

Dr. Budi Raharjo, S.Kom., M.Kom., MM.

UANG MASA DEPAN

BLOCKCHAIN, BITCOIN, CRYPTOCURRENCIES



YAYASAN PRIMA AGUS TEKNIK

UANG MASA DEPAN

BLOCKCHAIN, BITCOIN, CRYPTOCURRENCIES

BIODATA PENULIS



Dr. Budi Raharjo, S.Kom, M.Kom, MM lahir di Semarang, tanggal 22 Februari 1985. Beliau adalah Alumni dari Universitas Bina Nusantara (BINUS University) Jakarta dan juga alumni Universitas Kristen Satya wacana (UKSW) Salatiga. Dr. Budi Raharjo telah menjadi Dosen pada Universitas STEKOM pada mata kuliah Kepemimpinan (Leadership), mata kuliah Pengantar Akuntansi, Manajemen Proses, Manajemen Akuntansi dan Manajemen Resiko Bisnis. Selain sebagai dosen Universitas STEKOM, Dr. Budi Raharjo, M.Kom, MM juga mempunyai bisnis sendiri dalam bidang perhotelan dan juga sebagai wirausaha dalam bidang pemasok unggas (ayam) beku, ke berbagai kota besar, khususnya Jakarta dan sekitarnya.

Pengalaman beliau berwirausaha menjadi bekal utama dalam penulisan buku ajar yang diterbitkan oleh Yayasan Prima Agus Teknik (YPAT) Semarang. Oleh sebab itu bukunya berisi langkah-langkah praktis yang mudah diikuti oleh para mahasiswa, saat mahasiswa mengikuti proses perkuliahan pada Universitas Sains dan Teknologi Komputer (Universitas STEKOM). Jabatan struktural yang diembannya saat ini adalah Wakil Rektor 1 (Akademik) Universitas STEKOM Semarang.



YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

UANG MASA DEPAN

BLOCKCHAIN, BITCOIN, CRYPTOCURRENCIES

Dr. Budi Raharjo, S.Kom., M.Kom., MM.



YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

UANG MASA DEPAN : Blockchain, Bitcoin, Cryptocurrencies

Penulis :

Dr. Budi Raharjo, S.Kom., M.Kom., MM.

ISBN :

Editor :

Dr. Mars Caroline Wibowo. S.T., M.Mm.Tech

Penyunting :

Dr. Joseph Teguh Santoso, M.Kom.

Desain Sampul dan Tata Letak :

Irdha Yunianto, S.Ds., M.Kom

Penerbit :

Yayasan Prima Agus Teknik

Redaksi :

Jl. Majapahit no 605 Semarang

Telp. (024) 6723456

Fax. 024-6710144

Email : penerbit_ypat@stekom.ac.id

Distributor Tunggal :

Universitas STEKOM

Jl. Majapahit no 605 Semarang

Telp. (024) 6723456

Fax. 024-6710144

Email : info@stekom.ac.id

Hak cipta dilindungi undang-undang

Dilarang memperbanyak karya tulis ini dalam bentuk dan dengan cara apapun tanpa ijin dari penulis

KATA PENGANTAR

Puji syukur pada Tuhan Yang Maha Esa bahwa buku yang berjudul "*UANG MASA DEPAN : Blockchain, Bitcoin, Cryptocurrencies*" ini dapat diselesaikan dengan baik. Buku ini berisi informasi untuk tujuan pendidikan dan informasi umum saja. Jadi konten apa pun yang terkandung dalam buku ini boleh dianggap hanya sebagai saran saja. Para pembaca harus mempertimbangkan aspek hukum, keuangan dan perpajakan yang berhubungan dengan keputusan bisnis yang ada sangkut pautnya dengan *Blockchain, Bitcoin, Cryptocurrencies*.

Apa sebenarnya teknologi Blockchain, teknologi *Blockchain* dapat disebut sebagai inovasi terbesar semenjak kemajuan teknologi internet. Pendukung teknologi ini mengklaim bahwa teknologi ini tidak akan mengganggu industri yang ada saat ini atau berdampak pada kehidupan semua orang yang ada di planet ini. Apakah teknologi *blockchain* menjadi salah satu revolusi teknologi yang terbesar dalam sejarah? Apakah teknologi *blockchain* akan menyebabkan pemerintah dan sistem perbankan harus mengubah cara mereka memproses informasi atau masihkah melakukan bisnis seperti biasa? Apakah perusahaan perintis teknologi blockchain terlalu bersemangat dalam menciptakan gelembung teknologi lain, yang pada dasarnya hanyalah cara baru untuk membuat database?

