

Blockchain Basics

Nakamoto menyatakan bahwa penulisan kode untuk bitcoin dimulai pada tahun 2007. Pada 18 Agustus 2008, dia atau rekannya mendaftarkan nama domain bitcoin.org, dan membuat situs web di alamat tersebut. Pada tanggal 31 Oktober, Nakamoto menerbitkan buku putih di milis kriptografi di metzdowd.com yang menjelaskan tentang cryptocurrency digital, berjudul "Bitcoin: A Peer-to-Peer Electronic Cash System".

Pada 9 Januari 2009, Nakamoto merilis versi 0.1 dari perangkat lunak bitcoin di SourceForge, dan meluncurkan jaringan dengan mendefinisikan blok genesis bitcoin (blok nomor 0), yang memiliki hadiah 50 bitcoin. Tertanam dalam transaksi coinbase dari blok ini adalah teks: "The Times 03/Jan/2009 Chancellor di ambang bailout kedua untuk bank", mengutip berita utama di surat kabar Inggris The Times yang diterbitkan pada tanggal tersebut. Catatan ini telah ditafsirkan sebagai stempel waktu dan komentar mengejek atas dugaan ketidakstabilan yang disebabkan oleh perbankan cadangan fraksional.

Nakamoto terus berkolaborasi dengan pengembang lain pada perangkat lunak bitcoin hingga pertengahan 2010, membuat semua modifikasi pada kode sumbernya sendiri. Dia kemudian memberikan kendali atas repositori kode sumber dan kunci peringatan jaringan kepada Gavin Andresen, mentransfer beberapa domain terkait ke berbagai anggota terkemuka komunitas bitcoin, dan menghentikan keterlibatannya yang diakui dalam proyek tersebut.

Buterin adalah salah satu pendiri dan penemu Ethereum, digambarkan sebagai "jaringan penambangan terdesentralisasi dan platform pengembangan perangkat lunak yang digabungkan menjadi satu" yang memfasilitasi pembuatan mata uang kripto baru dan program yang berbagi satu blockchain (buku besar transaksi kriptografi).

Buterin pertama kali mendeskripsikan Ethereum dalam buku putih pada November 2013. Buterin berpendapat bahwa bitcoin membutuhkan bahasa skrip untuk pengembangan aplikasi. Tetapi ketika dia gagal mendapatkan persetujuan, dia mengusulkan pengembangan platform baru dengan bahasa skrip yang lebih umum.

Smart Contract adalah program komputer yang di-host dan dieksekusi di jaringan blockchain. Setiap Smart Contract terdiri dari kode yang menentukan kondisi yang telah ditentukan sebelumnya, yang bila dipenuhi, memicu hasil. Dengan berjalan di blockchain terdesentralisasi alih-alih server terpusat, kontrak pintar memungkinkan banyak pihak untuk mencapai hasil bersama dengan cara yang akurat, tepat waktu, dan anti-rusak.

Smart Contract adalah infrastruktur yang kuat untuk otomatisasi karena tidak dikendalikan oleh administrator pusat dan tidak rentan terhadap satu titik serangan oleh entitas jahat. Ketika diterapkan pada perjanjian digital multi-pihak, aplikasi kontrak pintar dapat mengurangi risiko pihak lawan, meningkatkan efisiensi, menurunkan biaya, dan memberikan tingkat transparansi baru ke dalam proses.

Hybrid Smart Contract menggabungkan kode yang berjalan di blockchain (on-chain) dengan data dan komputasi dari luar blockchain (off-chain) yang disediakan oleh Decentralized Oracle Networks. Hybrid Smart Contract memungkinkan bentuk koordinasi ekonomi dan sosial tingkat lanjut yang memiliki sifat blockchain yang tahan-rusak dan tidak dapat diubah namun memanfaatkan layanan oracle off-chain yang aman untuk mencapai kemampuan baru, seperti skalabilitas, kerahasiaan, keadilan pesanan, dan konektivitas ke real- sumber atau sistem data dunia.

Blockchain Oracle adalah perangkat atau entitas apa pun yang menghubungkan blockchain deterministik dengan data off-chain. Ada banyak hal yang harus dibongkar dalam satu kalimat

itu. Untuk memahami apa itu blockchain oracle dan mengapa kita membutuhkannya, mari kembali ke salah satu fitur inti dari blockchain — desentralisasi.

Blockchain adalah database atau buku besar terdistribusi yang dibagikan di antara node jaringan komputer. Sebagai database, blockchain menyimpan informasi secara elektronik dalam format digital. Blockchain terkenal karena peran penting mereka dalam sistem cryptocurrency, seperti Bitcoin, untuk menjaga catatan transaksi yang aman dan terdesentralisasi. Inovasi dengan blockchain adalah menjamin kesetiaan dan keamanan catatan data dan menghasilkan kepercayaan tanpa perlu pihak ketiga yang tepercaya.

Salah satu perbedaan utama antara database biasa dan blockchain adalah bagaimana data terstruktur.

Blockchain mengumpulkan informasi bersama dalam kelompok, yang dikenal sebagai blok, yang menyimpan kumpulan informasi. Blok memiliki kapasitas penyimpanan tertentu dan, ketika diisi, ditutup dan ditautkan ke blok yang diisi sebelumnya, membentuk rantai data yang dikenal sebagai blockchain. Semua informasi baru yang mengikuti blok yang baru ditambahkan dikompilasi menjadi blok yang baru terbentuk yang kemudian juga akan ditambahkan ke rantai setelah diisi.

Database biasanya menyusun datanya ke dalam tabel, sedangkan blockchain, seperti namanya, menyusun datanya menjadi potongan-potongan (blok) yang dirangkai. Struktur data ini secara inheren membuat garis waktu data yang tidak dapat diubah ketika diimplementasikan dalam sifat terdesentralisasi. Ketika sebuah blok diisi, itu akan menjadi batu dan menjadi bagian dari garis waktu ini. Setiap blok dalam rantai diberi stempel waktu yang tepat ketika ditambahkan ke rantai.