Mengenal Blockchain: Teknologi dibelakang Bitcoin

Husni@Trunojoyo.ac.id

Apa Itu Blockchain?

Dalam bahasa yang sederhana, Blockchain dapat didefinisikan sebagai suatu rantai blok (*chain of the block*) yang mengandung informasi. Teknik ini digunakan untuk men*timestamp* dokumen digital sehingga tidak mungkin untuk mem*backdate atau merubahnya*.

Blockchain digunakan untuk mengamankan transfer item-item seperti uang, properti, kontrak, tanpa memerlukan perantara pihak ketiga seperti Bank atau Pemerintah. Begitu data direkam ke dalam suatu blockchain, maka sudah sangat sulit untuk mengubahnya.

Blockchain merupakan suatu protokol software (seperti SMTP untuk email). Namun, Blockchains tidak dapat berjalan tanpa Internet. Disebut pula meta-technology karena ia mempengaruhi teknologi lain. Blockchain tersusun dari beberapa bagian: database, aplikasi software, beberapa komputer yang terkoneksi, dll.

Beberapa kali diistilahkan sebagai Bitcoin Blockchain atau Ethereum Blockchain dan kadang-kadang mata uang virtual atau token digital lainnnya. Namun, sebagian besarnya berbicara mengenai buku besar terdistribusi (*distributed ledgers*).

Dalam tutorial ini, kita akan mempelajari:

- Apa itu Blockchain?
- Bukan Blockchain!
- Arsitektur Blockchain
- Bagaimana Transaksi Blockchain Bekerja?
- Mengapa kita membutuhkan Blockchain?
- Versi Blockchain
- Varian Blockchain
- Kasus Penggunaan Blockchain
- Kasus Penggunaan Nyata dari Blockchain
- Bitcoin cryptocurrency: Aplikasi Blockchain Paling Populer
- Blockchain vs. Basis Data Bersama
- Mitos tentang Blockchain
- Keterbatasan teknologi Blockchain

Blockchain Bukanlah…

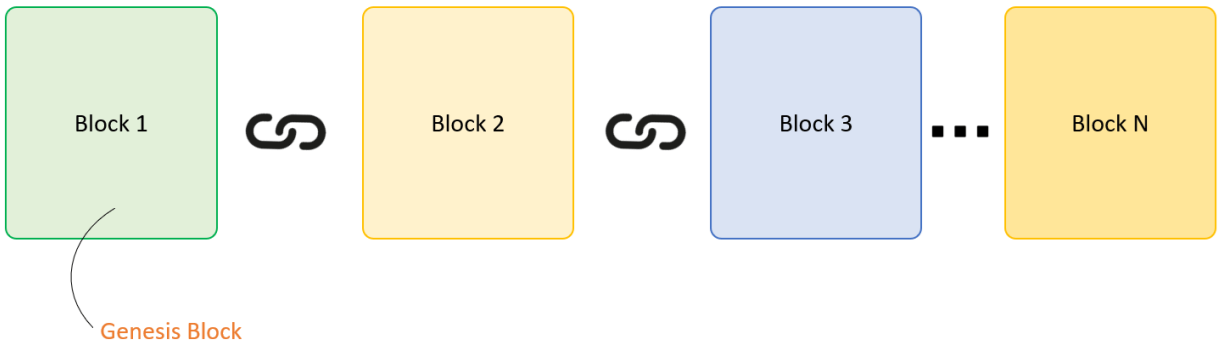
- Blockchain bukan Bitcoin, tetapi itu adalah teknologi di balik Bitcoin
- Bitcoin adalah token digital dan blockchain adalah buku besar untuk melacak siapa yang memiliki token digital
- Anda tidak dapat memiliki Bitcoin tanpa blockchain, tetapi Anda dapat memiliki blockchain tanpa Bitcoin.

Arsitektur Blockchain

Mari kita pelajari arsitektur Blockchain dengan memahami berbagai komponennya:

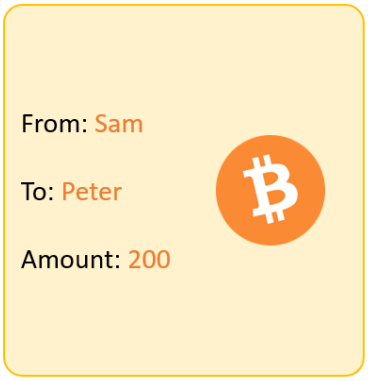
Apa itu Block?

Blockchain adalah rantai blok yang berisi data



Blockchain adalah rantai blok yang berisi informasi. Data yang disimpan di dalam blok tergantung pada jenis blockchain.

Misalnya, Blok Bitcoin berisi informasi tentang Pengirim, Penerima, jumlah bitcoin yang akan ditransfer.



