cara menyembunyikan informasi. Melalui kriptografi, sebuah pesan rahasia diacak menjadi pesan yang seolah-olah tidak berbentuk, dan dikirimkan kepada pihak yang dituju. Sementara itu hanya pihak yang dituju sajalah yang dapat mengartikan pesan acak tersebut dan mengubahnya kembali menjadi pesan rahasia dari sang pengirim. Sejarah kriptografi dimulai pada zaman romawi kuno, ketika julius caesar berniat mengirimkan pesan pada salah satu jendral di medan perang, kemudian pesan itu ia harus kirimkan melalui kurir, namun ia tidak ingin jika pesan tersebut dibuka oleh kurir sebelum diterima oleh sang jenderal. Maka ia mengirimkan pesan tersebut dengan mengacak huruf dalam pesan. Cara yang beliau lakukan yaitu dengan mengganti huruf a, b, c, d dengan huruf, e, f, g, h dan seterusnya. Selama bertahun-tahun kriptografi menjadi bidang khusus yang hanya dipelajari oleh pihak militer, seperti agen keamanan nasional amerika serikat (national security agency), uni soviet, inggris, perancis, israel dan negara-negara lainnya yang telah membelanjakan miliaran dolar untuk mengamankan komunikasi mereka dari pihak luar, tetapi mereka selalu mempelajari kode-kode rahasia negara lain, dengan adanya persaingan ini maka kriptografi terus berkembang sesuai dengan perkembangan zaman.

Aset digital yang menggunakan kriptografi untuk keamanan, beroperasi secara independen dari bank sentral. Berbeda dengan mata uang tradisional, kripto memanfaatkan teknologi blockchain untuk mencatat dan memverifikasi transaksi secara terdesentralisasi.

Konsep ini revolusioner dalam dunia keuangan karena menghilangkan kebutuhan akan pihak ketiga yang terpercaya seperti bank dalam transaksi keuangan. Sebaliknya, kripto bergantung pada jaringan komputer terdistribusi yang menjalankan software open-source untuk memvalidasi dan mencatat setiap transaksi. Kriptografi, yang menjadi dasar nama “cryptocurrency”, digunakan untuk mengamankan transaksi dan mengontrol penciptaan unit baru [25]. ini memastikan bahwa aset digital tidak dapat diduplikasi atau dipalsukan, memberikan tingkat keamanan yang tinggi. Blockchain, teknologi yang mendasari sebagian besar kripto, adalah buku besar digital yang didistribusikan ke seluruh jaringan. Setiap “blok” dalam rantai ini berisi sekelompok transaksi yang telah diverifikasi oleh para pengguna jaringan. Begitu sebuah blok ditambahkan ke rantai, sangat sulit untuk diubah, memberikan tingkat transparansi dan keamanan yang tinggi. Desentralisasi adalah fitur kunci lainnya dari kripto. Tidak ada otoritas pusat yang mengontrol nilainya atau mengatur peredarannya. Sebaliknya, ini ditentukan oleh algoritma dan konsensus jaringan. Hal ini membuat kripto tahan terhadap manipulasi oleh pemerintah atau lembaga keuangan, dan potensial sebagai alat keuangan yang lebih demokratis [26]. Namun, penting untuk dicatat bahwa sifat desentralisasi dan kurangnya regulasi juga membawa risiko, termasuk volatilitas harga yang tinggi dan potensi penggunaan untuk aktivitas ilegal. Meskipun demikian, banyak yang melihat kripto sebagai masa depan keuangan, menawarkan cara yang lebih cepat, murah, dan aman untuk mentransfer nilai di seluruh dunia.

Pada tahun 1983, seorang programmer berkeley bernama david chaum menciptakan sebuah teknologi blind signature yaitu sistem pembayaran yang tidak bisa dilacak yang memisahkan identitas seseorang dari transaksi yang telah mereka lakukan [27]. Sekitar 2,9 hingga 5,8 juta pengguna swasta dan institusional juga secara aktif bertukar token dan menjalankan berbagai jaringan transaksi. Pada Mei 2017, kapitalisasi pasar mata uang kripto aktif melampaui \$91 miliar. Financial stability board (2018) menyebutkan bahwa pada 8 Januari 2018, kapitalisasi pasar gabungan aset kripto naik hingga \$830 miliar, di mana sekitar 35% disebabkan oleh bitcoin. Kemudian pada 4 Oktober 2018 turun menjadi sekitar \$210 miliar. Hingga saat ini bitcoin tetap mendominasi pasar, namun disisi lain bitcoin dihadapi oleh masalah teknis dan juga peningkatan teknologi mata uang kripto lainnya.