Buku ini akan memberikan jawaban atas pertanyaan-pertanyaan di atas serta akan membahas berbagai argumen yang mendukung dan menentang teknologi blockchain. Buku ini akan menjelaskan apa itu teknologi blockchain, bagaimana cara kerjanya, dan dampak apa yang akan timbul dari potensi teknologi tersebut. Meskipun dalam buku ini mencakup banyak aplikasi dan manfaat yang potensial, namun ini buku hanya akan membahas teknologi blockchain sebagai jawaban atas masalah di pemerintahan, sistem perbankan, atau industri. Tujuan dari buku ini adalah untuk memberikan pemahaman yang seimbang tentang teknologi *blockchain*, yang menggabungkan manfaat dan potensi risiko dari penggunaan blockchain, termasuk kerugian, dan cara mengatasinya.

Buku ini ditulis dengan tujuan untuk mengenalkan teknologi *blockchain* kepada orang-orang yang belum tahu dan sedang mencari pemahaman non-teknis tentang teknologi tersebut. Ada beberapa aspek teknis yang dibahas pada akhir buku ini, namun tidak hanya detail teknis dari *blockchain*, juga dibahas *Bitcoin* dan *Cryptocurrencies*. Ketika pertama kali belajar tentang teknologi blockchain, kita akan menemukan banyak informasi teknis tentang teknologi blockchain yang tersebar dan tidak terstruktur dengan baik.

Setiap akhir dari bab dalam buku ini ada ringkasan, yang berisi pengulangan informasi yang ada dalam bab tersebut. Kebanyakan orang yang lebih suka mendapatkan ringkasan informasi tentang poin-poin penting. Ringkasan ini juga akan membantu kita menemukan poin penting untuk dicatat, atau dengan cepat menemukan materi untuk referensi, tanpa harus membaca seluruh bab lagi. Akhir kata semoga buku ini berguna untuk para pembaca.

Semarang, Februari 2022
Penulis

Dr. Budi Raharjo, S.Kom, M.Kom, MM.

DAFTAR ISI

Halaman Judul	i
Kata Pengantar	iii
Daftar Isi	iv
BAB 1 APA ITU <i>BLOCKCHAIN</i>	1
1.1 Resiko dan masalah <i>blockchain</i>	2
1.2 Perbedaan antara <i>blockchain</i> dan Bitcoin	3
1.3 Ringkasan	4
BAB 2 CARA KERJA <i>BLOCKCHAIN</i>	5
2.1 Mengapa disebut <i>Blockchain</i> ?	6
2.2 Mengubah transaksi dan blokir setelah ditambahkan	6
2.3 Pengeluaran ganda	6
2.4 Pertukaran nilai di <i>blockchain</i>	7
2.5 Konsensus terdistribusi	8
2.6 Cara kerja <i>blockchain</i>	9
2.7 Ringkasan	10
BAB 3 SEJARAH <i>BLOCKCHAIN</i> DAN BITCOIN	11
3.1 Mata Uang Digital	12
3.2 Ringkasan	15
BAB 4 MANFAAT TEKNOLOGI <i>BLOCKCHAIN</i>	17
4.1 Transparansi	17
4.2 Penghapusan perantara	17
4.3 Desentralisasi	18
4.4 Berbagai Potensi Penggunaan	19
4.5 Peningkatan kecepatan transaksi	20
4.6 Ringkasan	20
BAB 5 BAHAYA MENGGUNAKAN <i>BLOCKCHAIN</i>	22
5.1 Kurangnya Privasi	22
5.2 Masalah Keamanan	23
5.3 Tidak Ada Kontrol Terpusat	24
5.4 Risiko serangan 51%	25
5.5 Teknologi baru yang belum terbukti	25
5.6 Biaya	25
5.7 Kurangnya skalabilitas	26
5.8 Kepercayaan, Reputasi, dan Pemahaman tentang <i>Blockchains</i>	27
5.9 Regulasi dan Integrasi	27
5.10 Promosi sensasional	28
5.11 Ringkasan	29
BAB 6 <i>BLOCKCHAIN</i> DAN INDUSTRI KEUANGAN	31
6.1 Ripple	32
6.2 Ringkasan	33

