

Materi TIDAK untuk Diperjual Belikan

BLOCKCHAIN BITCOIN CRYPTOCURRENCY

The New Era Of Technology



DISCLAIMER

Materi dalam presentasi ini dibuat untuk tujuan edukasi dan informasi saja. Seluruh konten, termasuk teks, gambar, dan data, dilindungi oleh hak cipta yang dimiliki oleh penulis dan sumber aslinya. Dilarang memperjualbelikan atau mendistribusikan materi ini tanpa izin tertulis dari pemilik hak cipta.

Copyrights © RegionsID 2024. All Rights Reserved

**“ I NEVER DREAMED
ABOUT SUCCESS.
I WORKED FOR IT. ”**

- ESTÉE LAUDER

Materi TIDAK untuk Diperjual Belikan



BLOCKCHAIN



**Materi TIDAK
untuk Diperjual
Belikan**

Blockchain adalah basis data terdistribusi atau buku besar yang dibagikan di antara node dalam jaringan komputer. Blockchain paling dikenal karena perannya yang krusial dalam sistem cryptocurrency untuk menjaga catatan transaksi yang aman dan terdesentralisasi, tetapi penggunaannya tidak terbatas pada cryptocurrency. Blockchain dapat digunakan untuk membuat data di industri mana pun menjadi tidak dapat diubah—istilah yang digunakan untuk menggambarkan ketidakmampuan untuk diubah.

Karena tidak ada cara untuk mengubah sebuah blok, kepercayaan hanya diperlukan pada titik di mana pengguna atau program memasukkan data. Aspek ini mengurangi kebutuhan akan pihak ketiga yang terpercaya, yang biasanya adalah auditor atau manusia lain yang menambah biaya dan membuat kesalahan.

Sejak diperkenalkannya Bitcoin pada tahun 2009, penggunaan blockchain telah meledak melalui penciptaan berbagai cryptocurrency, aplikasi keuangan terdesentralisasi (DeFi), token non-fungible (NFT), dan kontrak pintar.

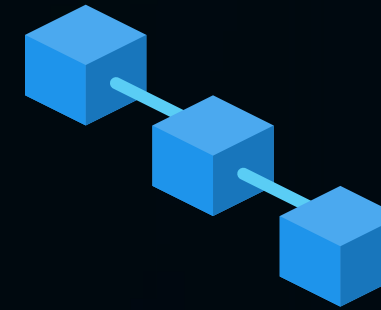
BLOCKCHAIN



**Materi TIDAK
untuk Diperjual
Belikan**

Poin Penting:

- **Struktur Blockchain:** Jenis basis data bersama yang berbeda dari basis data biasa dalam cara menyimpan informasi; blockchain menyimpan data dalam blok yang dihubungkan melalui kriptografi.
- **Penyimpanan Serbaguna:** Berbagai jenis informasi dapat disimpan di blockchain, tetapi penggunaan yang paling umum adalah sebagai buku besar untuk transaksi.
- **Desentralisasi:** Dalam kasus Bitcoin, blockchain bersifat terdesentralisasi, sehingga tidak ada satu orang atau grup yang memiliki kontrol—sebaliknya, semua pengguna secara kolektif mempertahankan kontrol.
- **Tidak Dapat Diubah:** Blockchain terdesentralisasi tidak dapat diubah, yang berarti data yang dimasukkan tidak dapat diubah. Untuk Bitcoin, transaksi dicatat secara permanen dan dapat dilihat oleh siapa saja.



BLOCKCHAIN

Blockchain adalah buku kas digital dengan basis data yang terdistribusi ke banyak komputer dalam satu jaringan. Yang membedakan blockchain dengan buku kas atau database lainnya adalah struktur datanya. Hal ini karena blockchain mengumpulkan data-data transaksi ke dalam satu blok dengan kapasitas yang terbatas.

Setiap blok dapat menyimpan data dalam beberapa MB. Tergantung ukuran data transaksinya, sebuah blok tunggal dapat menyimpan ribuan data transaksi keuangan.

Setiap blok yang sudah diverifikasi akan memiliki kode berupa angka dan huruf yang tidak beraturan, yang disebut dengan hash. Kode atau hash ini diproses dari data yang ada di dalam blok dan juga hash dari blok sebelumnya, sehingga blok-blok ini saling terhubung membentuk rantai berkelanjutan. Sehingga, kalau data yang ada di dalam blok berubah, otomatis hash akan berubah. Kalau hash pada satu blok berubah, maka hash pada blok berikutnya pun akan ikut berubah.

Hash Blok Sebelumnya : dsad1dex90d98sa

Input	Hash
Ann gave 10 coins to Mary	8977e7c112aea5b0a62e9c5f3084a203
Mary gave 5 coins to Jack 8977e7c112aea5b0a62e9c5f3084a203	e37a8d1cc39ed9f54afadb6c6cafe639
Mary gave 3 coins to Ann e37a8d1cc39ed9f54afadb6c6cafe639	5b9foe325f58766f5a2dfe7eec636f6d
Ann gave 1 coins to Adam 5b9foe325f58766f5a2dfe7eec636f6d	55f28ee65412b22aa3d6002bcf7d67201

Hash Blok ini : dsad99999779ax008sa

Hash Blok sebelumnya : dsad99999779ax008sa

Input	Hash
Ann gave 10 coins to Mary	8977e7c112aea5b0a62e9c5f3084a203
Mary gave 5 coins to Jack 8977e7c112aea5b0a62e9c5f3084a203	e37a8d1cc39ed9f54afadb6c6cafe639
Mary gave 3 coins to Ann e37a8d1cc39ed9f54afadb6c6cafe639	5b9foe325f58766f5a2dfe7eec636f6d
Ann gave 1 coins to Adam 5b9foe325f58766f5a2dfe7eec636f6d	55f28ee65412b22aa3d6002bcf7d67201

Hash Blok ini : sdasdx9019xfsd



SEJARAH BLOCKCHAIN



**Materi TIDAK
untuk Diperjual
Belikan**

Stuart Haber dan Scott Stornetta

Blockchain saat ini selalu diasosiasikan dengan cryptocurrency, meskipun sebenarnya teknologi ini sudah dikembangkan jauh sebelum Bitcoin ada. Adalah dua orang ilmuwan, Stuart Haber dan Scott Stornetta, yang menciptakan konsep blockchain pada awal tahun 1990-an. Mereka memperkenalkan sistem timestamping untuk dokumen digital yang tidak dapat diubah atau dihapus, sehingga menciptakan fondasi bagi teknologi blockchain.



SEJARAH BLOCKCHAIN

Pada tahun 2008, seorang atau sekelompok individu dengan nama samaran Satoshi Nakamoto memperkenalkan konsep blockchain Bitcoin. Nakamoto merilis whitepaper berjudul "Bitcoin: A Peer-to-Peer Electronic Cash System," yang menjelaskan bagaimana teknologi blockchain dapat digunakan untuk menciptakan mata uang digital yang aman dan desentralisasi. Dalam whitepaper tersebut, Nakamoto mengutip tiga hasil riset kriptografer Haber dan Stornetta, menunjukkan bagaimana teknologi blockchain dapat meningkatkan keamanan pengiriman mata uang digital melalui sistem desentralisasinya.