Kripto memiliki beberapa jenis data yang digunakan pada teknologi ini bergantung pada tujuan blockchain itu sendiri. Contohnya, dalam bitcoin data blok berisikan seluruh detail transaksi, mulai dari jumlah koin, pengirim, hingga penerima. Hash berisikan data berupa tanda tangan atau sidik jari atau tanda tangan. Hash digunakan untuk mengidentifikasi blok dan seluruh isinya dalam kode unik. Hash dari blok sebelumnya merupakan bagian yang membawa jejak informasi sebelumnya sekaligus mengamankan rantai blockchain. Blockchain adalah teknologi baru yang dikembangkan untuk sistem penyimpanan data digital. Teknologi ini terhubung melalui kriptografi dan penggunaannya sendiri tak bisa lepas dari mata uang bitcoin dan cryptocurrency. Kendati dianggap teknologi modern, ide awal blockchain sendiri sudah dicetuskan oleh scott dalam jurnalnya yang berjudul *journal of cryptography: how to time-stamp a digital document* sejak tahun 1991.

Bitcoin yang merupakan salah satu mata uang virtual (cryptocurrency) diciptakan oleh tokoh dengan nama samaran satoshi nakamoto dengan latar belakang untuk menghapus pihak otoritas pengendali pusat yang mengontrol sistem keuangan. Bitcoin diperoleh melalui penambangan secara virtual (mining), pembelian, atau dengan melakukan transfer pemberian (reward) [28].

Harga cryptocurrency tidak tetap karena selalu berubah setiap waktu. Naik turunnya nilai dari mata uang kripto tersebut akibat penawaran dan permintaan. Semakin banyak

permintaan maka nilai barang mengalami kenaikan, namun semakin banyak penawaran maka terjadi penurunan harga pada nilai barang tersebut. Bitcoin yang pada awalnya tidak mempunyai nilai jual atau tukar lambat laun mengalami progress dan mendapatkan harga jual. Nilai jual yang pertama kali ditetapkan adalah senilai satu dolar as yakni 1,309.03 btc atau sekitar delapan seperseratus sen per bitcoin. Pihak yang pertama kali menyediakan layanan jual beli bitcoin tersebut adalah new liberty standard pada 5 oktober 2009. Penyebab naiknya dan turunnya harga tersebut salah satunya karena spekulasi dan persepsi masyarakat. Faktor ini didasarkan pada persepsi masyarakat terhadap mata uang tersebut. Misalnya, bila bitcoin semakin mendapat perspektif yang baik, permintaan bitcoin akan semakin meningkat. Diikuti dengan semakin naiknya harga bitcoin. Sebaliknya, bila bitcoin mendapat persepsi yang kurang baik, harga bitcoin semakin turun. Persepsi tersebut meliputi bagaimana kemudahan menggunakan bitcoin, persepsi bagaimana harga bitcoin masa mendatang, dan persepsi seberapa besar keuntungan berinvestasi bitcoin. Harga yang fluktuatif liar dari cryptocurrency didapatkan dari persepsi masyarakat. Ketika pengguna cryptocurrency menghargai dan menggunakan cryptocurrency kemudian semakin persepinya baik maka cryptocurrency dapat menguntungkan pula bagi penggunanya. Namun sebaliknya, jika adanya persepsi yang buruk maka dapat pula merugikan penggunanya.

## **HASIL DAN PEMBAHASAN**

Bagaimana & mengapa bitcoin bekerja dengan menjalankan perangkat lunak bitcoin. Perhatikan bahwa program perangkat lunak yang disebut bit.dompert koin dapat berjalan di smartphone atau komputer pribadi dan memungkinkan pengguna untuk melakukan pembayaran melalui jaringan bitcoin. dalam konteks bitcoin, halaman yang membentuk buku besar disebut blok karena mereka mewakili "blok" data. Rantai blok, com berpose dari banyak blok individu, tumbuh terus-menerus dalam panjang dan kontramenyimpan semua transaksi yang dilakukan dalam bitcoin sejak diluncurkan pada bulan januari 2009 [11].

