



Blockchain adalah buku besar digital terdesentralisasi, terdistribusi dan publik, yang dikelola bersama oleh banyak pihak, menggunakan kriptografi untuk memastikan keamanan transmisi dan akses, untuk mencapai penyimpanan data konsistensi, bukti kerusakan data, dan pencegahan penolakan. Itu juga dikenal sebagai Teknologi Ledger Terdistribusi (DLT). Blockchain yang khas menyimpan data dalam satuan blok. Setiap blok menyertakan kriptografi hash dari blok sebelumnya di blockchain untuk menghubungkan dua blok yang berdekatan. Keterkaitan blok adalah "rantai". Blockchain, sebagai komputasi baru paradigma dan model kolaborasi dalam persaingan yang tidak dipercaya lingkungan, sedang mengubah skenario aplikasi dan aturan operasi banyak industri dengan mekanisme pembangunan kepercayaan yang unik. Itu adalah salah satu teknologi yang sangat diperlukan untuk membangun sistem kepercayaan baru dan berkembang ekonomi digital di masa depan.

Dalam sistem blockchain yang khas, masing-masing pihak berbagi informasi dan jangkauan konsensus sesuai dengan aturan yang disepakati sebelumnya. Untuk mencegah informasi konsensus dirusak, sistem menyimpan data dalam satuan blok yang membentuk rantai kriptografi struktur data dalam urutan kronologis, dan catatan node dipilih oleh konsensus mekanisme untuk menentukan data dari blok terbaru dan node lainnya berpartisipasi dalam verifikasi, penyimpanan, dan pemeliharaan data terbaru blok. Setelah data dikonfirmasi, sulit untuk menghapus dan memodifikasi, dan hanya operasi permintaan yang sah yang dapat dilakukan. Bergantung kepada apakah sistem memiliki mekanisme penerimaan / kontrol node, blockchains dapat diklasifikasikan ke dalam Blockchains yang Diiijinkan dan Tanpa Izin Blokir. Bergabung dan keluar dari node di diizinkan blockchain membutuhkan izin dari sistem blockchain. Bergantung kepada Apakah entitas dengan hak kontrol terpusat atau tidak, Diiijinkan blockchain dapat dibagi ke dalam Konsorsium Blockchain dan Blockchain Pribadi. Blockchain Izin, juga disebut sebagai Blockchain Publik, benar-benar terbuka, di mana node dapat bergabung dan keluar di kapan saja.

#### A. Karakteristik Blockchain

Dibandingkan dengan database terdistribusi tradisional, blockchain mencerminkan karakteristik berikut: Pertama, dari akuntansi entri ganda ke akuntansi terdistribusi. Dalam sistem informasi tradisional, setiap akuntan mencatat secara terpisah, dan Ada beberapa buku besar yang berbeda pada setiap rekonsiliasi. Blockchain memecah akuntansi entri ganda asli

dan menjadi buku akun terdistribusi untuk "seluruh jaringan untuk dibagikan", di mana para pihak yang terlibat dalam pembukuan mencegah gangguan data dan memastikan konsistensi data. Melalui mekanisme koordinasi yang sinkron, menghindari proses rekonsiliasi multi-partai yang rumit. Kedua, dari "penyisipan, penghapusan, pemilihan dan pembaruan" ke "penyisipan dan pemilihan". Database tradisional memiliki empat operasi klasik untuk menyisipkan, menghapus, memperbarui, dan memilih. Dari prospektif seluruh buku jaringan, teknologi blockchain setara dengan basis data menyerah menghapus dan memperbarui opsi4, hanya menyisakan dua manipulasi, penyisipan dan seleksi, melalui struktur "blok-rantai" blok dan daftar tertaut, dan cap waktu yang sesuai untuk mengkonsolidasikan voucher membentuk kumpulan data tepercaya yang saling terkait dan sulit diubah. Ketiga, dari perawatan unilateral hingga pemeliharaan multi-lateral. Untuk setiap entitas, database tradisional adalah sistem informasi yang dikelola satu pihak, apakah itu arsitek terdistribusi atau arsitek terpusat, yang memiliki tingkat kontrol yang tinggi terhadap catatan data. Blockchain memperkenalkan buku besar terdistribusi, yang merupakan sistem informasi terdistribusi yang dikelola bersama oleh banyak pihak tanpa satu pun titik kegagalan. Penulisan data dan sinkronisasi tidak terbatas pada satu subjek dan lebih lanjut perlu diverifikasi oleh banyak pihak untuk mencapai konsensus untuk memutuskan data mana yang dapat ditulis. Keempat, dari kontrak plug-in ke kontrak bawaan. Secara tradisional, aliran modal keuangan dan aliran informasi bisnis adalah dua proses bisnis yang berbeda. Kontrak yang ditandatangani oleh kerja sama bisnis, setelah tinjauan manual dan verifikasi hasil, dapat memberi tahu keuangan untuk melakukan pembayaran dan membentuk aliran modal yang sesuai. Munculnya kontrak pintar, berdasarkan aturan yang diatur, dilakukan secara independen melalui eksekusi kode, penulisan kolaboratif, dan "kontrak bawaan" yang mengintegrasikan aliran informasi dan aliran modal melalui kode algoritmik.