Teknologi ini kemudian menjadi fondasi Bitcoin yang diciptakan oleh Satoshi Nakamoto pada tahun 2009. Bitcoin memanfaatkan blockchain untuk mencatat setiap transaksi dalam sebuah buku besar publik yang terdesentralisasi. Setiap blok dalam blockchain berisi sejumlah transaksi yang diverifikasi oleh jaringan peer-to-peer sebelum ditambahkan ke rantai blok sebelumnya, menciptakan sistem yang transparan dan sulit untuk diubah tanpa konsensus dari seluruh jaringan.

Penggunaan blockchain tidak hanya terbatas pada cryptocurrency. Teknologi ini memiliki potensi aplikasi yang luas dalam berbagai bidang, termasuk supply chain management, voting systems, healthcare, dan banyak lagi, karena sifatnya yang aman, transparan, dan terdesentralisasi.

Materi TIDAK untuk Diperjual Belikan



KEUNTUNGAN BLOCKCHAIN

-  Aman: Jaringan blockchain diamankan menggunakan teknologi kriptografi yang menjamin keamanannya dari berbagai macam serangan. Namun, terdapat titik kelemahan dalam berbagai teknologi yang dihubungkan ke jaringan blockchain seperti dompet digital, server penyimpanan data, situs web, dan platform aplikasi terdesentralisasi.
-  Anonimitas data transaksi: Blockchain menawarkan pseudonymity di mana data pribadi setiap transaksi disamarkan. Sistem seperti ini memberikan perlindungan terhadap data pribadi setiap pengguna dan tetap memberikan transparansi.
-  Global: Aplikasi dan platform yang menggunakan sistem blockchain bersifat global dan tidak dibatasi oleh batasan negara atau wilayah. Pemindahan aset dan transaksi pada blockchain bisa dilakukan dari semua wilayah yang memiliki akses internet.
-  Peer-to-peer (P2P): Semua transaksi pada sistem terdesentralisasi diproses secara peer-to-peer (P2P) tanpa membutuhkan pihak ketiga.
-  Transparan: Semua data transaksi yang pernah terjadi pada sebuah blockchain publik dapat diakses secara mudah melalui berbagai situs seperti ETHscan. Data ini juga meliputi nominal, waktu, dan alamat tujuan transaksi.

Materi TIDAK untuk Diperjual Belikan



KELEMAHAN BLOCKCHAIN

- ⚡ Membutuhkan energi besar: Teknologi blockchain membutuhkan energi listrik yang cukup besar. Energi ini dibutuhkan penambang sebagai node yang memproses penambahan blok ke dalam rantai blockchain. Bitcoin mengonsumsi sekitar 80 TWh per tahun (CCAF).
- 🐢 Kepadatan jaringan: Kepadatan jaringan dalam sebuah blockchain dapat menyebabkan berbagai hal seperti biaya transaksi mahal, proses transaksi lambat, dan bahkan transaksi gagal. Blockchain generasi awal seperti Bitcoin dan Ethereum hanya dapat memproses sejumlah transaksi dalam satu waktu.
- 💻 Skalabilitas: Salah satu hambatan paling besar terhadap penggunaan massal blockchain adalah skalabilitas. Teknologi blockchain sendiri masih dalam tahap perkembangan dan kita belum mengetahui apakah jaringannya dapat menahan beban saat digunakan oleh jutaan orang sekaligus dalam waktu bersamaan. Dalam hal ini, banyak teknologi blockchain baru berusaha memecahkan masalah skalabilitas dan kecepatan transaksi.

Materi TIDAK untuk Diperjual Belikan



TIPE-TIPE JARINGAN BLOCKCHAIN

Public Blockchain

- Public blockchain adalah tipe jaringan blockchain paling populer dan paling banyak digunakan. Ia adalah jaringan terbuka yang datanya dapat diakses siapa pun dan bebas digunakan. Blockchain jenis ini biasanya diamankan menggunakan metode konsensus proof-of-work (PoW) atau proof-of-stake (PoS). Selain itu, mayoritas public blockchain terdesentralisasi secara penuh dengan sejumlah node yang bertugas memproses transaksi.
- Public blockchain biasanya membutuhkan energi listrik yang sangat besar karena ia harus mampu memproses ribuan transaksi setiap detiknya. Contoh public blockchain: Bitcoin (BTC), Ethereum (ETH), dan Solana (SOL).

Private Blockchain

- Private blockchain adalah tipe jaringan blockchain terbatas yang dibuat oleh sebuah entitas. Jenis jaringan ini terbatas bagi mereka yang memiliki izin akses. Selain itu, private blockchain biasanya menggunakan sistem verifikasi yang tersentralisasi dan dikontrol oleh pembuat jaringan tersebut. Ia memiliki sistem tertutup yang biasanya didesain khusus untuk memenuhi tujuan tertentu. Private blockchain pada umumnya juga lebih cepat dan lebih stabil daripada public blockchain. Namun, sifatnya yang tersentralisasi membuatnya lebih rentan terhadap serangan pihak ketiga.
- Terakhir, private blockchain biasanya harus memenuhi semua izin dari pemerintah dan instansi negara tertentu. Ia juga bisa dibuat khusus untuk perusahaan tertentu yang membutuhkan sistem blockchain. Contoh private blockchain adalah Ripple (XRP).