Permintaan transaksi bitcoin berisi hal-hal berikut:

1. Alamat bitcoin pembayar, yang berisi sumber dana untuk pembayaran,
2. Alamat bitcoin penerima (penerima pembayaran), dan
3. Jumlah bitcoin yang ditransfer.

Karena rantai blok berisi riwayat semua keluar dan pembayaran masuk yang terkait dengan alamat bitcoin pembayar, miners, yang juga mengelola jaringan bitcoin, dapat memvalidasi bahwa pembayar memiliki dana yang cukup untuk menutupi pembayaran. Kapan saja, siapa pun bisa lihat jumlah bitcoin yang ditautkan ke (atau, secara abstrak, disimpan di) alamat bitcoin tertentu. Lihat sendiri. Buka blockchain.info dan masukkan alamat berikut. Di bawah "cari", jumlah bitcoin yang terkait dengan alamat ini akan dikembalikan. Meskipun identitas pemiliknya tidak dapat diketahui dari bitcoin-nya alamat tanpa dia memberikan informasi ini, transfer apa pun masuk dan keluar dari rekeningnya, serta saldonya saat ini, secara publik tersedia untuk dilihat.

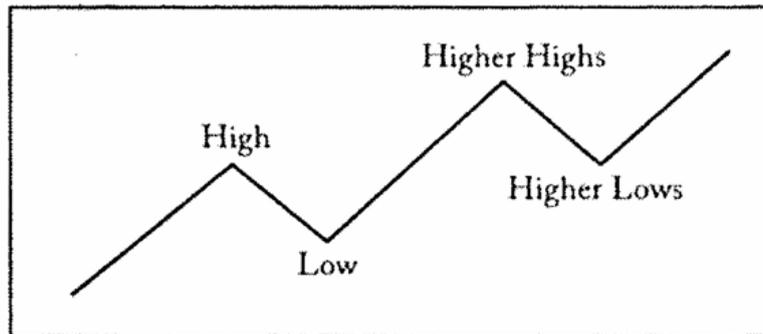
### **Uptrend, downtrend & sideways**

Tren adalah salah satu dari tiga butir pemikiran dasar dalam technical analysis yang sudah kita bahas didepan, yaitu : prices move in trend, secara ringkas, tren bisa didefinisikan sebagai kecenderungan arah pergerakan harga pada suatu pasar. Dalam dow theory dikarenakan bahwa terdapat tiga jenis tren, antara lain:

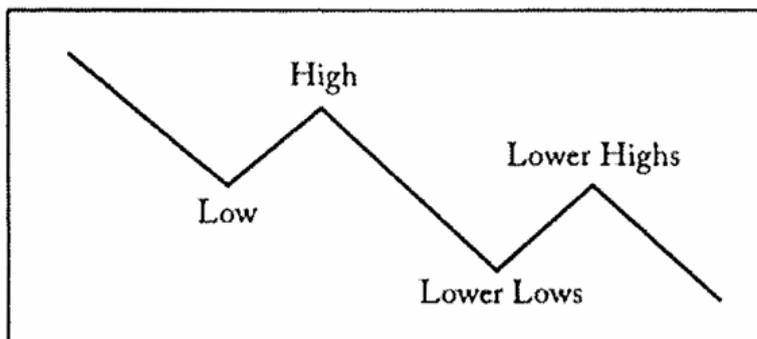
1. Uptrend (kecenderungan harga naik)
2. Downtrend (kecenderungan harga turun)
3. Sideways (kecenderungan harga ke samping/tetap), sideways juga sering disebut

dengan trendless atau tidak memiliki trend.