BAB 7 BLOCKCHAIN DAN INDUSTRI SELAIN KEUANGAN	34
7.1 Manajemen identitas dan identitas digital	34
7.2 Pemungutan Suara Digital	35
7.3 Perawatan Kesehatan dan Rekam Medis	35
7.4 Sertifikat Akademi	36
7.5 Musik	36
7.6 Penyimpanan <i>Cloud</i>	37
7.7 Rental Mobil	37
7.8 Berbagi Perjalanan	37
7.9 Properti	38
7.10 Sewa Apartemen	38
7.11 Industri perjalanan	38
7.12 Program Loyalitas / Hadiah	39
7.13 Prediksi dan perjudian	39
7.14 Ringkasan	40
BAB 8 ETHEREUM, KONTRAK PINTAR, DAN APLIKASI TERDESENTRALISASI	41
8.1 Pengantar Ethereum	41
8.2 Perbedaan Antara Ethereum Dan Bitcoin	41
8.3 Manfaat Ethereum	42
8.4 Aplikasi Terdesentralisasi (Dapps)	42
8.5 Kontrak Pintar	42
8.6 Ringkasan	44
BAB 9 MASA DEPAN BLOCKCHAIN	46
9.1 Sumber Terbuka Terdesentralisasi Vs Sumber Tertutup Terpusat	46
9.2 Buku besar terdistribusi	47
9.3 <i>Blockchain</i> 2.0 - Aplikasi terdesentralisasi (dApps) dan Kontrak Cerdas	48
9.4 <i>Blockchain</i> dalam kehidupan sehari-hari	48
9.5 Ringkasan	49
BAB 10 PANDUAN TEKNIS UNTUK BLOCKCHAIN	51
10.1 Pengantar Panduan Teknis Untuk <i>Blockchain</i>	51
10.2 Panduan Teknis Tentang Cara Kerja <i>Blockchain</i>	51
10.3 Hashing Transaksi Menjadi Blok	52
10.4 Membuat <i>Blockchain</i>	53
10.5 Mengubah <i>Blockchain</i>	54
10.6 Meningkatkan Kesulitan Jaringan	56
10.7 Permasalahan Yang Dihadapi	57
10.8 Ringkasan	58
DAFTAR PUSTAKA	62

BAB 1

APA ITU *BLOCKCHAIN*?

Sederhananya, *blockchain* seperti database; itu adalah cara menyimpan catatan nilai dan transaksi. Sayangnya, definisi sederhana itu tidak akan membuat orang tertarik dan akan membuat banyak orang berpikir, "Jadi apa? Semua hype untuk tipe database baru?" Namun, menyebut *blockchain* sebagai jenis database baru seperti mengatakan bahwa email adalah cara baru untuk mengirim surat kepada orang-orang. Sementara *blockchain* adalah database, definisi itu tidak menjelaskan kejeniusan sejati di balik bagaimana *blockchain* menyimpan catatan nilai dan transaksi.

Di masa lalu ketika aset bernilai atau transaksi dicatat dalam database, orang mengandalkan pihak ketiga seperti bank, pemerintah, atau perusahaan untuk mencatat informasi ini. Orang percaya bahwa bank tidak akan mencuri uang mereka karena pemerintah mengatur mereka. Jika bank gagal, masyarakat percaya bahwa pemerintah akan memastikan simpanan uang mereka aman. Saat mentransfer uang atau membayar barang dan jasa, orang percaya perusahaan kartu kredit dan bank akan mengambil jumlah yang benar dari rekening bank mereka dan menyetorkannya ke rekening penjual. Penjual percaya bahwa perusahaan kartu kredit akan membayar mereka uang dan jika ada perselisihan atau penipuan pada transaksi itu akan ditangani melalui perusahaan kartu kredit.

Jika pembeli di sebuah toko membayar dengan uang tunai, penjual percaya bahwa mereka dapat mengambil selembar kertas dengan nomor di atasnya yang didukung oleh pemerintah ke toko lain dan menukarinya untuk membayar barang dan jasa lain. Penjual juga percaya bahwa jika mereka membawa catatan ke bank, mereka dapat mengubahnya menjadi saldo tunai digital di rekening bank mereka yang dapat digunakan untuk membayar pembelian menggunakan kartu kredit atau transaksi online. Orang-orang mempercayai lembaga eksternal ini dengan uang dan informasi mereka. Orang-orang percaya bahwa perusahaan kartu kredit dan bank akan menjaga kerahasiaan dan keamanan detail kartu kredit mereka. Mereka percaya bahwa perusahaan kartu kredit dan bank memiliki database dengan catatan saldo dan transaksi mereka yang dipelihara secara akurat. Bank percaya bahwa pemerintah memiliki database dan catatan catatan yang diterbitkan.