Materi TIDAK untuk Diperjual Belikan

TIPE-TIPE JARINGAN BLOCKCHAIN



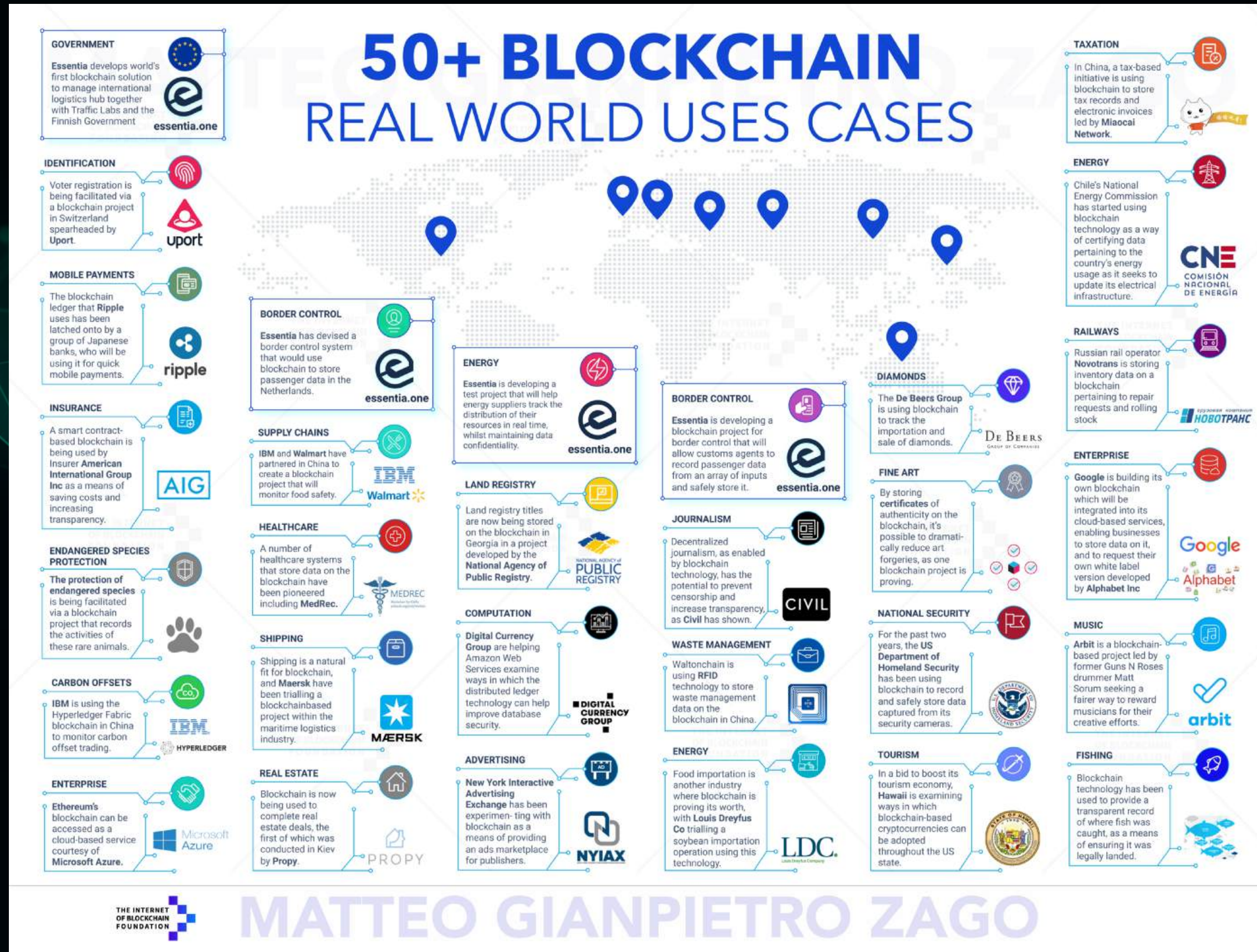
**Materi TIDAK
untuk Diperjual
Belikan**

	Public Blockchain	Private Blockchain
Otoritas	Terdesentralisasi	Bisa terpusat
Akses	Terbuka untuk publik, bisa diakses siapa saja	Jaringan hanya terbuka untuk pihak tertentu
Transaksi per detik	Lebih sedikit	Lebih banyak
Token asli	Ada	Tidak diperlukan
Kecepatan	Lebih lambat	Lebih cepat
Konsumsi energi	Tinggi	Sedikit
Risiko	Risiko penyerangan tinggi	Risiko penyerangan lebih rendah

MENGAPA BLOCKCHAIN PENTING ?



Materi TIDAK
untuk Diperjual
Belikan





MENGAPA BLOCKCHAIN PENTING ?

Penggunaan Teknologi Blockchain

Penggunaan teknologi blockchain pada dasarnya tidak terbatas. Teknologi ini pada dasarnya adalah fondasi penyimpanan data yang bisa digunakan untuk industri mana pun. Saat ini kita sudah melihat penerapan teknologi blockchain di luar industri finansial seperti identitas digital, industri data, musik, rantai pasokan, dan sektor kesehatan. Meskipun begitu, perkembangan dalam industri-industri tersebut masih terbatas.

Salah satu perkembangan pesat penggunaan teknologi blockchain adalah **CBDCs atau central bank digital currencies**. CBDCs adalah mata uang fiat yang dibangun di atas jaringan blockchain namun dikontrol oleh pemerintah yang membuatnya. Negara seperti Indonesia dan AS sedang dalam proses merencanakan dan membuat CBDCs.

**Sentralisasi
Vs
Desentralisasi
Vs
Terdistribusi**

Karakteristik	Sentralisasi	Desentralisasi	Terdistribusi
Definisi	Kontrol terpusat di satu titik atau entitas.	Kontrol tersebar di beberapa titik atau entitas.	Data dan kontrol tersebar di seluruh jaringan tanpa titik pusat.
Contoh	- Bank tradisional - Perusahaan besar	- Blockchain (misalnya, Bitcoin) - Organisasi otonom terdesentralisasi (DAO)	- Jaringan peer-to-peer (misalnya, BitTorrent) - Sistem file terdistribusi (misalnya, IPFS)
Keuntungan	- Kontrol yang lebih mudah - Pengambilan keputusan lebih cepat	- Tidak ada titik tunggal kegagalan - Meningkatkan keamanan dan ketahanan	- Skalabilitas tinggi - Kinerja yang lebih baik - Tidak ada titik tunggal kegagalan
Kelemahan	- Titik tunggal kegagalan - Risiko penyalahgunaan kekuasaan	- Pengambilan keputusan bisa lebih lambat - Koordinasi antar entitas bisa menantang	- Kompleksitas lebih tinggi dalam manajemen - Mungkin ada masalah konsistensi data
Skalabilitas	Dibatasi oleh kapasitas pusat	Bergantung pada jumlah node yang berpartisipasi	Sangat tinggi, dapat menambah node tanpa mengurangi kinerja
Keamanan	Rentan terhadap serangan di titik pusat	Lebih aman karena tidak ada titik tunggal kegagalan	Sangat aman karena data diduplikasi di seluruh jaringan
Kinerja	Bergantung pada kapasitas entitas pusat	Bisa lebih rendah dibandingkan sentralisasi karena perlu konsensus dari banyak entitas	Kinerja tinggi karena beban dibagi di seluruh jaringan
Ketahanan	Rentan terhadap kegagalan pusat	Tinggi, karena kegagalan satu node tidak mempengaruhi keseluruhan sistem	Sangat tinggi, kegagalan beberapa node tidak mempengaruhi keseluruhan sistem
Contoh Penerapan	- Server pusat - Pemerintah pusat	- Jaringan blockchain - Cryptocurrency	- Jaringan peer-to-peer - Cloud storage terdistribusi