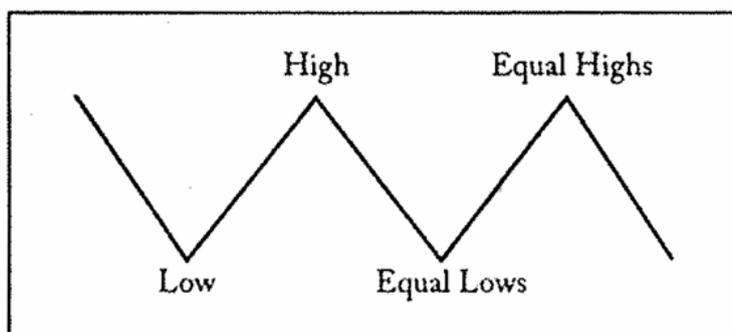
Namun, harga tentu tidak bergerak “naik terus-menerus” ataupun “turun terus-menerus”, tetapi naik-turun berulang kali sehingga membentuk gerakan zigzag. di dalam gerakan zigzag tersebut terdapat berbagai puncak (top) dan dasar (bottom) yang dapat memberikan acuan dalam menentukan kecenderungan arah market (trend). pada sebuah pola uptrend, puncak maupun dasar yang terbentuk semakin lama semakin tinggi pada pola downtrend, puncak dan dasar yang terbentuk semakin lama semakin rendah. Sedangkan pada pola sideways puncak ke puncak dan dasar ke dasar yang terbentuk (hampir) sama [29].



Gambar 1 Uptrend



Gambar 2 Downtrend



Gambar 3 Sideways

Blockchain adalah salah satu inovasi terbesar abad ke-21 yang mempengaruhi berbagai sektor, seperti keuangan, manufaktur, dan lembaga pendidikan. Sejarah blockchain bermula dari awal tahun 1990-an yang masih belum diketahui oleh banyak orang. Sebelum memahami evolusi blockchain, kita sebaiknya memahami evolusi internet terlebih dahulu. Apa yang kita gunakan saat ini adalah internet konvensional yang berfokus pada berbagi informasi. Semua situs web membantu pengguna untuk mempublikasikan dan berbagi informasi dengan orang lain di internet. Semua perusahaan

menggunakan internet konvensional ini untuk berbagi informasi dengan para pemangku kepentingan dan memberikan pengalaman pengguna yang baik, sehingga mereka mendapatkan lebih banyak pendapatan dari bisnis mereka. Pada saat yang sama, kita mencoba menciptakan internet nilai yang membawa nilai yang ditransaksikan melalui internet, yang hanya mungkin melalui teknologi blockchain.

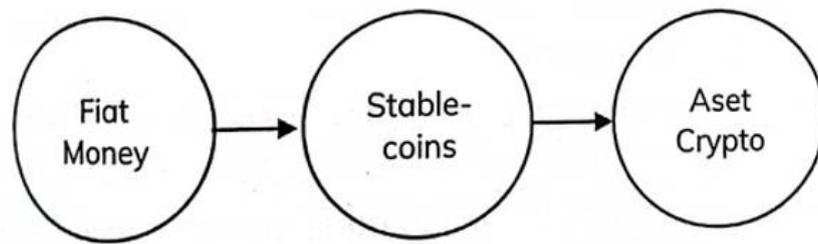
Pada awal tahun 1990-an, banyak orang mulai fokus pada mata uang digital. Pada tahun 1982, David Chaum mengusulkan uang digital melalui sebuah makalah dengan tanda tangan kosong untuk pembayaran yang tidak dapat dilacak. Banyak orang terlibat dalam menciptakan mata uang digital. Pada tahun 2008, Satoshi Nakamoto [3] mengkonseptualisasikan Bitcoin dalam makalahnya dan meluncurkannya pada tahun berikutnya. Para peneliti menemukan bahwa konsepnya sangat membantu dalam memecahkan banyak masalah perusahaan. Dalam waktu kurang dari satu dekade, teknologi blockchain berkembang dengan cepat dari versi 1.0 hingga 3.0. Setelah peluncuran blockchain pada tahun 2008, Ripple, mata uang lain yang dikenal, diperkuat oleh Ryan Fugger, kemudian Vitalik Buterin, pencipta Ethereum, memulai perjalanan blockchain 2.0 dengan menghadirkan teknologi blockchain ke dunia perusahaan. Linux Foundation juga bergabung dalam proyek Hyperledger mereka, dan setelah itu, Cardano Foundation dan IOTA mengambilnya ke level berikutnya, yaitu versi 3.0. Mari kita memahaminya secara bertahap.