## B. Desain Blockchain

Ekosistem Blockchain semuanya memiliki kesamaan tertentu, tetapi memiliki perbedaan penting. Tiga aspek kunci dari setiap blockchain harus dievaluasi untuk memahami penerapannya pada situasi tertentu: desain teknologi, model tata kelola dan model konsensus.

### 1. Desain Teknologi

Desain teknis setiap blockchain menentukan jenis informasi apa yang dapat disimpan di blockchain. Sementara semua blockchains dapat menyimpan setidaknya beberapa jenis data minimum tertentu, mereka berbeda dalam cara mereka mendukung cryptocurrency (mata uang digital), logika bisnis dari transaksi tidak berantai dan struktur data lainnya.

### 2. Model Pemerintahan

Siapa yang bertanggungjawab? Setiap blockchain memiliki sarana untuk membuat keputusan yang penting untuk pengoperasian dan evolusi seiring waktu. Blockchain pribadi yang dijalankan oleh perusahaan dengan infrastruktur sendiri diatur oleh perusahaan itu, yang dapat mengubahnya sesuka hati. Blockchain yang dibagikan dalam model konsorsium dapat memiliki model tata kelola di mana beberapa atau semua anggota konsorsium dapat memberikan suara pada perubahan. Blockchain publik, yang tidak memiliki pemilik, biasanya mewujudkan model tata kelola dalam teknologi dan struktur basis data, memungkinkan siapa saja yang memenuhi kriteria tertentu untuk secara efektif memberikan suara pada perubahan kritis.

### 3. Model Konsensus

Bagaimana blok baru dibuat (atau dalam terminologi blockchain, "ditambang"?) Setiap blockchain memiliki proses dan aturan sendiri untuk bagaimana blok baru disetujui. Dalam blockchain pribadi, ini hanya modul perangkat lunak yang diizinkan membuat blok baru sesuka hati. Jika konsorsium atau grup perusahaan membagikan blockchain, mungkin ada aturan yang mengatakan semua, atau persentase tertentu, dari peserta harus menyetujui blok baru sebelum dapat ditambahkan. Di blockchain publik, blok baru dibuat oleh penambang (peserta yang mengumpulkan transaksi dan mencoba membuat blok baru untuk mendapatkan cryptocurrency), menggunakan salah satu dari beberapa pendekatan.

Setiap pendekatan dirancang untuk memastikan tidak mungkin bagi penambang aktor buruk untuk menyetujui blok baru. Untuk mencapai hal ini, berbagai blockchain bergantung pada campuran berbagai faktor, termasuk:

- Kebutuhan akan kekuatan komputasi yang besar lebih dari yang dapat dikumpulkan oleh satu penambang bitcoin atau kelompok
- Persaingan antar penambang bitcoin
- Crypto economics menciptakan insentif bagi penambang untuk menjaga blockchain tetap sehat (mis., Tidak bergabung dengan aktor jahat untuk merusaknya) untuk melindungi investasi mereka di dalamnya

#### C. Jenis-jenis Blockchain

Dimulai dengan Bitcoin pada tahun 2008, banyak arsitektur berbeda telah dikembangkan untuk memenuhi berbagai tujuan desain teknis, bisnis, dan tata kelola. Istilah 'blockchain' tidak memiliki definisi konseptual yang jelas dan digunakan untuk banyak perkembangan berbeda. Ada perbedaan luas dalam properti dari berbagai jenis blockchain seperti tingkat desentralisasi, kemampuan transaksi, mekanisme konsensus, aksesibilitas, ketetapan, skalabilitas atau transparansi. Akibatnya, praktisi blockchain dan media sering membuat pernyataan umum tentang blockchain seolah-olah mereka berlaku untuk semua blockchain, padahal sebenarnya pernyataan tersebut hanya terkait dengan satu blockchain atau satu keluarga teknologi blockchain. Juga, banyak praktisi percaya hanya bentuk tertentu dari blockchain yang "sah." Buku putih ini tidak membuat penilaian itu, tetapi menyajikan berbagai bentuk menggunakan terminologi populer bahkan jika itu tidak disetujui secara universal.