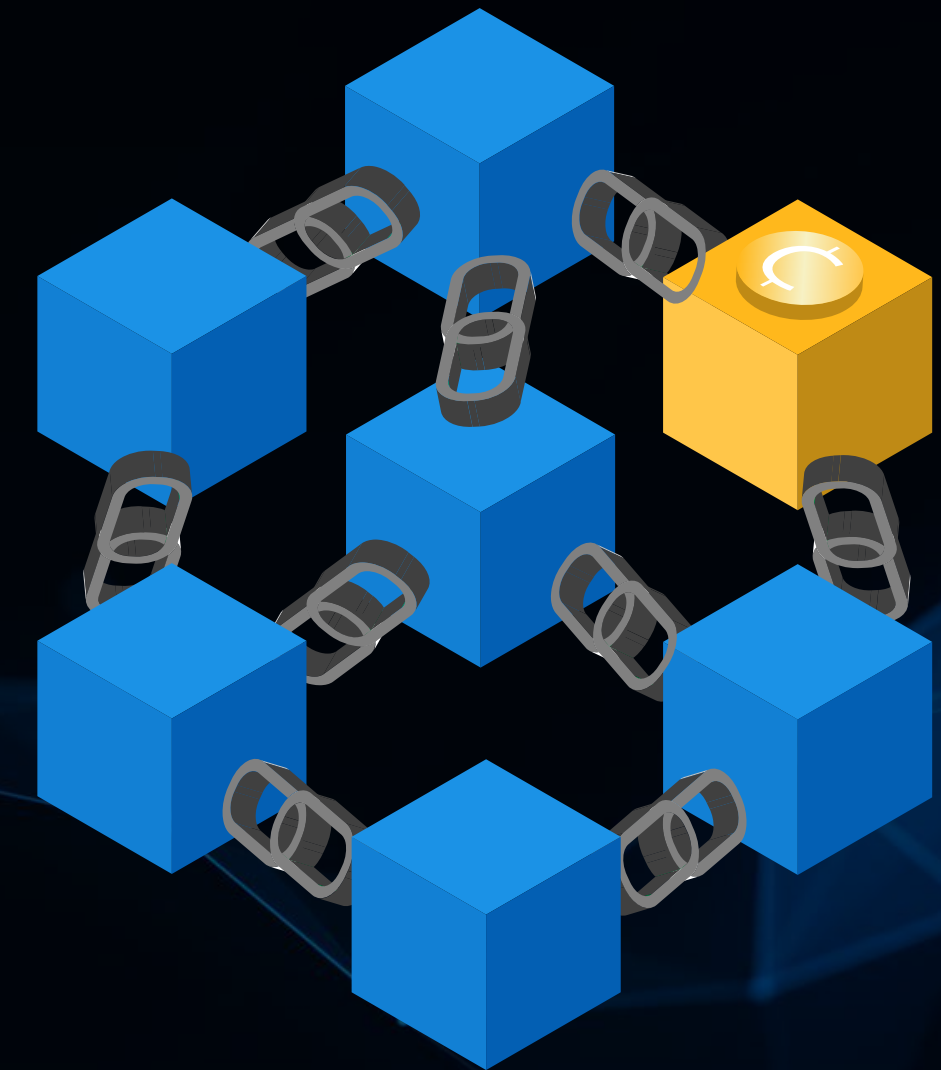
Sentralisasi Vs Desentralisasi Vs Terdistribusi



Data Terpusat



**Memiliki beberapa
node pusat**



**Tidak Terpusat (Data
Terdistribusi ke setiap node)**



Sentralisasi Vs Desentralisasi Vs Terdistribusi

- **Sentralisasi:** Sistem sentralisasi mengandalkan satu titik atau entitas pusat untuk kontrol dan pengambilan keputusan. Contoh umum adalah bank tradisional atau perusahaan besar di mana semua keputusan penting dibuat oleh pusat.
- **Desentralisasi:** Sistem desentralisasi membagi kontrol di antara beberapa entitas atau node. Misalnya, dalam blockchain, setiap node memiliki salinan dari seluruh data dan keputusan dibuat melalui konsensus.
- **Terdistribusi:** Sistem terdistribusi menyebarkan data dan kontrol di seluruh jaringan tanpa titik pusat. Ini sering digunakan dalam jaringan peer-to-peer dan sistem file terdistribusi di mana data diduplikasi di seluruh node untuk meningkatkan keandalan dan kinerja.

BITCOIN

Bitcoin (BTC) adalah mata uang kripto (mata uang virtual) yang dirancang untuk bertindak sebagai uang dan bentuk pembayaran di luar kendali satu orang, kelompok, atau entitas. Hal ini menghilangkan kebutuhan akan keterlibatan pihak ketiga yang tepercaya (misalnya, percetakan uang atau bank) dalam transaksi keuangan. Bitcoin diberikan kepada penambang blockchain yang memverifikasi transaksi dan dapat dibeli di beberapa bursa.

Bitcoin diperkenalkan ke publik pada tahun 2009 oleh seorang pengembang anonim atau sekelompok pengembang yang menggunakan nama Satoshi Nakamoto. Sejak saat itu, Bitcoin telah menjadi mata uang kripto paling terkenal dan terbesar di dunia. Popularitasnya telah menginspirasi pengembangan banyak mata uang kripto lainnya.

Materi TIDAK untuk Diperjual Belikan



SIAPA PENEMU BITCOIN?

Pada tahun 2008 nama domain .org dibeli dan sebuah white paper akademis berjudul Bitcoin: A Peer-to-Peer Electronic Cash System diunggah. White paper tersebut memaparkan teori dan desain sistem mata uang digital yang bebas dari kendali organisasi atau pemerintah mana pun.

Penulisnya, yang menggunakan nama Satoshi Nakamoto , menulis: "Akar masalah dengan mata uang konvensional adalah semua kepercayaan yang dibutuhkan untuk membuatnya berfungsi. Bank sentral harus dipercaya untuk tidak merendahkan nilai mata uang, tetapi sejarah mata uang fiat penuh dengan pelanggaran kepercayaan itu."

Tahun berikutnya perangkat lunak yang dijelaskan dalam makalah tersebut selesai dan dirilis ke publik, meluncurkan jaringan bitcoin pada tanggal 9 Januari 2009.

Nakamoto terus mengerjakan proyek tersebut dengan berbagai pengembang hingga tahun 2010 ketika ia mengundurkan diri dari proyek tersebut dan membiarkannya berjalan sendiri. Identitas asli Nakamoto tidak pernah terungkap dan mereka tidak pernah membuat pernyataan publik apa pun selama bertahun-tahun.

Kini perangkat lunak tersebut bersifat sumber terbuka, yang berarti siapa pun dapat melihat, menggunakan, atau berkontribusi pada kode tersebut secara gratis. Banyak perusahaan dan organisasi berupaya untuk meningkatkan perangkat lunak tersebut, termasuk MIT.

Materi TIDAK untuk Diperjual Belikan

FREQUENTLY ASKED QUESTIONS ABOUT BITCOIN

Bisakah bitcoin dikonversi menjadi uang tunai?

Bitcoin dapat ditukar dengan uang tunai seperti aset lainnya. Ada banyak bursa mata uang kripto daring tempat orang dapat melakukan ini, tetapi transaksi juga dapat dilakukan secara langsung atau melalui platform komunikasi apa pun , yang memungkinkan bahkan usaha kecil untuk menerima bitcoin. Tidak ada mekanisme resmi yang dibangun dalam bitcoin untuk mengonversi ke mata uang lain.

Tidak ada hal yang secara inheren berharga yang menjadi dasar jaringan bitcoin. Namun, hal ini berlaku untuk banyak mata uang nasional paling stabil di dunia sejak meninggalkan standar emas , seperti dolar AS dan pound Inggris.

Apa tujuan bitcoin?

Bitcoin diciptakan sebagai sarana bagi orang untuk mengirim uang melalui internet. Mata uang digital ini dimaksudkan untuk menyediakan sistem pembayaran alternatif yang beroperasi tanpa kendali pusat, tetapi dapat digunakan seperti mata uang tradisional.

FREQUENTLY ASKED QUESTIONS ABOUT BITCOIN

Materi TIDAK
untuk Diperjual
Belikan

Apakah Bitcoin Aman ?

Kriptografi dan Algoritma:

- Bitcoin menggunakan algoritma SHA-256 yang dirancang oleh Badan Keamanan Nasional AS.
- SHA-256 adalah algoritma kriptografi yang sangat aman, dan memecahkannya dianggap hampir mustahil.
- Jumlah kemungkinan kunci pribadi yang harus diuji untuk memecahkan SHA-256 lebih banyak dari jumlah atom di alam semesta, menjadikan serangan brute-force tidak praktis.