Selain enkripsi simetris, seperti pada kode Caesar, di mana kunci yang sama digunakan untuk enkripsi dan dekripsi, kita juga berbicara tentang enkripsi asimetris. Untuk tujuan ini, pasangan kunci publik-privat dibuat. Untuk enkripsi, digunakan kunci yang berbeda daripada untuk dekripsi. Kunci publik dapat didistribusikan kepada siapa saja; itu bersifat publik. Ini berarti bahwa, misalnya, jika orang A ingin menulis pesan, mereka dapat menggunakan kunci publik akan mendekripsi pesan yang dikirim dengan kunci privatnya. Ini mirip dengan kotak masuk email Anda. Alamat email Anda diketahui, siapa pun yang ingin menulis pesan kepada Anda. Tetapi sebagai penerima, Anda hanya dapat mendekripsi pesan ini dengan kunci privat Anda. Untuk tujuan ini, enkripsi email menggunakan solusi seperti Pretty Good Privacy (PGP) dengan pasangan kunci asimetris.

Dalam konteks blockchain, tampaknya tidak (perlu) menggunakan tanda tangan digital sebagai pesan (atau transaksi) yang disertifikasi, karena ini sebenarnya diimplementasikan dalam sistem blockchain. Blockchain memetakan melalui mekanisme konsensus kapan dan di bawah kondisi apa transaksi valid. Tidak diperlukan sertifikasi oleh instansi pusat (terpercaya) untuk ini. Jaringan yang memutuskan. Meskipun demikian, blockchain menggunakan metode enkripsi asimetris dengan fungsi satu arah yang disebut untuk memastikan otentikasi. Untuk ini, pengguna memilih kunci pribadi yang dibuat secara acak.[30]

### **Deposit & withdrawal**

Bagaimana cara untuk berinvestasi cryptocurrency dan bagaimana melakukan setoran di awal merupakan pertanyaan paling dasar yang selalu ditanyakan ketika pertama kali berinvestasi di market cryptocurrency. Untuk berinvestasi pada market cryptocurrency, langkah pertama yang dilakukan adalah menukarkan uang fiat dari semua currency yang kalian miliki (dolar, rupiah, peso, dinar, dan lain sebagainya) ke stablecoins (USDT, USDC, USDP, USDD, USDJ, dan lain sebagainya).[31] Untuk melakukan proses memindahkan fiat ke stablecoins adalah sebagai berikut:



Gambar 4 Process fiat money to stablecoins

Lalu bagaimana untuk melakukan cash out atau withdrawal? Untuk melakukan suatu cash out atau melakukan withdrawal langkah yang dilakukan adalah menukarkan atau menjual aset crypto yang kita miliki kedalam stablecoins [32]. Kemudian dari stablecoins tersebut kita tukarkan ke fiat yang ada dalam exchange. Langkah terakhir barulah kita mengajukan penarikan dari fiat kita ke bank lokal yang bekerja sama dengan exchange yang kita gunakan. Secara proses skema cash out adalah seperti ini:



Gambar 5 Process skema cash out

### **Security issues involved in blockchain systems**

Blockchain terutama berkonsentrasi pada tiga konsep keamanan yaitu kerahasiaan, integritas, dan ketersediaan. Pada dasarnya, block chain adalah sistem terdistribusi, sehingga memberikan ketersediaan dan semua node dalam blockchain setuju berdasarkan rantai transaksi maka integritas data tetap terjaga. Dengan bantuan kunci kriptografi yang tepat, kerahasiaan transaksi dapat dijaga. Pendekatan holistik dalam sistem blockchain meliputi otentikasi dan otorisasi entitas yang menggunakan blockchain, transparansi transaksi, verifikasi dan keamanan infrastruktur komunikasi, keamanan dari orang dalam yang tidak berwenang, node yang disusupi atau kegagalan server. Sistem blockchain terutama melihat keamanan dalam aspek-aspek berikut.

1. ledger level security.
2. network level security.
3. transaction-level security
4. associated surround system security.
5. smart contract security

#### **Ledger level security**

Anggota yang sah hanya dapat berpartisipasi dalam blockchain. Transaksi yang diprakarsai oleh anggota harus ditandatangani dan peserta yang sah membuat transaksi dalam jaringan.

#### **Network level security**

Komunikasi antara komponen dari node yang berbeda harus aman dari sudut pandang jaringan. Ia harus tahan dari berbagai vektor serangan eksternal dan internal dalam jaringan. Buku besar harus memiliki kemampuan untuk menahan serangan dos.