Contoh Blok Bitcoin

Blok pertama dalam rantai disebut blok **Genesis** (Kejadian). Setiap blok baru dalam rantai terkait dengan blok sebelumnya.

Memahami SHA256 - Hash

Suatu blok juga memiliki hash. Ini dapat dipahami sebagai sidik jari yang unik untuk setiap blok. Ini mengidentifikasi blok dan semua isinya, dan selalu unik, seperti sidik jari. Jadi begitu sebuah blok dibuat, setiap perubahan di dalam blok tersebut akan menyebabkan hash berubah.

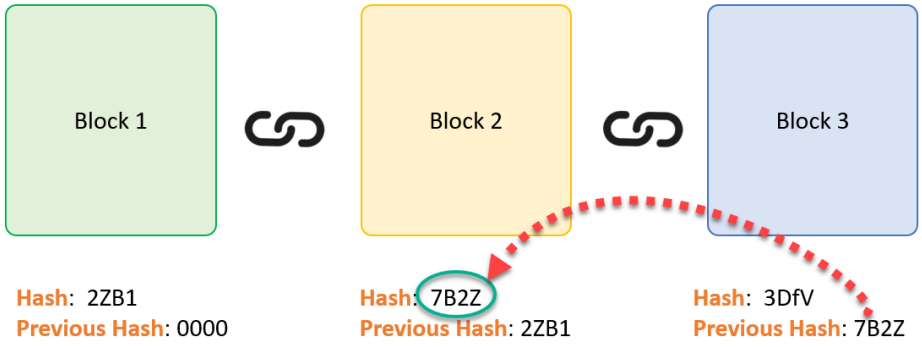
Hash bertindak sebagai sidik jari unik dari blok tersebut

Oleh karena itu, hash sangat berguna ketika Anda ingin mendeteksi perubahan pada persimpangan. Jika sidik jari suatu blok berubah, itu tidak tetap menjadi blok yang sama.

Setiap blok mempunyai

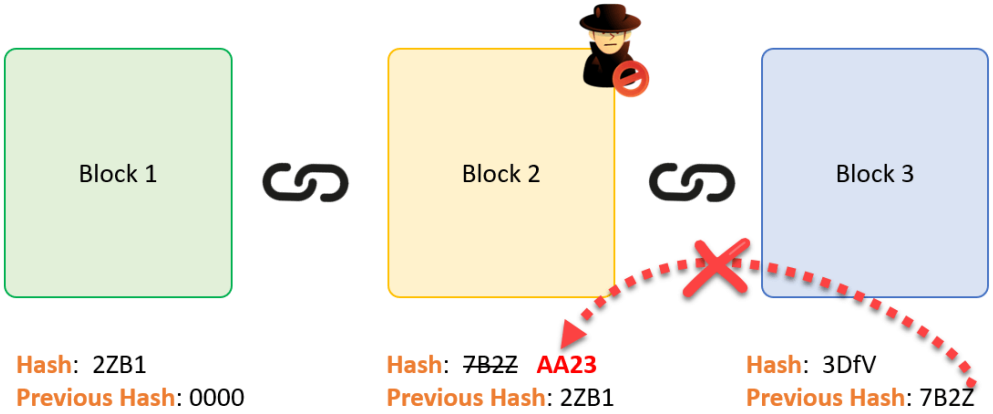
1. Data
2. Hash
3. Hash dari blok sebelumnya.

Pertimbangkan contoh berikut, di mana kita memiliki rantai 3 blok. Blok 1 tidak memiliki pendahulu. Oleh karena itu, tidak mengandung blok sebelumnya. Blok 2 berisi hash dari blok 1. Sedangkan blok 3 berisi hash dari blok 2.



Oleh karena itu, semua blok mengandung hash dari blok sebelumnya. Ini adalah teknik yang membuat blockchain sangat aman. Mari kita lihat cara kerjanya…

Asumsikan penyerang dapat mengubah data yang ada di Blok 2. Sejalan dengan itu, Hash dari Blok juga berubah. Tapi, Blok 3 masih berisi Hash lama dari Blok 2. Ini membuat Blok 3, dan semua blok berikutnya tidak valid karena mereka tidak memiliki hash yang benar dari blok sebelumnya.



Oleh karena itu, mengubah satu blok dapat dengan cepat membuat semua blok berikut tidak valid.