Kasus Peretasan:

- Peretasan yang terjadi umumnya menargetkan bursa atau layanan penyimpanan pihak ketiga, bukan jaringan Bitcoin itu sendiri.
- Bursa sering kali menyimpan mata uang digital atas nama pelanggan, dan keamanan mereka bisa menjadi target peretasan.

Serangan 51%:

- Dalam teori, jika seorang penyerang dapat mengendalikan lebih dari 50% dari seluruh daya komputasi jaringan Bitcoin, mereka bisa mengendalikan blockchain dan memanipulasi transaksi.
- Namun, seiring bertambahnya jumlah node, serangan ini menjadi semakin sulit dan tidak praktis karena membutuhkan sumber daya komputasi yang sangat besar.

FREQUENTLY ASKED QUESTIONS ABOUT BITCOIN

Tidak Ada Otoritas Pusat:

- Salah satu risiko dalam menggunakan Bitcoin adalah ketiadaan otoritas pusat. Jika pengguna melakukan kesalahan seperti mengirim Bitcoin ke alamat yang salah atau kehilangan kunci pribadi, tidak ada pihak yang dapat membantu memulihkan dana tersebut.

Komputasi Kuantum:

- Komputasi kuantum dapat menjadi ancaman bagi keamanan kriptografi saat ini, termasuk Bitcoin.
- Komputer kuantum memiliki potensi untuk memecahkan kalkulasi matematika yang mendasari kriptografi dengan lebih cepat daripada komputer konvensional.
- Meskipun demikian, teknologi komputasi kuantum praktis masih dalam tahap pengembangan dan belum menjadi ancaman nyata bagi Bitcoin saat ini.

Ringkasan

Bitcoin memiliki sistem keamanan yang sangat kuat berbasis kriptografi SHA-256, yang saat ini tidak dapat dipecahkan oleh komputer konvensional. Meskipun ada risiko keamanan terkait dengan penggunaan layanan pihak ketiga seperti bursa, jaringan Bitcoin itu sendiri tetap aman. Namun, ketiadaan otoritas pusat berarti bahwa pengguna bertanggung jawab penuh atas keamanan kunci pribadi dan transaksi mereka. Ancaman dari komputasi kuantum tetap menjadi perhatian di masa depan, tetapi belum berdampak pada keamanan Bitcoin saat ini.

WHITE PAPER BITCOIN

1. Introduction

Masalah yang Dipecahkan:

- Sistem keuangan tradisional bergantung pada pihak ketiga tepercaya seperti bank untuk memproses pembayaran elektronik.
- Sistem ini memiliki kelemahan, seperti biaya transaksi yang tinggi dan ketidakmampuan untuk menghindari double-spending (pembelanjaan ganda).

Solusi:

- Satoshi Nakamoto mengusulkan sistem pembayaran elektronik peer-to-peer (P2P) yang memungkinkan transaksi langsung antara dua pihak tanpa memerlukan pihak ketiga tepercaya.
- Menggunakan bukti kriptografi dan jaringan peer-to-peer untuk mencatat transaksi pada blockchain, memastikan keamanan dan integritas data.

2. Transactions

Transaksi Bitcoin:

- Transaksi Bitcoin melibatkan transfer nilai bitcoin dari satu pihak ke pihak lain.
- Setiap transaksi ditandatangani secara kriptografi dengan kunci pribadi pengirim, memberikan bukti otentikasi dan integritas.
- Transaksi kemudian disiarkan ke jaringan dan divalidasi oleh node-node yang ada di jaringan tersebut.

WHITE PAPER BITCOIN

3. Timestamp Server

Server Cap Waktu:

- Menggunakan timestamp server untuk menandai data dengan cap waktu yang mencatat keberadaan data pada waktu tertentu.
- Setiap cap waktu memasukkan cap waktu sebelumnya dalam hash, membentuk rantai (chain) yang memastikan urutan kronologis dari transaksi.

4. Proof-of-Work

Mekanisme Proof-of-Work:

- Proof-of-Work (PoW) digunakan untuk mengamankan jaringan dengan memerlukan usaha komputasi yang signifikan untuk menambahkan blok baru ke blockchain.
- PoW mengharuskan penambang (miners) untuk menemukan nilai hash yang memenuhi persyaratan tertentu, memastikan bahwa blok baru valid dan menghindari modifikasi data sebelumnya.

5. Network

Proses Jaringan:

- Node-node di jaringan Bitcoin mengumpulkan transaksi baru dan membentuknya menjadi blok.
- Blok-blok ini disiarkan ke seluruh jaringan, di mana node-node lain memverifikasi validitas transaksi dan blok tersebut.
- Blok valid ditambahkan ke blockchain, membentuk catatan permanen dari transaksi.

WHITE PAPER BITCOIN

6. Incentive

Insentif untuk Penambang:

- Penambang diberikan insentif dalam bentuk bitcoin baru yang dihasilkan serta biaya transaksi dari transaksi yang mereka validasi.
- Insentif ini memotivasi penambang untuk mendukung keamanan dan kelangsungan jaringan.

7. Reclaiming Disk Space

Penghematan Ruang Disk:

- Menggunakan pohon Merkle untuk memungkinkan penyimpanan yang lebih efisien.
- Hanya cabang-cabang pohon yang relevan yang perlu disimpan, bukan seluruh rantai blok, sehingga menghemat ruang penyimpanan.

8. Simplified Payment Verification (SPV)

Verifikasi Pembayaran Sederhana:

- Pengguna dapat memverifikasi transaksi tanpa harus menjalankan node penuh dengan hanya mengunduh header blok dari blockchain.
- SPV memungkinkan pengguna untuk memverifikasi bahwa transaksi mereka termasuk dalam blok yang valid tanpa memerlukan seluruh riwayat blockchain.

WHITE PAPER BITCOIN

9. Combining and Splitting Value

Penggabungan dan Pemisahan Nilai:

- Transaksi dapat menggabungkan beberapa input dan menghasilkan beberapa output, memberikan fleksibilitas dalam mengelola nilai bitcoin.
- Ini memungkinkan pengguna untuk memecah atau menggabungkan nilai sesuai kebutuhan mereka.

10. Privacy

Privasi dalam Transaksi:

- Identitas pengguna Bitcoin tetap anonim selama alamat publik mereka tidak terkait dengan identitas di luar jaringan.
- Setiap transaksi menggunakan pasangan kunci kriptografi yang berbeda, meningkatkan privasi dan keamanan pengguna.

11. Calculation

Perhitungan Keamanan:

- Menggunakan probabilitas untuk memastikan integritas blockchain. Blok-blok yang valid bertambah seiring waktu, membuat modifikasi data sebelumnya menjadi semakin sulit.
- Semakin panjang rantai blok, semakin sulit untuk memodifikasinya, memberikan keamanan yang lebih tinggi.