#### **Transaction-level security**

Transaksi harus dienkripsi dengan konsep pki sehingga tidak ada yang berkompromi dengan pihak-pihak yang tidak berkepentingan. Identitas dan otorisasi pembuatan

transaksi harus dijaga, misalnya hanya nama 'x' tertentu yang dapat melakukan transaksi dengan menggunakan nama 'x' tersebut. Tidak ada yang dapat memodifikasi atau mengubah informasi transaksi dan fitur multisignature tersedia untuk transaksi yang sensitif dalam blockchain.

#### **Associated surround system security**

Komponen sistem surround yang terkait seperti basis data bayangan harus diakses oleh pengguna yang valid. Untuk mencapai hal ini, terapkan mekanisme otentikasi dan otorisasi. Hal ini juga dalam berbagai dokumen untuk mencegah virus, worm, dan malware.

#### **Smart contract security**

Kontrak blockchain atau kontrak digital atau kontrak yang dapat dieksekusi sendiri atau kontrak pintar bertindak sebagai perjanjian; kontrak ini dapat dibuat sebelumnya dengan kemampuan untuk dieksekusi sendiri dan ditegakkan sendiri. Kontrak yang dimuat dalam blockchain harus mengikuti aturan dasar yang diberikan oleh jaringan. Kontrak-kontrak ini mungkin membutuhkan data dari sumber eksternal yang mungkin saja merupakan data yang dirusak. Untuk menghindari hal ini, bukti kriptografi harus dilampirkan. Bukti tersebut berasal dari sumber yang terpercaya dan tidak dirusak.

#### **Privacy issues in blockchain systems**

Salah satu blockchain yang terkenal adalah mata uang kripto bitcoin. Bitcoin hadir dengan buku besar blockchain tanpa izin, sehingga setiap transaksi akan terlihat oleh semua orang dan siapa pun dapat memverifikasi. Privasi transaksional dan ketidakterkaitan adalah dua kategori untuk menyediakan mekanisme privasi dalam sistem blockchain.

#### **Transactional privacy**

Hanya pihak-pihak yang bertransaksi, regulator, dan auditor yang dapat melihat detail transaksi. Node yang berpartisipasi memiliki teknik teknologi untuk memvalidasi transaksi dengan mempertimbangkan ketersediaan dana, di mana transaksi sepenuhnya dienkripsi.

#### **Unlinkability**

Entitas arbitrer tidak dapat mengetahui rincian transaksi antara satu sama lain. Dimungkinkan untuk menambang data dari beberapa transaksi sehingga informasi mungkin berguna untuk mendapatkan informasi tentang pihak-pihak yang terlibat dalam transaksi. Ide dari ketidakterkaitan adalah tentang menghindari pemotongan tersebut dilakukan.

#### **Consensus mechanisms in blockchain**

Mekanisme konsensus menyediakan urutan transaksi yang pasti dan memvalidasi blok transaksi. Dalam aplikasi blockchain, ada dua masalah yang harus diselesaikan

1. double spending problem: pada satu waktu menggunakan kembali mata uang dalam dua transaksi.
2. byzantine generals problem: pada sistem terdistribusi, data ditransfer antar node melalui komunikasi peer to peer dan ada kemungkinan beberapa node dalam sistem dapat diserang yang menyebabkan perubahan isi komunikasi sehingga kita harus mengidentifikasi node yang tidak aman.

## **KESIMPULAN**

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, berikut adalah kesimpulan dari kajian mengenai pengaruh teknologi blockchain terhadap keamanan dan privasi pada sistem pembayaran berbasis kriptografi.

- a. Sistem mata uang digital terdesentralisasi yang dikenal sebagai "bitcoin" menggunakan teknologi blockchain sebagai buku besar publik untuk mencatat semua

transaksi. Para miner menjalankan proses verifikasi untuk memverifikasi transaksi bitcoin, yang memastikan apakah pengirim memiliki dana yang cukup. Untuk menjaga keamanan dan privasi transaksi, bitcoin menggunakan enkripsi asimetris, yang menggunakan kunci publik dan pribadi untuk enkripsi dan dekripsi data.