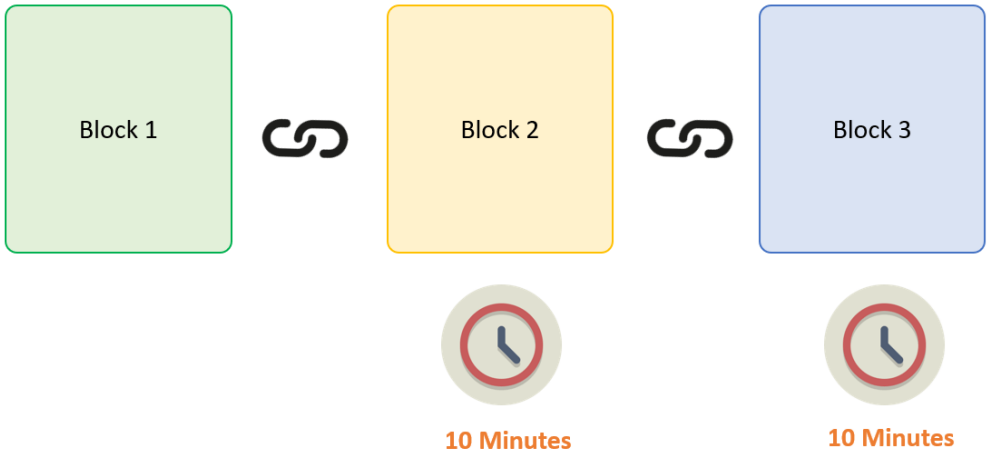
Proof-of-Work

Hash adalah mekanisme yang sangat baik untuk mencegah terjadinya perubahan tetapi komputer saat ini mempunyai kecepatan tinggi dan dapat menghitung ratusan ribu hash per detik. Dalam beberapa menit, penyerang dapat merusak blok, dan kemudian menghitung ulang semua hash blok lain untuk membuat blockchain valid lagi.

Untuk menghindari masalah ini, blockchains menggunakan konsep *proof-of-work*. Ini adalah mekanisme yang memperlambat pembuatan blok baru.

Suatu *proof-of-work* adalah masalah komputasi yang membutuhkan upaya penyelesaian tertentu. Tetapi waktu yang diperlukan untuk memverifikasi hasil dari masalah komputasi sangat kurang dibandingkan dengan upaya yang diperlukan untuk menyelesaikan masalah komputasi itu sendiri.

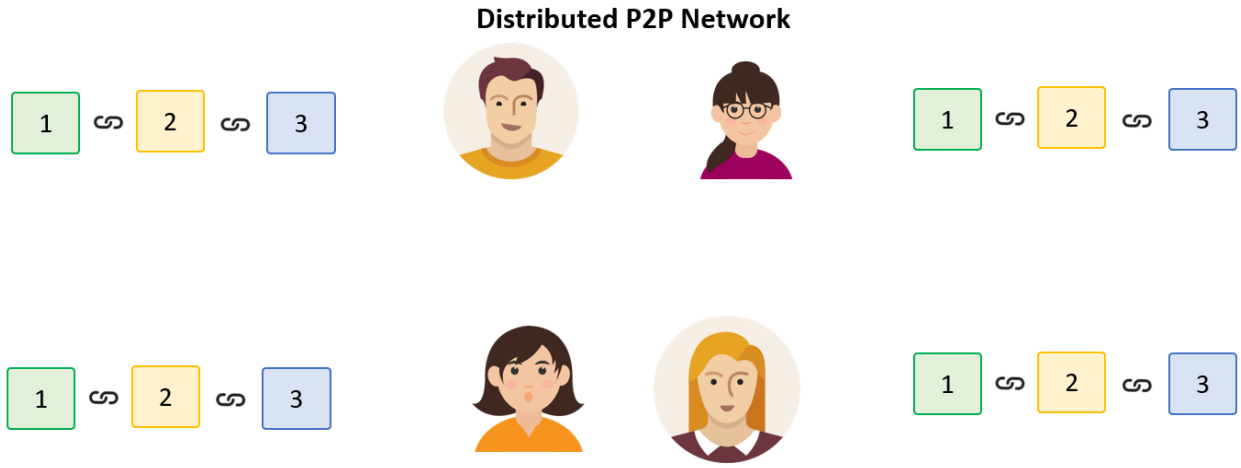
Dalam hal Bitcoin, dibutuhkan hampir 10 menit untuk menghitung bukti kerja yang diperlukan untuk menambahkan blok baru ke rantai. Mempertimbangkan contoh kita, jika seorang hacker ingin mengubah data di Blok 2, dia perlu melakukan bukti kerja (yang akan memakan waktu 10 menit) dan barulah kemudian membuat perubahan di Blok 3 dan semua blok sampai berhasil.