Kepercayaan pada institusi ini tidak hanya finansial tetapi meluas ke setiap area kehidupan kita. Jika Anda pernah meminjam buku dari perpustakaan, perpustakaan menyimpan database semua buku yang mereka miliki. Perpustakaan juga memelihara database anggota, semua buku yang telah dipinjam, tanggal pengembalian setiap buku, dan buku-buku yang lewat jatuh tempo. Perpustakaan memelihara database pusat dari detail pribadi Anda, alamat rumah, dan informasi. Jika Anda tidak mengembalikan buku yang telah Anda pinjam, mereka dapat mengirimkan denda kepada Anda, dan jika diperlukan, mereka dapat mengambil tindakan hukum terhadap Anda karena pencurian. Catatan database tentang detail pribadi Anda, buku yang Anda pinjam, kebiasaan membaca Anda — semua informasi ini bersifat pribadi dan disimpan oleh perpustakaan, dan Anda yakin mereka tidak akan membagikan informasi itu kepada orang lain.

Informasi ini dipusatkan di lembaga-lembaga ini dengan masing-masing dari mereka memelihara catatan dan sistem mereka sendiri. Tema umum dari transaksi sehari-hari adalah bahwa kita memercayai institusi dan database terpusat yang mereka pertahankan untuk mencatat kehidupan kita secara akurat.

Tema lain yang mendasari umum adalah bahwa kita tidak percaya satu sama lain. Coba bayangkan skenario di atas tanpa organisasi terpusat tepercaya yang terlibat dalam transaksi. Bayangkan Anda memiliki sebuah toko dan seseorang memberikan Anda selembar kertas yang bertuliskan "Saya berhutang Rp 1.500.000 dengan nama mereka ditandatangani di sana. Mereka memberi tahu Anda bahwa jika Anda membawa selembar kertas itu ke toko lain, Anda dapat menggunakannya untuk membeli barang senilai Rp 1.500.000 dari toko itu.

Apakah Anda akan mempercayai mereka? Jawabannya mungkin tidak, namun itulah yang dilakukan orang setiap hari dengan mata uang kertas. Uang kertas Rp 1.500.000 hanyalah selembar kertas dengan tulisan "Saya berhutang Rp 1.500.000 dari pemerintah". Anda menerima dan menggunakan catatan ini hampir setiap hari dengan kepercayaan bahwa toko akan menerimanya, dan mereka percaya bahwa penjual lain akan menerimanya dan seterusnya. Di mana *blockchain* menawarkan potensi signifikan di negara-negara di mana orang tidak mempercayai bank, institusi, pemerintah, mata uang, atau satu sama lain.

Bahkan di Amerika Serikat, yang memiliki salah satu sistem keuangan paling maju dan teregulasi di dunia, lembaga keuangan besar gagal selama Krisis Keuangan Hebat. Perusahaan keuangan yang telah ada selama ratusan tahun runtuh hampir dalam semalam dengan membawa serta tabungan hidup orang-orang. Pada tahun 2015 di Yunani, negara maju yang merupakan bagian dari Euro, bank membekukan semua simpanan rekening bank dan hanya mengizinkan orang untuk menarik sekitar Rp 1.050.000 sehari dari ATM. Alternatif apa yang dimiliki orang selain menyetor uang ke bank dan perusahaan yang mereka yakini dapat dipercaya? Simpan semua uang mereka dan sembunyikan di bawah kasur? Jika seseorang mengetahui tabungan hidup Anda ada di rumah Anda, maka Anda berisiko mencurinya. Jika rumah Anda terbakar, maka Anda berisiko kehilangan semua uang Anda dalam kebakaran.

Jika bank dapat runtuh dan pemerintah dapat membekukan penarikan bank di AS dan Eropa, bagaimana orang-orang di negara-negara yang kurang berkembang dan teregulasi dapat mempercayai bank dan pemerintah mereka? Jawaban sederhananya adalah mereka tidak bisa mempercayai mereka.