WHITE PAPER BITCOIN

12. Conclusion

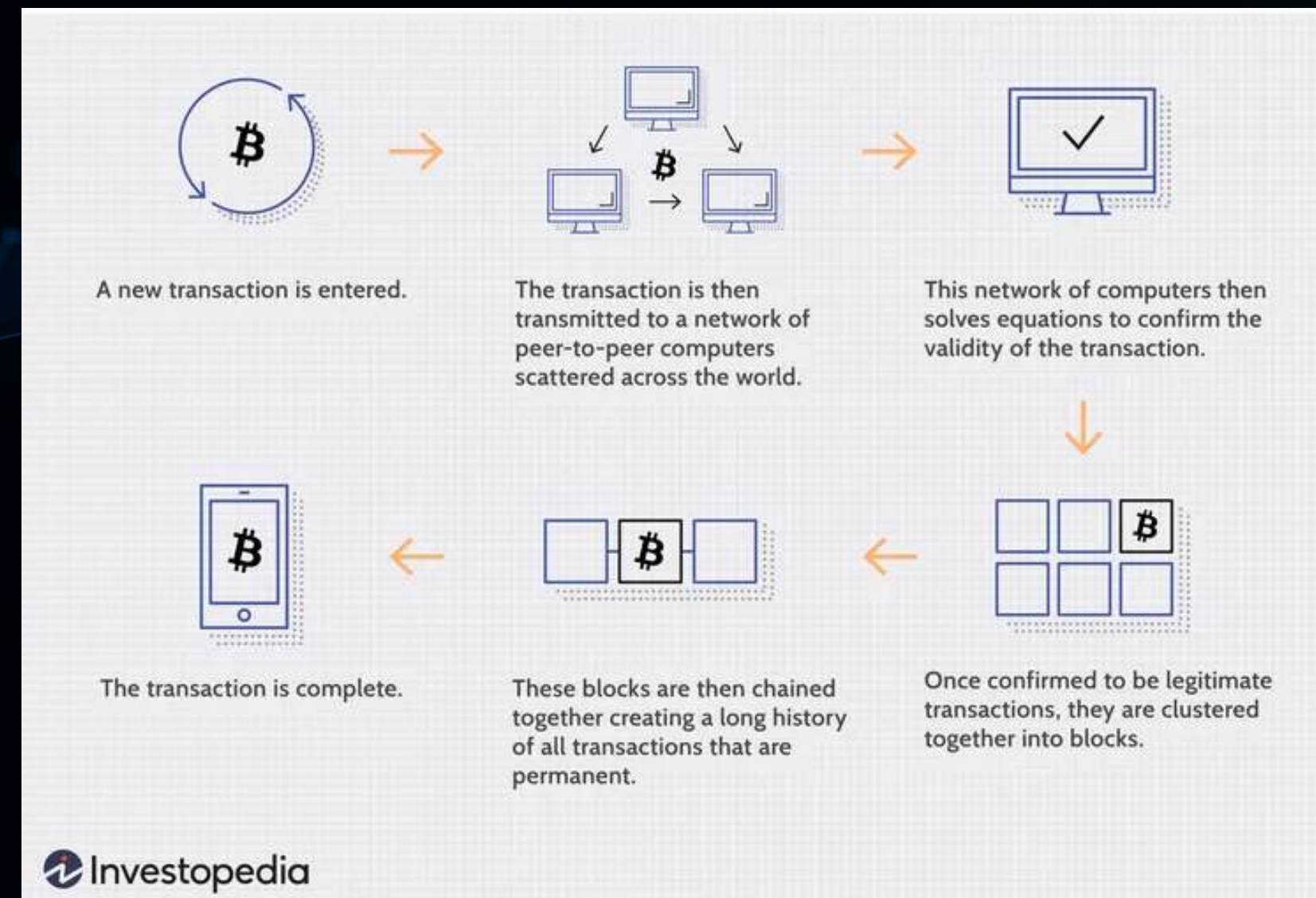
Kesimpulan:

- Bitcoin adalah sistem pembayaran elektronik peer-to-peer yang aman dan dapat diandalkan, mengatasi masalah double-spending tanpa memerlukan pihak ketiga yang terpercaya.
- Dengan menggunakan jaringan peer-to-peer dan bukti kriptografi, Bitcoin memberikan solusi inovatif untuk sistem keuangan digital.

PROSES TRANSAKSI

Transaksi mengikuti proses tertentu, tergantung pada blockchain tempat transaksi tersebut terjadi. Misalnya, pada blockchain Bitcoin, jika Anda memulai transaksi menggunakan dompet cryptocurrency Anda—aplikasi yang menyediakan antarmuka untuk blockchain—itu memulai serangkaian peristiwa.

Pada Bitcoin, transaksi Anda dikirim ke memory pool, tempat transaksi disimpan dan diantre hingga seorang penambang mengambilnya. Setelah transaksi dimasukkan ke dalam sebuah blok dan blok tersebut penuh dengan transaksi, blok tersebut ditutup, dan proses penambangan dimulai.



Setiap node dalam jaringan mengusulkan blok mereka sendiri karena mereka memilih transaksi yang berbeda. Masing-masing bekerja pada blok mereka sendiri, mencoba menemukan solusi untuk target kesulitan dengan menggunakan "nonce," singkatan dari "number used once" (angka yang digunakan sekali).

Nilai nonce adalah bidang dalam header blok yang dapat diubah, dan nilainya meningkat secara bertahap setiap kali mencoba. Setiap penambang mulai dengan nonce bernilai nol. Jika hash yang dihasilkan tidak sama dengan atau kurang dari target hash, nilai satu ditambahkan ke nonce, hash baru dihasilkan, dan seterusnya. Nonce berulang sekitar setiap 4,5 miliar percobaan (yang memakan waktu kurang dari satu detik) dan menggunakan nilai lain yang disebut extra nonce sebagai penghitung tambahan. Ini berlanjut sampai seorang penambang menghasilkan hash yang valid, memenangkan perlombaan, dan menerima hadiah.

Menghasilkan hash-hash ini hingga nilai tertentu ditemukan adalah "proof-of-work" yang sering Anda dengar—itu "membuktikan" bahwa penambang telah melakukan pekerjaan. Jumlah pekerjaan yang dibutuhkan untuk memvalidasi hash adalah alasan mengapa jaringan Bitcoin mengkonsumsi begitu banyak daya komputasi dan energi.

Setelah sebuah blok ditutup, transaksi dianggap selesai. Namun, blok tersebut tidak dianggap dikonfirmasi sampai lima blok lainnya telah divalidasi. Konfirmasi memerlukan waktu sekitar satu jam untuk diselesaikan oleh jaringan karena rata-rata membutuhkan waktu kurang dari 10 menit per blok (blok pertama dengan transaksi Anda dan lima blok berikutnya dikalikan 10 menit sama dengan 60 menit).

Tidak semua blockchain mengikuti proses ini. Misalnya, jaringan Ethereum secara acak memilih satu validator dari semua pengguna yang memiliki ether yang di-stake untuk memvalidasi blok, yang kemudian dikonfirmasi oleh jaringan. Proses ini jauh lebih cepat dan tidak memerlukan banyak energi dibandingkan proses Bitcoin.



CRYPTOCURRENCY

Secara terminologis, cryptocurrency adalah kombinasi kata crypto dan currency. Kata "crypto" berasal dari "cryptography" dengan arti kode rahasia. Sedangkan kata "currency" berasal dari bahasa Inggris berarti mata uang. Dengan demikian, cryptocurrency adalah uang elektronik dibuat berdasarkan teknologi kriptografi, dengan kode kepemilikan dirahasiakan bagi para pemiliknya saja.