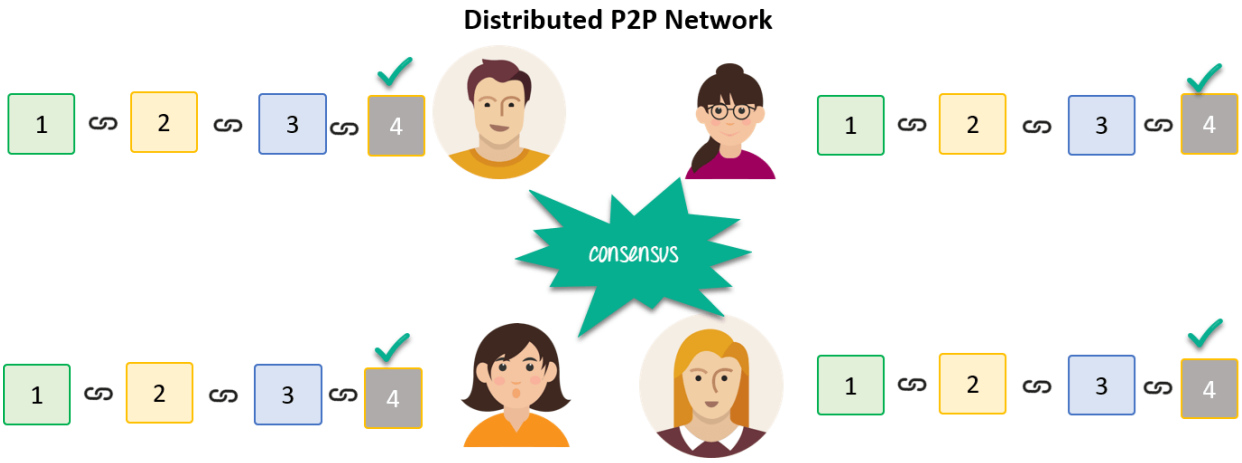
Mekanisme semacam ini membuatnya cukup sulit untuk merusak blok sehingga bahkan jika Anda mengutak-atik hanya satu blok, Anda perlu menghitung ulang bukti kerja untuk semua blok setelahnya. Jadi, mekanisme *hashing* dan *proof of work* membuat Blockchain dikatakan aman.

Jaringan P2P Terdistribusi

Namun, ada satu metode lagi yang digunakan oleh Blockchains untuk mengamankan dirinya secara mandiri, dan itu adalah dengan pendistribusian. Alih-alih menggunakan entitas pusat untuk mengelola rantai, Blockchains menggunakan jaringan peer-peer terdistribusi, dan semua orang diizinkan untuk bergabung. Ketika seseorang memasuki jaringan ini, ia akan mendapatkan salinan penuh dari Blockchain. Setiap komputer disebut node.



Mari kita lihat apa yang terjadi ketika pengguna membuat blok baru. Blok baru ini dikirim ke semua pengguna di jaringan. Setiap node perlu memverifikasi blok untuk memastikan bahwa itu belum diubah. Setelah selesai memeriksa, setiap node menambahkan blok ini ke Blockchain mereka.



Semua node di jaringan ini membuat konsensus. Mereka setuju tentang blok mana yang valid dan mana yang tidak. Node dalam jaringan akan menolak blok yang dirusak.

Jadi, untuk dapat berhasil mengutak-atik Blockchain:

1. Anda harus mengutak-atik semua blok pada rantai
2. Ulangi bukti kerja untuk setiap blok
3. Kendalikan lebih dari 50% dari jaringan *peer-to-peer*.

Setelah melakukan semua ini, blok Anda yang dirusak menjadi diterima oleh semua orang. Ini tentu hampir tugas yang mustahil. Karenanya, Blockchains sangat aman.

Bagaimana Transaksi Blockchain Bekerja?

- Langkah **1**) Beberapa orang meminta transaksi. Transaksi dapat melibatkan mata uang kripto, kontrak, catatan atau informasi lainnya.
- Langkah **2**) Transaksi yang diminta disiarkan ke jaringan P2P dengan bantuan node.
- Langkah **3**) Jaringan node memvalidasi transaksi dan status pengguna dengan bantuan algoritma yang dikenal.
- Langkah **4**) Setelah transaksi selesai, blok baru kemudian ditambahkan ke Blockchain yang ada. Sedemikian rupa sehingga permanen dan tidak dapat diubah.

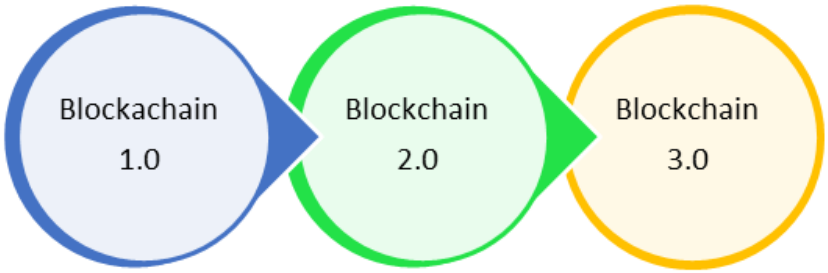
Mengapa kita membutuhkan Blockchain?

Di sini, ada beberapa alasan mengapa teknologi Blockchain menjadi sangat populer.