1.1 RESIKO DAN MASALAH *BLOCKCHAIN*

Ada miliaran orang di dunia yang tinggal di negara-negara di mana pemerintah dijalankan oleh kediktatoran militer, pemerintah memiliki bank dan mencuri atau menyita uang dari rekening, mata uang lokal tidak diterima di toko, kejahatan tinggi, dan tidak ada sistem hukum untuk melindungi orang dan aset mereka. Ada banyak negara di mana bahkan jika Anda dapat percaya bahwa bank tidak akan mencuri uang Anda atau bangkrut, simpanan Anda dipantau dengan cermat oleh pemerintah dan mereka dapat menangkap, memenjarakan, atau mengeksekusi Anda berdasarkan transaksi Anda.

Dalam contoh perpustakaan, database terpusat yang tampaknya tidak berbahaya bagi Anda untuk berbagi informasi. Anda dapat meminjam buku dari perpustakaan yang tidak disetujui oleh pemerintah di negara tersebut seperti Panduan Pemula untuk menggulingkan kediktatoran militer atau buku 1984 karya George Orwell. Pemerintah dapat menandai kebiasaan membaca Anda sebagai hal yang mencurigakan yang berpotensi mengarah pada penyelidikan kehidupan pribadi Anda, penangkapan atau lebih buruk di negara tertentu.

Di negara-negara di mana ada kurangnya kepercayaan pada perusahaan dan pemerintah, itu membuat transaksi berisiko dan sulit. Jika orang menaruh uang di bank, mereka berisiko muncrinya oleh bank atau pemerintah. Saat melakukan pembelian besar seperti membeli rumah, orang mungkin terpaksa menyimpan uangnya dalam bentuk tunai, emas, permata, atau logam untuk ditabung untuk pembelian besar ini dengan mengambil risiko bahwa uang ini dicuri atau dihancurkan dalam api.

Bahkan setelah semua risiko ini, jika seseorang dapat menyimpan cukup uang untuk pembelian besar seperti rumah, mereka masih mengambil risiko penjual rumah itu mencuri uang mereka dan tidak memberikan mereka kepemilikan rumah. Tidak ada sistem hukum yang stabil untuk menantang kepemilikan atau melaporkan pencurian. Jika pembelian dibayar tunai atau emas dan bukan transaksi elektronik, juga tidak ada bukti transaksi itu terjadi.

Basis data dan lembaga terpusat berfungsi ketika ada kepercayaan pada sistem hukum, peraturan, pemerintah, keuangan, dan manusia. Bahkan ketika semua faktor ini dapat dipercaya di suatu negara, kepercayaan ini terkadang masih dikhianati sehingga menyebabkan orang kehilangan uang dan aset. Basis data terdesentralisasi yang dibangun di atas *blockchain* menghilangkan kebutuhan akan institusi dan basis data terpusat. Semua orang di *blockchain* dapat melihat dan memvalidasi transaksi yang menciptakan transparansi dan kepercayaan. Kepercayaan terletak pada inti dari *blockchain*; itu menyediakan sistem kepercayaan antara orang-orang tanpa perlu perantara yang terlibat dalam transaksi. *Blockchain* memungkinkan orang untuk bertransaksi antara satu sama lain dengan sesuatu yang berharga. Dalam contoh yang diberikan itu adalah buku, tetapi ini dapat digunakan untuk properti, saham, uang, file digital... hampir semua hal.

1.2 PERBEDAAN ANTARA *BLOCKCHAIN* DAN *BITCOIN*

Referensi pertama ke *blockchain* ada di dalam kode sumber Bitcoin—pada dasarnya *blockchain* pertama dibuat ketika Bitcoin dibuat. Sejarah Bitcoin dan *blockchain* akan dibahas di bab berikutnya, jadi bab ini tidak akan membahas ini secara mendetail.

Blockchain adalah salah satu teknologi yang mendasari Bitcoin. Ada kesalahpahaman bahwa *blockchain* adalah satu-satunya teknologi di balik Bitcoin. Namun, Bitcoin telah dibuat menggunakan berbagai teknologi kriptografi lainnya yang dikombinasikan dengan *blockchain*. Bitcoin adalah mata uang digital, terutama digunakan untuk pembayaran. Bitcoin menggunakan teknologi *blockchain* satu arah; namun, *blockchain* dapat digunakan untuk merekam dan mentransfer apa pun yang berharga, bukan hanya transaksi keuangan.