- b. Blockchain yang berisi catatan transaksi dikenal sebagai "blockchain", teknologi utama yang mendasari bitcoin. Setiap blok dalam blockchain mencatat transaksi yang diverifikasi oleh jaringan. Ini memastikan bahwa transaksi tidak dapat diubah atau dihapus dan memastikan bahwa blockchain aman dari serangan dari sumber luar. Blockchain memungkinkan transfer aset atau nilai secara digital tanpa memerlukan pihak ketiga yang dapat diandalkan.
- c. Tiga tren utama dalam analisis teknikal pasar adalah uptrend, downtrend, dan sideways. Tren-tren ini menunjukkan pola pergerakan harga di pasar yang dapat digunakan untuk membuat keputusan investasi.
- d. Keamanan blockchain berpusat pada tiga ide utama, kerahasiaan, integritas, dan ketersediaan. Sistem blockchain menjaga keamanan di berbagai tingkatan, seperti pada tingkat buku besar, jaringan, transaksi, dan sistem pendukung, melalui penggunaan mekanisme enkripsi dan otentikasi.
- e. Mekanisme konsensus, seperti proof of work (pow), digunakan untuk memastikan integritas dan urutan transaksi dalam blockchain. Mereka juga membantu menghindari masalah seperti serangan yang sering terjadi pada sistem terdistribusi dan pengeluaran ganda (double spending).
- f. Dalam blockchain, privasi sangat penting, terutama dalam sistem seperti bitcoin, di mana setiap transaksi dapat dilihat oleh publik. Privasi dapat dicapai melalui teknik yang menghindari entitas atau transaksi yang terkait, meskipun jaringan dapat melihat setiap transaksi.
- g. Penggunaan dalam cryptocurrency: untuk memulai investasi dalam mata uang kripto, pengguna harus menukar uang fiat menjadi stablecoins seperti usdt atau usdc. Enkripsi melindungi setiap transaksi yang terjadi dalam sistem blockchain. Ini memastikan bahwa hanya pihak yang sah yang dapat melakukan dan memvalidasi transaksi.

Secara keseluruhan, teknologi blockchain memiliki potensi besar untuk melindungi sistem pembayaran berbasis kriptografi dari keamanan, privasi, dan integritas, dengan menerapkan lapisan perlindungan kriptografi yang kompleks dan mekanisme konsensus yang terdesentralisasi. Namun, masih ada masalah privasi dan keamanan yang perlu diperhatikan, terutama ketika mengelola kontrak pintar dan data yang berasal dari sumber eksternal.

## DAFTAR PUSTAKA

- “bitcoin and beyond.” [online]. Available: [www.routledge.com/ripe-determinan-penggunaan-mata-uang-kripto-di-indonesia](http://www.routledge.com/ripe-determinan-penggunaan-mata-uang-kripto-di-indonesia).
- “e-book-crypto-trading-guide-akademi-crypto-lpdf\_compress”.
- “overview • about myself • what is bitcoin, cryptocurrency? • breaking it down into layers • explore the blockchain • send some ether.”
- “technical-analysis-for-mega-profit-by-edianto-ong\_compress”.
- “the book of satoshi the collected writings of bitcoin creator satoshi nakamoto phil cha mpagne foreword by jeff berwick.”
- a. Al-dmour, r. Al-dmour, h. Al-dmour, and a. Al-adwan, “blockchain applications and commercial bank performance: the mediating role of ais quality,” *journal of open innovation: technology, market, and complexity*, vol. 10, no. 2, jun. 2024, doi: 10.1016/j.joitmc.2024.100302.