- ***Resilience* (tangguh):** Blockchain sering berupa arsitektur direplikasi. Rantai masih tetap beroperasi dengan sebagian besar node jika terjadi serangan besar-besaran terhadap sistem.
- **Reduksi Waktu:** Dalam industri keuangan, blockchain dapat memainkan peranyang vital dengan memungkinkan penyelesaian perdagangan lebih cepat karena tidak memerlukan proses verifikasi, penyelesaian dan perijinan yang panjang karena suatu versi tunggal dari data yang disepakati dari share ledger tersedia di antara semua stack holders.
- **Reliabilitas:** Blockchain mengesahkan dan memverifikasi identitas pihak yang berkepentingan. Ini menghapus catatan ganda, mengurangi tarif dan mempercepat transaksi.
- **Transaksi Tidak dapat diubah:** Dengan mendaftarkan transaksi dalam urutan kronologis, Blockchain mengesahkan ketidakterbalikan (*unalterability*), dari semua operasi yang berarti ketika ada blok baru yang ditambahkan ke rantai buku besar, itu tidak dapat dihapus atau dimodifikasi..
- **Pencegahan *Fraud*:** Konsep informasi dan konsensus bersama (*shared*) mencegah kemungkinan kerugian karena penipuan atau penggelapan. Dalam industri berbasis logistik, blockchain sebagai mekanisme pemantauan bertindak untuk mengurangi biaya.
- **Keamanan:** Menyerang database tradisional adalah menjatuhkan target tertentu. Dengan bantuan Teknologi Ledger Terdistribusi, masing-masing pihak memegang salinan dari rantai asli, sehingga sistem tetap beroperasi, bahkan dikala sejumlah besar node lainnya jatuh.
- **Transparansi:** Perubahan pada blockchain publik dapat dilihat secara publik oleh semua orang. Ini menawarkan transparansi yang lebih besar, dan semua transaksi tidak dapat diubah (*immutable*).

- **Kolaborasi:** Mengizinkan para pihak untuk bertransaksi secara langsung satu sama lain tanpa perlu memediasi pihak ketiga.
- **Desentralisasi:** Ada aturan standar tentang bagaimana setiap node bertukar informasi blockchain. Metode ini memastikan bahwa semua transaksi divalidasi, dan semua transaksi yang valid ditambahkan satu per satu.

Versi Blockchain



1. **Blockchain 1.0: Currency** (mata uang)

   Implementasi dari DLT (*distributed ledger technology*) mengarah ke aplikasi pertama dan nyata: *cryptocurrencies*. Ini memungkinkan transaksi keuangan berdasarkan pada teknologi blockchain. Ini digunakan dalam mata uang dan pembayaran. Bitcoin adalah contoh paling menonjol di segmen ini.

2. **Blockchain 2.0: Kontrak Pintar**

   Konsep-konsep kunci yang baru adalah Smart Contracts, program komputer kecil yang "hidup" di blockchain. Itu adalah program komputer gratis yang dijalankan secara otomatis, dan memeriksa kondisi yang ditentukan sebelumnya seperti fasilitasi, verifikasi, atau penegakan. Ini digunakan sebagai pengganti kontrak tradisional.

3. **Blockchain 3.0: DApps**

   DApps adalah singkatan dari aplikasi terdesentralisasi. Ini memiliki kode backend mereka berjalan pada jaringan peer-to-peer terdesentralisasi. DApp dapat memiliki kode frontend dan antarmuka pengguna yang ditulis dalam bahasa apa pun yang dapat melakukan panggilan ke backendnya, seperti Aplikasi tradisional.

Varian Blockchain

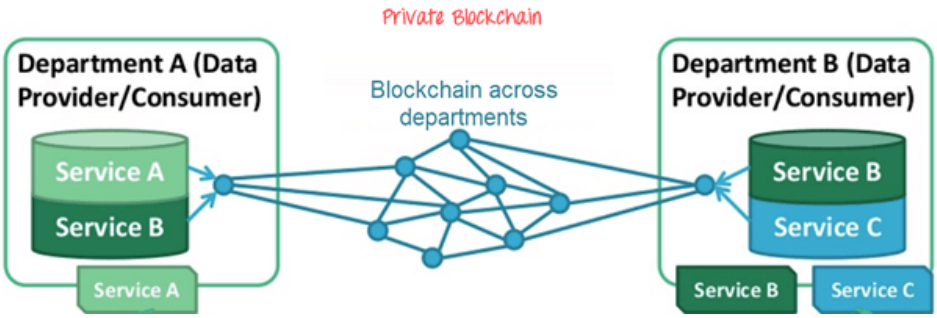
1. **Publik:**

   Dalam jenis blockchain ini, buku besar dapat dilihat oleh semua orang di internet. Ini memungkinkan siapa saja untuk memverifikasi dan menambahkan blok transaksi ke

blockchain. Jaringan publik memiliki insentif bagi orang untuk bergabung dan gratis untuk digunakan. Siapa pun dapat menggunakan jaringan blockchain publik.