Sistem berbasis *Blockchain* digunakan untuk berbagai aplikasi di berbagai industri, termasuk identitas digital, jejaring sosial, pemungutan suara, penyimpanan *cloud*, aplikasi terpusat, dan lebih banyak lagi yang dibahas nanti dalam buku ini. Tampaknya ada

kemungkinan tak terbatas untuk sistem berbasis *blockchain* yang sedang dikembangkan oleh perusahaan dan pemerintah. Bitcoin, di sisi lain, masih hanya digunakan untuk pembayaran digital. Sementara Bitcoin semakin populer dengan harganya yang terus mencapai rekor tertinggi, Bitcoin dirancang terutama sebagai metode pembayaran. Di bab berikutnya, kita akan membahas secara mendetail dengan contoh bagaimana tepatnya *blockchain* bekerja.

1.3 RINGKASAN:

- *Blockchain* seperti database; itu adalah cara menyimpan catatan nilai dan transaksi. Hampir semua hal dapat direkam di *blockchain*.
- Sebagian besar transaksi saat ini antara orang-orang memerlukan perantara untuk memberikan kepercayaan, keamanan, dan memfasilitasi transaksi, misalnya, bank, lembaga keuangan.
- Teknologi *Blockchain* menghilangkan kebutuhan akan perantara, memungkinkan orang untuk bertransaksi secara langsung satu sama lain.
- Miliaran orang di dunia tinggal di negara-negara di mana mereka tidak dapat mempercayai perantara seperti bank, pemerintah, dan sistem hukum untuk transaksi atau pencatatan yang akurat. *Blockchain* sangat berguna dalam kasus ini untuk membantu memberikan kepercayaan dan jaminan kepada orang-orang saat bertransaksi satu sama lain.
- Bitcoin adalah sistem berbasis *blockchain*. *Blockchain* bukanlah sistem berbasis Bitcoin.
- Bitcoin terutama digunakan untuk pembayaran. Sistem berbasis *Blockchain* memiliki berbagai kegunaan untuk mentransfer hampir semua hal yang berharga.

BAB 2

CARA KERJA *BLOCKCHAIN*

Bab sebelumnya memperkenalkan Anda pada teknologi *blockchain* dengan gambaran singkat tentang bagaimana hal itu dapat digunakan untuk menggantikan perantara dalam transaksi. Dalam bab ini; kita akan membahas secara mendetail dengan contoh cara kerja *blockchain*. Jika kita kembali ke contoh perpustakaan dari bab sebelumnya, perpustakaan adalah perantara yang memelihara database terpusat dari orang-orang yang meminjam buku. Jika seseorang telah meminjam buku yang ingin Anda pinjam, Anda dapat meminta perpustakaan memberi tahu Anda saat buku itu dikembalikan, tetapi perpustakaan tidak akan memberi tahu Anda detail orang yang meminjam buku itu.

Orang yang memiliki buku itu mungkin tinggal di jalan Anda, lebih dekat dari perpustakaan untuk Anda berdua, tetapi Anda tidak bisa pergi ke rumah mereka dan bertanya apakah Anda bisa meminjamnya dari mereka. Perpustakaan memelihara database pusat dari semua informasi buku yang dipinjam dan tidak membaginya dengan anggota. Sekarang, bayangkan sebuah perpustakaan bersama di mana Anda menyumbangkan buku-buku Anda dan memungkinkan orang untuk meminjamnya dari Anda. Anda mungkin memiliki banyak buku yang orang lain ingin pinjam dari Anda, dan kemungkinan ada banyak orang lain yang memiliki buku yang ingin Anda pinjam dan baca.

Dalam contoh perpustakaan bersama ini, siapa saja dapat bergabung, dan ketika mereka meminjam buku, mereka juga dapat meminjamkan buku kepada orang lain, tanpa membawanya kembali ke perpustakaan atau pemilik aslinya. Bagaimana Anda menyimpan catatan tentang siapa yang telah meminjam buku, buku mana yang mereka miliki, dan siapa pemilik asli buku itu?

Catatan yang perlu Anda pertahankan bukan hanya untuk buku Anda, tetapi untuk semua buku di perpustakaan bersama. Anda perlu menyimpan catatan semua buku yang saat ini ada di perpustakaan, pemilik aslinya, buku-buku yang telah dipinjam, dan kepada siapa orang lain meminjamkan buku tersebut. Anda dapat menugaskan satu orang dalam grup untuk memelihara catatan, tetapi Anda baru saja kembali memiliki perpustakaan asli dan model database terpusat. Ini mungkin tampak rumit, dan pada titik ini, Anda mungkin bertanya pada diri sendiri mengapa saya setuju untuk bergabung dengan perpustakaan bersama ini ketika saya bisa mendapatkan buku-buku ini di Kindle.