**Materi TIDAK
untuk Diperjual
Belikan**

KARAKTERISTIK CRYPTOCURRENCY

Digital

- Pertama, karakteristik cryptocurrency adalah digital. Mata uang ini tidak memiliki wujud nyata seperti uang kertas atau koin, sehingga tidak bisa dipegang. Oleh karena itu, cryptocurrency adalah mata uang yang hanya bisa digunakan di dunia maya.

Peer-to-peer Transaction

- Transaksi menggunakan cryptocurrency terjadi dari satu orang ke orang lainnya secara virtual. Proses transaksi cryptocurrency adalah dengan meneruskan dari pengirim ke penerima secara online, tanpa ada pertemuan langsung antar pihak terlibat dalam transaksi.

Global

- Selanjutnya, karakteristik cryptocurrency adalah berlaku secara global. Berbeda dengan mata uang fisik yang transaksinya terbatas, cryptocurrency bisa digunakan di mana saja tanpa ada batas negara dan perbedaan harga karena kurs.

KARAKTERISTIK CRYPTOCURRENCY

Encrypted

- Karakteristik selanjutnya cryptocurrency adalah encrypted atau terenkripsi. Saat bertransaksi di dunia blockchain, Anda tidak bisa mengetahui siapa pemilik cryptocurrency sebenarnya, karena identitas pemilik telah dilindungi kode rahasia.

Decentralized

- Transaksi cryptocurrency terjadi tanpa melibatkan pihak penengah. Masing-masing pengguna bertanggung jawab atas transaksinya masing-masing, tanpa ada pihak pelindungnya. Oleh karena itu, saat terjadi kerugian di dunia blockchain, pemilik cryptocurrency tidak dapat menuntut ke lembaga keuangan manapun.

Truthless

- Terakhir, karakteristik cryptocurrency adalah truthless. Dalam transaksi mata uang digital ini, Anda tidak bisa mempercayakan saldo crypto pada suatu pihak atau lembaga seperti bank. Satu-satunya cara menyimpan uang crypto Anda adalah dengan memanfaatkan akun e-wallet dari provider transaksi atau membuat penyimpanan Anda sendiri.

FUNGSI CRYPTOCURRENCY

1. Membeli barang atau jasa

Saat ini, ada banyak toko yang mulai memberlakukan cryptocurrency sebagai alat pembayarannya, termasuk dua perusahaan ternama Overstock dan Newegg.

Kamu juga bisa menggunakan cryptocurrency di banyak restoran, hotel, penerbangan, aplikasi, dan bar. Bahkan, dikutip dari [Cointelegraph](#), ada perguruan tinggi yang juga sudah memberlakukan cryptocurrency.

Namun, kebanyakan perusahaan tersebut baru menerima Bitcoin.

2. Investasi

Fungsi cryptocurrency lainnya adalah investasi.

Pada awal cryptocurrency populer, harganya terus meningkat tajam. Tak heran banyak orang 'mendadak kaya' setelah investasi melalui cryptocurrency.

Prinsipnya kurang lebih sama dengan prinsip ekonomi, yaitu harga akan naik ketika ada banyak permintaan.

Semakin banyak orang melakukan investasi dengan cryptocurrency, maka harganya juga akan semakin naik. Namun, belakangan kenaikan harga mata uang digital tersebut tidak signifikan beberapa tahun silam.

Investasi dengan cryptocurrency juga termasuk dalam kategori high risk.

FUNGSI CRYPTOCURRENCY

3. Mining

Mining atau pertambangan merupakan hal penting dalam cryptocurrency.

Pada dasarnya, pengguna harus memecahkan teka-teki cryptography yang rumit untuk mengonfirmasi transaksi dan mencatatnya dalam blockchain.

Teka-teki tersebut bisa dipecahkan dengan cara mining. Semakin besar daya komputasi pengguna, maka semakin besar pula peluang mereka untuk memecahkannya.

Jika berhasil memecahkan teka-teki tersebut, kamu akan menerima hadiah sebagai biaya transaksi.

JENIS-JENIS CRYPTOCURRENCY

Bitcoin

- Bitcoin adalah jenis cryptocurrency paling pertama dan populer di kalangan investor crypto. Mata uang satu ini diciptakan pada tahun 2008 oleh seorang persona internet bernama Satoshi Nakamoto. Pada awalnya, harga cryptocurrency bitcoin dipatok sebesar \$1 per keping. Akan tetapi, saat ini harganya sudah melambung menjadi \$20 ribu per kepingnya.

Altcoin

- Altcoin adalah jenis cryptocurrency sebagai sebutan yang mengacu pada koin apapun kecuali Bitcoin. Kata "altcoin" berarti "alternatif dari Bitcoin". Seperti yang diketahui bahwa bitcoin memiliki komputasi matematika yang rumit. Nah altcoin diciptakan sebagai bentuk sederhana dari bitcoin. Hingga saat ini, ada ratusan merk altcoin telah dibuat, seperti Peercoin, Litecoin, Dogecoin, Auroracoin, dan Namecoin.

JENIS-JENIS CRYPTOCURRENCY

Token

- Selanjutnya, jenis cryptocurrency adalah token. Tidak seperti altcoin, token dibuat dan diberikan melalui Penawaran Koin Awal (ICO). Bentuk penawarannya sama seperti penawaran saham. Token dapat direpresentasikan seperti Token nilai (Bitcoin), Token keamanan (untuk melindungi akun Anda), dan Token utilitas (ditunjuk untuk penggunaan tertentu).

Government Currency

- Terakhir, jenis cryptocurrency adalah government cryptocurrency. Jenis ini merupakan cryptocurrency yang dikeluarkan atau diresmikan oleh pemerintah di suatu negara. Belum banyak negara memiliki government crypto sendiri. Akan tetapi, Bank Indonesia baru-baru ini mengumumkan sedang merencanakan pembuatan BI Crypto.

PERBEDAAN BLOCKCHAIN BITCOIN CRYPTOCURRENCYS

Karakteristik	Blockchain	Bitcoin	Cryptocurrency
Definisi	Teknologi dasar yang digunakan untuk mencatat transaksi dalam buku besar digital yang terdesentralisasi.	Cryptocurrency pertama yang dibuat menggunakan teknologi blockchain.	Mata uang digital yang menggunakan teknologi kriptografi untuk keamanan dan biasanya dibangun di atas teknologi blockchain.
Fungsi Utama	Menyediakan platform untuk mencatat transaksi dengan cara yang aman, transparan, dan tidak dapat diubah.	Bertindak sebagai mata uang digital yang dapat digunakan untuk transaksi peer-to-peer.	Bertindak sebagai alat tukar, penyimpan nilai, dan unit akun dalam bentuk digital.
Pencipta	Dikembangkan oleh berbagai ilmuwan komputer dan kriptografer, konsep pertama kali oleh Stuart Haber dan Scott Stornetta.	Diciptakan oleh seseorang atau kelompok dengan nama samaran Satoshi Nakamoto pada tahun 2009.	Diciptakan oleh berbagai individu dan organisasi setelah keberhasilan Bitcoin, termasuk Ethereum, Ripple, Litecoin, dan lainnya.
Penggunaan	Digunakan dalam berbagai aplikasi seperti mata uang digital, smart contracts, supply chain management, voting systems, dll.	Digunakan terutama sebagai mata uang digital dan alat investasi.	Digunakan dalam berbagai konteks, termasuk sebagai alat pembayaran, investasi, token utilitas untuk aplikasi tertentu, dan lainnya.