2. **Privat:**

   Blockchain pribadi berada dalam satu organisasi. Ini memungkinkan hanya orang tertentu dari organisasi untuk memverifikasi dan menambahkan blok transaksi. Namun, semua orang di internet pada umumnya diizinkan untuk melihat.



3. **Konsorsium:**

   Dalam varian Blockchain ini, hanya sekelompok organisasi yang dapat memverifikasi dan menambahkan transaksi. Di sini, buku besar dapat dibuka atau dibatasi untuk grup tertentu. Blockchain konsorsium digunakan lintas organisasi. Ini hanya dikendalikan oleh node pra-resmi (sudah diotorisasi sebelumnya).

Kasus Penggunaan Blockchain

Teknologi Blockchain digunakan secara luas di berbagai sektor seperti yang diberikan dalam tabel berikut.

Sektor	Pemanfaatan
Pasar	• Billing, monitoring dan transfer data • Manajemen kuota dalam Jejaring Rantai Pasok (*Supply Chain*)
Pemerintahan	• Layanan tata kelola terpersonalisasi transnasional • *Voting, propositions P2P bond*, • Digitalisasi dokumen / kontrak dan bukti kepemilikan untuk transfer • Pendaftaran & Identifikasi • Layanan tele-pengacara • Registrasi dan pertukaran IP • Layanan notaris penerimaan pajak dan registrasi dokumen
IoT	• Jaringan sensor pertanian & drone

	• Jejaring rumah pintar • Kota pintar terintegrasi • Sensor rumahan pintar • Mobil Self-driving • Robot, komponen robot personalisasi • Drone yang dipersonalisasi • Asisten dijital
Kesehatan	• Manajemen data • Bank data Kesehatan EMR Universal • *QS Data Commons* • Analitika aliran data kesehatan yang besar • *Digital health wallet Smart property* • Token Kesehatan • Kontrak pengembangan pribadi
Sains dan Seni	• Supercomputing • Analisis orang banyak (*crowd*) • Sumber daya P2P • Layanan *digital mind fit*
Keuangan dan Akuntansi	• Pembayaran Mata Uang Digital • Pembayaran & Pengiriman Uang • Pasar Modal yang dideklarasikan menggunakan jaringan komputer di Blockchain • Akuntansi antar-divisi • Kliring & Perdagangan & Derivatif • Pembukuan

Kasus Penggunaan Penting Blockchain Dalam Kehidupan

1. Dubai: The Smart City

Pada tahun 2016, kantor pintar Dubai memperkenalkan strategi Blockchain. Dengan menggunakan teknologi ini, pengusaha dan pengembang akan dapat terhubung dengan investor dan perusahaan terkemuka. Tujuannya adalah untuk menerapkan sistem dasar blockchain yang mendukung pengembangan berbagai jenis industri untuk menjadikan Dubai “kota paling bahagia” di dunia'

2. Memberikan Insentif Untuk Penyimpanan Pelanggan

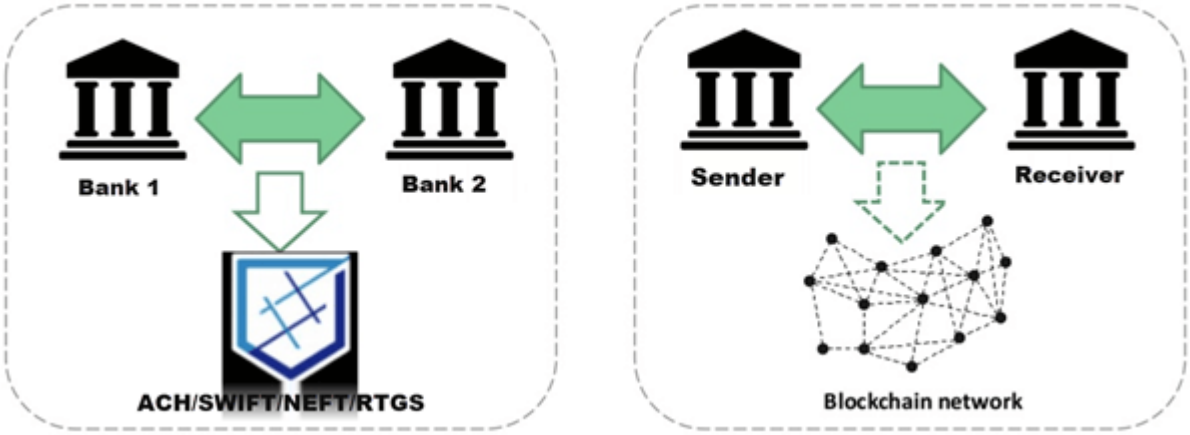
Pemberian Insentif pada CRaaS (Penyimpanan konsumen sebagai layanan) berdasarkan teknologi Blockchain. Ini adalah program loyalitas yang didasarkan pada menghasilkan token

untuk bisnis yang berafiliasi dengan jaringan terkait. Dalam sistem ini, blockchain dipertukarkan secara instan, dan dapat disimpan dalam portofolio digital dari telepon pengguna atau mengakses melalui browser.