Ini adalah situasi di mana manfaat teknologi *blockchain* benar-benar dapat dilihat dari database tradisional. *Blockchain* dapat menyediakan database terdistribusi terdesentralisasi dari semua catatan buku di perpustakaan. Dengan database terdesentralisasi, semua orang di perpustakaan mendapatkan akses ke catatan. Mereka akan melihat semua buku di perpustakaan, siapa pemilik aslinya, siapa yang meminjam setiap buku, mereka bisa melihat apakah mereka akan meminjamkan buku itu kepada orang lain. Setiap kali sebuah buku dipinjam dari perpustakaan bersama, semua catatan database buku yang dapat diakses setiap orang diperbarui. Tidak ada database atau institusi pusat yang diperlukan untuk mengoperasikan ini; semua orang memelihara database.

Anda dapat mengoperasikan perpustakaan tanpa memerlukan database pusat dan lembaga eksternal yang mengoperasikannya.

2.1 MENGAPA DISEBUT *BLOCKCHAIN*?

Dalam contoh perpustakaan, setiap kali sebuah buku dipinjam maka terjadilah transaksi. Ada banyak sekali transaksi yang terjadi pada saat yang bersamaan, sehingga transaksi-transaksi ini kemudian dikelompokkan dan ditambahkan ke dalam blok baru.

Blok baru ini ditambahkan "di atas" blok sebelumnya dengan mengacu pada blok sebelumnya, menghubungkannya bersama-sama. Sebagai contoh:

Blokir 10 tautan untuk memblokir 9

Blokir 9 Tautan untuk memblokir 8

Blokir 8 Tautan untuk memblokir 7 Dll.

Dengan menghubungkan blok-blok ini bersama-sama, itu menciptakan rantai blok, maka nama "*blockchain*." Setiap blok baru merujuk ke blok sebelumnya, dan blok itu merujuk ke blok sebelum semuanya kembali ke awal. Dalam contoh perpustakaan, siapa pun dapat pergi ke blok terbaru di rantai. Mereka bisa melihat semua buku yang dipinjam dan oleh siapa. Mereka kemudian dapat melihat transaksi-transaksi di blok sebelumnya, untuk melihat siapa yang memiliki buku-buku itu sebelum mereka, sepanjang perjalanan kembali ke awal untuk melihat pemilik aslinya.

Tidak ada database atau otoritas pusat; jika seseorang ingin mengklaim bahwa mereka adalah pemilik asli buku tersebut, hal itu dapat dilacak dari blok transaksi terakhir sampai ke blok pertama yang dikenal sebagai "blok genesis".

2.2 MENGUBAH TRANSAKSI DAN BLOKIR SETELAH DITAMBAHKAN

Blok yang ditambahkan ke *blockchain* tidak dapat diubah atau diubah, mereka ditambahkan secara permanen ke *blockchain*. Karena setiap blok mengacu pada blok sebelumnya, jika seseorang ingin melakukan penipuan dengan mengubah transaksi, mereka harus mengubah semua blok sebelum dan sesudah blok tersebut.

Jaringan Bitcoin memperkirakan bahwa setelah 6 blok ditambahkan di atas satu blok, tidak mungkin untuk mengubah transaksi apa pun di blok itu karena daya komputasi yang diperlukan akan membuatnya tidak mungkin untuk diubah. Jika transaksi terjadi di blok nomor 10, maka setelah *blockchain* mencapai blok 16, tidak mungkin untuk mengubah transaksi di blok 10. Jumlah blok di atas transaksi juga dapat disebut sebagai konfirmasi; beberapa perusahaan akan menunggu 6 konfirmasi sebelum menerima pembayaran sebagai jaminan bahwa transaksi tidak akan berubah di *blockchain*.

2.3 PENGELUARAN GANDA

Untuk memahami masalah lain yang dipecahkan oleh *blockchain*, mari kita lihat contoh di mana seseorang ingin mendapatkan keuntungan dari sistem perpustakaan bersama dengan mencuri buku. Setiap kali sebuah buku dipinjam, itu menciptakan transaksi yang tertunda, transaksi ini dikirim ke semua orang di jaringan untuk memvalidasi dan menambahkan ke

blockchain. Orang yang mengelompokkannya dengan transaksi tertunda lainnya dan menambahkan blok transaksi yang valid ke *blockchain* mendapat hadiah. Blok transaksi baru ditambahkan ke *blockchain* dan basis data setiap orang diperbarui dengan catatan transaksi. Setiap orang di jaringan dapat melihat siapa yang memiliki setiap buku dan dari siapa mereka meminjamnya. Karena semua orang tahu siapa yang memiliki setiap buku, seluruh jaringan dapat melihat apakah ada orang yang tidak mengembalikan buku dan statusnya kapan saja.