Perbedaan yang sering digunakan dari jenis blockchain dibuat berdasarkan aksesibilitas ke publik (mis. Tanpa izin) atau pribadi (mis. Diizinkan). Konsorsium adalah jenis khusus dari blockchain yang dianggap sebagai jenis berbeda dari blockchain, tetapi juga termasuk dalam jenis blockchain pribadi.

##### 1. Publik / Tanpa Izin

Blockchains publik, seperti Bitcoin, Ethereum, dan banyak lainnya, menawarkan akses sepenuhnya terbuka dan dapat dibaca atau ditulis oleh siapa saja, tanpa otorisasi sebelumnya. Game insentif teoritis<sup>2</sup> digunakan untuk mempromosikan kepercayaan antara node yang tidak dikenal. Blockchain publik dianggap sepenuhnya terdesentralisasi. Pendukung mengklaim bahwa karena pengembang aplikasi tidak memiliki wewenang untuk mengadaptasi atau memodifikasi platform setelah digunakan, independensi dan

ketahanan sensor terjamin. Berdasarkan karakteristik ini, penganjur blockchain publik menganggap teknologi sebagai enabler untuk keterbukaan, transparansi dan netralitas. Namun, tanpa mekanisme teknis atau hukum untuk menegakkan kepatuhan, blockchains publik mungkin berisiko beralih ke kekacauan. Blockchain publik membutuhkan keamanan yang kuat dan tata kelola yang matang untuk menghasilkan kepercayaan dan kepercayaan yang diperlukan di antara mereka yang akan membangun aplikasi komersial atau sensitif yang berumur panjang di atasnya.

## 2. Pribadi / Izin dan Konsorsium

Blokir privat / yang diizinkan telah muncul sebagai alternatif dari blockchain publik untuk menggunakan teknologi di antara serangkaian peserta yang dikenal dan dikenal. Dalam arsitektur blockchain pribadi (diizinkan), menulis izin (kemampuan untuk menambahkan catatan ke database) diberikan hanya untuk node yang disetujui. Izin baca lengkap atau terbatas dapat dibuat tersedia untuk semua node atau untuk publik atau sepenuhnya dibatasi.

Blokir pribadi dapat menarik untuk beberapa kasus penggunaan bisnis di mana diperlukan tingkat privasi, kemampuan audit dan tata kelola tertentu. Semua peserta dalam blockchain pribadi dapat diidentifikasi, tetapi tidak perlu saling mempercayai. Informasi terbatas mungkin dapat dilihat oleh publik, atau tidak. Berbeda dengan blockchain publik, otoritas yang didefinisikan dapat mengubah aturan yang ditetapkan untuk blockchain. Mekanisme konsensus dari blockchain privat bisa lebih sederhana, dengan satu node atau sekelompok node yang memiliki otoritas untuk memvalidasi blok baru.

Jenis khusus dari blockchain pribadi (sering dianggap sebagai jenis berbeda) adalah blockchain konsorsium, yang dapat dipahami sebagai blockchain di mana konsensus diperoleh oleh set node resmi, seperti node yang dimiliki oleh kumpulan lembaga keuangan. Jenis blockchain ini dapat dideskripsikan sebagai sebagian terdesentralisasi, di mana tidak ada satu simpul pun yang memiliki kendali penuh, tetapi tidak satu pun simpul yang diizinkan untuk bergabung dan berpartisipasi sesuka hati.

## Referensi

- <https://a16z.com/2018/02/10/cryptoreadings-resources/>
- <https://a16z.com/category/blockchaincryptocurrencies/>
- <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyondthe-hype-what-is-the-strategic-business-value>
- <http://www.caict.ac.cn/english/yjcg/bps/201901/P020190131402018699770.pdf>
- [https://cdn.ymaws.com/www.htng.org/resource/collection/CC1CE2B8-0377-457E-9AB0-27CFDD77E17B/2018-10-17\\_Blockchain\\_White\\_Paper\\_FINAL.pdf](https://cdn.ymaws.com/www.htng.org/resource/collection/CC1CE2B8-0377-457E-9AB0-27CFDD77E17B/2018-10-17_Blockchain_White_Paper_FINAL.pdf)