PERBEDAAN BLOCKCHAIN BITCOIN CRYPTOCURRENCYS

Desentralisasi	Ya, tergantung pada implementasi, tetapi umumnya terdesentralisasi.	Ya, sepenuhnya terdesentralisasi.	Sebagian besar terdesentralisasi, tetapi beberapa cryptocurrency dapat memiliki tingkat sentralisasi yang lebih tinggi (misalnya, Ripple).
Keamanan	Menggunakan teknik kriptografi untuk memastikan data tidak dapat diubah dan transaksi diverifikasi.	Menggunakan proof-of-work (PoW) untuk keamanan dan validasi transaksi.	Menggunakan berbagai mekanisme keamanan, termasuk proof-of-work (PoW), proof-of-stake (PoS), dan algoritma konsensus lainnya.
Nilai	Tidak memiliki nilai moneter; nilai berasal dari aplikasi dan penggunaan teknologi.	Memiliki nilai moneter yang berfluktuasi berdasarkan permintaan pasar.	Nilai bervariasi tergantung pada jenis cryptocurrency dan permintaan pasar.
Contoh	Bitcoin blockchain, Ethereum blockchain, Hyperledger Fabric, dll.	Bitcoin	Ethereum (ETH), Ripple (XRP), Litecoin (LTC), Binance Coin (BNB), dan banyak lagi.
Ekosistem	Melibatkan pengembang, validator, pengguna, dan entitas yang membangun aplikasi di atas platform blockchain.	Melibatkan penambang, pengguna, pengembang, dan berbagai layanan terkait seperti dompet dan bursa.	Melibatkan pengembang, pengguna, validator, bursa, dan berbagai layanan terkait seperti dompet digital, layanan DeFi, dan platform perdagangan.

MASA DEPAN BLOCKCHAIN DAN CRYPTOCURRENCY

Tren dan Perkembangan Terkini dalam Teknologi Blockchain dan Cryptocurrency

1. DeFi (Decentralized Finance):

- Pertumbuhan pesat dalam aplikasi keuangan terdesentralisasi yang memungkinkan pengguna melakukan transaksi keuangan seperti pinjaman, tabungan, dan perdagangan tanpa perantara tradisional.

2. NFT (Non-Fungible Tokens):

- Meningkatnya popularitas NFT sebagai cara untuk mewakili kepemilikan aset digital unik, seperti karya seni, musik, dan item dalam game.

3. CBDC (Central Bank Digital Currency):

- Bank sentral di berbagai negara sedang mengeksplorasi dan mengembangkan mata uang digital mereka sendiri untuk meningkatkan efisiensi sistem pembayaran.

4. Enterprise Blockchain:

- Adopsi teknologi blockchain oleh perusahaan untuk meningkatkan transparansi, efisiensi, dan keamanan dalam rantai pasokan, logistik, dan berbagai operasi bisnis lainnya.

5. Regulasi:

- Peningkatan upaya regulasi oleh pemerintah di seluruh dunia untuk mengatur dan mengawasi penggunaan cryptocurrency dan teknologi blockchain.

MASA DEPAN BLOCKCHAIN DAN CRYPTOCURRENCY

Potensi dan Tantangan di Masa Depan

1. Adopsi Massal:

- Potensi: Blockchain dapat meningkatkan efisiensi dan transparansi di berbagai sektor, termasuk keuangan, kesehatan, logistik, dan pemerintahan.
- Tantangan: Masalah regulasi, ketidakpastian hukum, dan kurangnya pemahaman umum dapat menghambat adopsi massal.

2. Skalabilitas:

- Potensi: Solusi seperti sharding dan layer 2 dapat meningkatkan kapasitas jaringan blockchain untuk menangani lebih banyak transaksi per detik.
- Tantangan: Mengatasi batasan skalabilitas tanpa mengorbankan desentralisasi dan keamanan tetap menjadi tantangan besar.

3. Interoperabilitas:

- Potensi: Pengembangan protokol interoperabilitas memungkinkan berbagai blockchain untuk berkomunikasi dan bertransaksi satu sama lain, memperluas ekosistem dan penggunaan.
- Tantangan: Standarisasi protokol dan teknologi yang berbeda dapat menjadi hambatan besar.

MASA DEPAN BLOCKCHAIN DAN CRYPTOCURRENCY

Potensi dan Tantangan di Masa Depan Adopsi Blockchain 3.0 dan Teknologi Terkait

Sharding:

- Teknik untuk membagi blockchain menjadi bagian-bagian lebih kecil yang dapat diproses secara paralel, meningkatkan kapasitas dan kecepatan jaringan.

Proof of Stake (PoS):

- Metode konsensus yang menggantikan proof of work, di mana validator dipilih berdasarkan jumlah cryptocurrency yang mereka "stake" atau taruh sebagai jaminan. PoS lebih hemat energi dan dapat meningkatkan skalabilitas.

Layer 2 Solutions:

- Teknologi yang dibangun di atas blockchain utama untuk mengurangi beban transaksi dan meningkatkan kecepatan dan efisiensi. Contoh populer adalah Lightning Network untuk Bitcoin dan Rollups untuk Ethereum.

Smart Contracts yang Lebih Canggih:

- Pengembangan kontrak pintar yang lebih kompleks dan fungsional, memungkinkan otomatisasi lebih banyak proses bisnis dan aplikasi.

Integrasi dengan Teknologi Lain:

- Integrasi blockchain dengan teknologi seperti Internet of Things (IoT), Artificial Intelligence (AI), dan Big Data untuk menciptakan solusi yang lebih inovatif dan efisien.

**“EVEN
MIRACLES TAKE
A LITTLE TIME.”**

- THE FAIRY GODMOTHER, CINDERELLA

Materi TIDAK untuk Diperjual Belikan



THANK YOU!

Materi TIDAK untuk Diperjual Belikan

SOURCES :

[HTTPS://WWW.INVESTOPEDIA.COM/TERMS/B/BLOCKCHAIN.ASP](https://www.investopedia.com/terms/b/blockchain.asp)

[HTTPS://PINTU.CO.ID/ACADEMY/POST/BAGAIMANA-CARA-KERJA-BLOCKCHAIN](https://pintu.co.id/academy/post/bagaimana-cara-kerja-blockchain)

[HTTPS://WWW.NEWSCIENTIST.COM/DEFINITION/BITCOIN/](https://www.newscientist.com/definition/bitcoin/)

[HTTPS://WWW.INVESTOPEDIA.COM/TERMS/B/BITCOIN.ASP](https://www.investopedia.com/terms/b/bitcoin.asp)

[HTTPS://GLINTS.COM/ID/LOWONGAN/CRYPTOCURRENCY-ADALAH/](https://glints.com/id/lowongan/cryptocurrency-adalah/)

[HTTPS://WWW.OCBC.ID/ID/ARTICLE/2021/06/07/CRYPTOCURRENCY-ADALAH](https://www.ocbc.id/id/article/2021/06/07/cryptocurrency-adalah)