- a. Kurniawan et al., “a review of blockchain: how does it work, applications, and challenges,” *journal of telematics and informatics (jti)*, vol. 7, no. 2, p. 69, 2019.
- ahmed. Banafa, *introduction to blockchain technology banafa*. River publishers, 2023.
- b. Ram and p. Verma, “application of blockchain technology in data security,” *ip indian journal of library science and information technology*, vol. 9, no. 1, pp. 51–55, aug. 2024, doi: 10.18231/j.ijlsit.2024.008.
- buntoro irawan, “humantech jurnal ilmiah multi disiplin indonesia implementasi teknologi blockchain untuk keamanan data internet of things,” 2023.
- d. Tapscott, “blockchain revolution: how the technology behind bitcoin and other cryptocurrencies is changing the world - pdfdrive.com,” 1995.
- e. D. Astutik and m. L. Ghozali, “cryptocurrency sebagai mata uang, komoditas, dan instrumen investasi dalam perspektif sad dzariah,” *al-manhaj: jurnal hukum dan pranata sosial islam*, vol. 4, no. 2, pp. 699–706, dec. 2022, doi: 10.37680/almanhaj.v4i2.2004.
- e. Jones’, “bitcoin, cryptocurrencies and blockchain a technology and financial services sector report.” [online]. Available: [www.edwardjones.ca](http://www.edwardjones.ca).
- h. Hellani, l. Sliman, a. E. Samhat, and e. Exposito, “overview on the blockchain-based supply chain systematics and their scalability tools,” *emerging science journal*, vol. 4, no. Special issue, pp. 45–69, 2020, doi: 10.28991/esj-2021-sp1-04.
- k. Adam, *blockchain technology for business processes: meaningful use of the new technology in businesses*. Springer berlin heidelberg, 2022. Doi: 10.1007/978-3-662-65818-5.
- m. Bahanan, s. Al-utsmami bondowoso, and m. Wahyudi, “analisis pengaruh penggunaan teknologi blockchain dalam transaksi keuangan pada perbankan syariah,” 2023.
- m. Kuliah, p. Internasional, d. Pengampu, : guru, and g. Zalzalalah, “makalah cryptocurrency & teknologi blockchain.”
- m. Mcnaught, “cryptocurrency chronicles unlocking the secrets of blockchain technology simple explanations for complex concepts,” 2023.
- m. Teodorescu and e. Korchagina, “applying blockchain in the modern supply chain management: its implication on open innovation,” *journal of open innovation: technology, market, and complexity*, vol. 7, no. 1, 2021, doi: 10.3390/joitmc7010080.
- n. Khan, t. Ahmad, and r. State, “blockchain-based micropayment systems: economic impact,” in *acm international conference proceeding series*, association for computing machinery, jun. 2019. Doi: 10.1145/3331076.3331096.
- p. Khordadpour and s. Ahmadi, “security and privacy enhancing in blockchain-based iot environments via anonym auditing,” 2024.
- p. S. G. A. Sri and d. L. Bhaskari, “a study on blockchain technology,” *international journal of engineering and technology(uae)*, vol. 7, pp. 418–421, 2018, doi: 10.14419/ijet.v7i2.7.10757.
- q. Deng, “application analysis on blockchain technology in cross-border payment,” 2020.
- r. Houben and a. Snyers, “cryptocurrencies and blockchain legal context and implications for financial crime, money laundering and tax evasion study requested by the tax3 committee policy department for economic, scientific and quality of life policies.”
- s. Steffen, b. Bichsel, r. Baumgartner, and m. Vechev eth zurich, “zeestar: private smart contracts by homomorphic encryption and zero-knowledge proofs,” 2022, doi: 10.1109/sp46214.2022.00114.
- untung raharfja, qurtul aini, m. Yusup, and aulia edliyanti, “penerapan teknologi blockchain sebagai media pengamanan proses transaksi e-commerce,” 2020.
- v. Buterin, j. Illum, m. Nadler, f. Schär, and a. Soleimani, “blockchain privacy and regulatory compliance: towards a practical equilibrium,” *blockchain: research and applications*, vol. 5, no. 1, mar. 2024, doi: 10.1016/j.bcr.2023.100176.
- v. Gugueoth, s. Safavat, s. Shetty, and d. Rawat, “a review of iot security and privacy using decentralized blockchain techniques,” nov. 01, 2023, elsevier ireland ltd. Doi: 10.1016/j.cosrev.2023.100585.
- x. Tang and l. Shi, “security analysis of smart contract migration from ethereum to arbitrum,” *blockchains*, vol. 2, no. 4, pp. 424–444, oct. 2024, doi: 10.3390/blockchains2040018.

- z. Xie, s. Dai, h.-n. Chen, and x. Wang, "blockchain challenges and opportunities: a survey," 2018.
- z. Zheng, s. Xie, h. Dai, x. Chen, and h. Wang, "an overview of blockchain technology: architecture, consensus, and future trends," in proceedings - 2017 ieee 6th international congress on big data, bigdata congress 2017, institute of electrical and electronics engineers inc., sep. 2017, pp. 557–564. Doi: 10.1109/bigdatacongress.2017.85.