3. Blockchain untuk Bantuan Kemanusiaan

Pada Januari 2017 program pangan dunia negara-negara bersatu memulai sebuah proyek yang disebut bantuan kemanusiaan. Proyek ini dikembangkan di daerah pedesaan di wilayah Sindh Pakistan. Dengan menggunakan teknologi Blockchain, penerima manfaat menerima uang, makanan, dan semua jenis transaksi terdaftar di blockchain untuk memastikan keamanan dan transparansi proses ini.

Bitcoin Cryptocurrency: Aplikasi Blockchain Paling Populer



Apa itu Cryptocurrency?

Cryptocurrency adalah salah satu media pertukaran seperti mata uang tradisional seperti USD, tetapi dirancang untuk bertukar informasi digital melalui proses yang dimungkinkan oleh prinsip-prinsip kriptografi tertentu. Cryptocurrency adalah mata uang digital dan diklasifikasikan sebagai bagian dari mata uang alternatif dan mata uang virtual.

Cryptocurrency adalah instrumen pembawa berdasarkan kriptografi digital. Dalam cryptocurrency semacam ini, pemegang mata uang memiliki kepemilikan. Tidak ada catatan lain yang disimpan sebagai identitas pemilik. Pada tahun 1998, Wei Dai menerbitkan "B-Money," suatu sistem cash elektronika terdistribusi yang anonymous.

Apa Itu Bitcoin?

Bitcoin diluncurkan pada 2009 oleh orang tak terkenal bernama Satoshi Nakamoto. Bitcoin adalah teknologi Peer-to-Peer yang tidak diatur oleh otoritas pusat atau bank. Saat ini, mengeluarkan Bitcoin dan mengelola transaksi dilakukan secara kolektif dalam jaringan. Saat ini cryptocurrency dominan di dunia. Ini adalah open source dan dirancang untuk masyarakat umum

berarti tidak ada yang memiliki kendali atas Bitcoin. Bahkan, hanya ada 21 juta Bitcoin yang diterbitkan. Saat ini, Bitcoin memiliki kapitalisasi pasar $ 12 miliar.

Siapa pun dapat menggunakan bitcoin tanpa membayar biaya proses apa pun. Jika Anda menangani Bitcoin, pengirim dan penerima bertransaksi secara langsung tanpa menggunakan pihak ketiga.

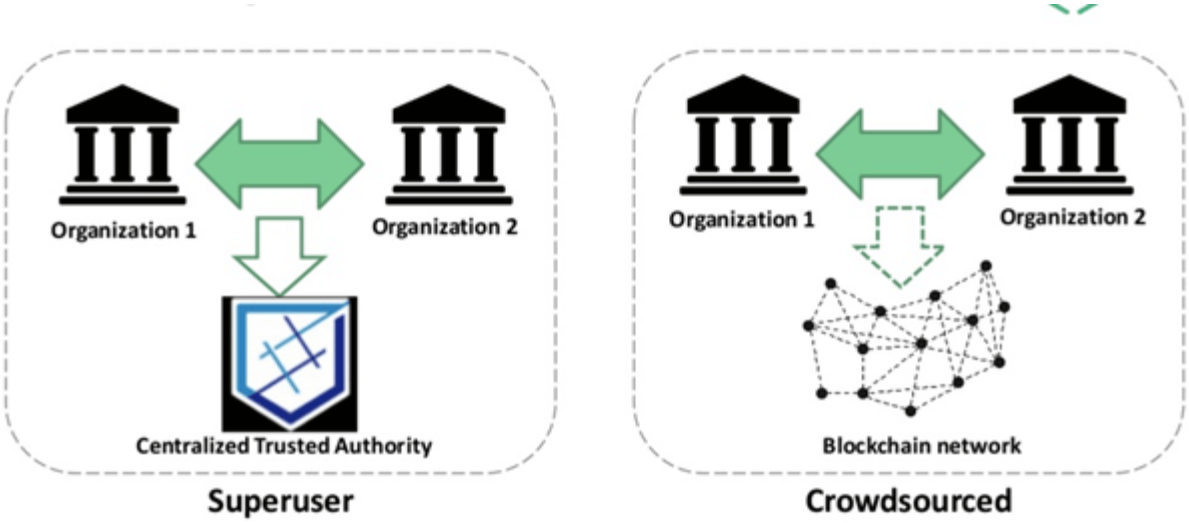
BlockChain dan Bitcoin:

Blockchain adalah teknologi di balik Bitcoin. Bitcoin adalah token digital, dan blockchain adalah buku besar yang melacak siapa yang memiliki token digital. Anda tidak dapat memiliki Bitcoin tanpa blockchain, tetapi Anda dapat memiliki blockchain tanpa Bitcoin.

Cryptocurrency terkemuka lainnya:

- Ethereum
- Bitcoin Cash
- Ripple
- Litecoin

Blockchain vs. Shared Database



Parameters	Blockchain	Shared Database
Operasi	Insert	Create/ Read/ Update dan Delete
Replikasi	Replikasi penuh pada setiap peer	Master-slave dan Multi-master
Konsensus	Sebagian besar peers sepakat mengenai outcome dari transaksi.	Transaksi terdistribusi yang diadakan dalam dua fase komit dan Paxos.
Validasi	Aturan global diberlakukan pada seluruh sistem blockchain.	Hanya menawarkan *integrity constraints* lokal

Disintermediasi	Diizinkan dengan blockchain.	Tidak memungkinkan.
Kerahasiaan	Sepenuhnya rahasia	Tidak rahasia secara total
Kekokohan	Teknologi yang sepenuhnya kuat.	Tidak sepenuhnya kuat.

Mitos Tentang Blockchain

Mitos	Realita
Memecahkan setiap masalah	Tidak, ini hanya database
Teknologi tanpa kepercayaan	Itu bisa menggeser kepercayaan dan juga menyebarkan kepercayaan
Aman	Ini berfokus pada integritas dan bukan kerahasiaan
Kontrak pintar selalu bidang hukum (legal)	Itu hanya mengeksekusi bagian dari beberapa kontrak hukum
Immutable	Ini hanya menawarkan ketidakstabilan probabilistik
Perlu buang listrik	Blokchain yang muncul efisien
Secara inheren tidak dapat diubah	Blokchain yang muncul dapat diskalakan

Keterbatasan Teknologi Blockchain

- **Higher costs (Biaya lebih tinggi):** Nodes mencari imbalan (*rewards*) yang lebih tinggi untuk menyelesaikan Transaksi dalam bisnis yang bekerja berdasarkan prinsip *Supply and Demand*
- **Slower transactions (Transaksi lebih lambat):** Node memprioritaskan transaksi dengan imbalan lebih tinggi, backlog transaksi bertambah
- **Smaller ledger (Ledger yang lebih kecil):** adalah tidak mungkin untuk menyalin penuh Blockchain, berpotensi yang dapat mempengaruhi keabadian, konsensus, dll.
- **Transaction costs, network speed (Biaya transaksi, kecepatan jaringan):** Biaya transaksi Bitcoin cukup tinggi setelah disebut-sebut sebagai 'hampir gratis' untuk beberapa tahun pertama.
- **Risk of error (Risiko kesalahan):** Selalu ada risiko kesalahan, selama faktor manusia terlibat. Jika blockchain berfungsi sebagai basis data, semua data yang masuk harus berkualitas tinggi. Namun, keterlibatan manusia dapat dengan cepat menyelesaikan kesalahan.
- **Wasteful (Boros):** Setiap node yang menjalankan blockchain harus mempertahankan konsensus di blockchain. Ini menawarkan downtime yang sangat rendah dan membuat data yang disimpan di blockchain selamanya tidak dapat diubah. Namun, semua ini boros, karena setiap node mengulangi tugas untuk mencapai konsensus.

Rangkuman

- Blockchain adalah rantai blok yang berisi informasi
- Blockchain bukan Bitcoin, tetapi itu adalah teknologi di balik Bitcoin
- Setiap blok berisi hash.
- Setiap blok memiliki hash dari blok sebelumnya
- Blockchain membutuhkan Bukti Kerja sebelum blok baru ditambahkan
- Basis data blockchain terganggu di antara banyak rekan dan tidak terpusat.
- Teknologi rantai blok adalah Ketangguhan, Desentralisasi, Pengurangan waktu, andal dan menawarkan transisi yang tidak dapat diubah
- Tiga versi Blockchain adalah Blockchain 1.0: Mata Uang, Blockchain 2.0: Kontrak Cerdas dan Blockchain 3.0: DApps
- Blockchain tersedia dalam tiga varian berbeda 1) Publik 2) Pribadi 3) Konsorsium
- Biaya lebih tinggi, transaksi lebih lambat, buku besar, risiko kesalahan adalah beberapa kelemahan menggunakan teknologi ini
- Dubai - Kota Cerdas, Retensi Pelanggan Incent, dan Blockchain untuk Bantuan Kemanusiaan adalah kasus nyata dalam penggunaan Blockchain
- Bitcoin menggunakan teknologi blockchain yang tidak diatur oleh otoritas pusat atau bank