2.4 PERTUKARAN NILAI DI *BLOCKCHAIN*

Mari tambahkan faktor lain ke perpustakaan bersama ini, setiap kali seseorang meminjam buku, mereka membayar orang yang mereka pinjam buku dari token yang disebut "bookcoin." Dengan asumsi seseorang hanya dapat meminjamkan buku kepada orang lain untuk mendapatkan keuntungan, mereka akan membayar saya bookcoin untuk meminjam buku dan akan menerima 1 bookcoin ketika seseorang meminjam buku dari mereka. Untuk mendapat untung, mereka perlu meminjamkan lebih banyak buku daripada meminjam. Sneaky Sam telah bergabung dengan perpustakaan bersama ini. Dia telah bergabung meskipun anggota lain mencurigai dia akan melakukan sesuatu yang licik. Bagaimanapun, Sneaky Sam menyumbangkan buku Romeo and Juliet ke perpustakaan, seseorang meminjam buku dari perpustakaan, dan dia mendapat 1 koin buku.

Menjadi orang yang licik, dia membuat rencana untuk mencoba dan meminjam lebih banyak buku daripada yang dia mampu dari saldo bookcoinnya.

Sneaky Sam meminjam buku 1984 dari David.

Sneaky Sam kemudian dengan cepat meminjam buku Hamlet dari Sally.

Keduanya membuat transaksi di jaringan. Transaksi pertama dikirim ke semua orang di jaringan untuk menyetujui peminjaman buku "1984" dan bahwa Sneaky Sam membayar David 1 koin buku untuk meminjam buku ini.

Transaksi ini diputuskan oleh semua orang di jaringan yang valid dan mereka menambahkan ke blok baru, yang ditambahkan ke *blockchain*:

Sneaky Sam meminjam 1984 dari David

Sneaky Sam membayar 1 bookcoin kepada David.

Setelah transaksi ini berjalan, jaringan menerima transaksi berikutnya untuk menyetujui:

Sneaky Sam meminjam Hamlet dari Sally

Sneaky Sam membayar 1 bookcoin kepada Sally.

Jaringan memeriksa saldo buku Sneaky Sam dan melihat bahwa dia hanya memiliki 1 bookcoin, dan dia mencoba membuat salinan koin untuk mencoba dan mengelabui jaringan. Karena jaringan terbuka dan setiap orang memiliki salinan catatan, mereka dapat melacak transaksi sampai ke awal. Mereka dapat melihat di mana Sneaky Sam menerima 1 bookcoin dari meminjamkan bukunya memberinya saldo 1 bookcoin.

Dia tidak memiliki 2 koin buku untuk dibelanjakan dan semua orang di jaringan dapat melihatnya. Mayoritas orang di jaringan setuju bahwa ini adalah transaksi yang tidak valid. Mereka tidak mengizinkannya untuk meminjam buku kedua dan pembayaran ini dianggap tidak sah. Transaksi ditolak dan tidak ditambahkan ke *blockchain*.

2.5 KONSENSUS TERDISTRIBUSI

Dalam contoh ini, disebutkan bahwa mayoritas orang di jaringan harus setuju bahwa transaksi itu sah untuk dilakukan, ini dikenal sebagai konsensus terdistribusi. Tidak akan layak bagi semua orang di jaringan untuk setuju karena akan ada orang di jaringan yang mencoba memasukkan transaksi ganda, menipu sistem dengan mencoba menyetujui transaksi palsu sebagai valid. Dengan banyak *blockchain*, ambang batas konsensus lebih dari 50%, jika lebih dari 50% orang di jaringan setuju bahwa suatu transaksi valid, maka transaksi tersebut diterima sebagai valid.

Beginilah cara kerja *blockchain* yang terdesentralisasi secara umum untuk menyetujui transaksi dan mengelola jaringan. Alih-alih satu entitas menyetujui semua transaksi dan menjaga database tetap akurat, ini dibagikan di antara jaringan. Semua orang yang terhubung ke jaringan dapat memiliki suara apakah suatu transaksi harus diterima ke *blockchain* atau tidak. Potensi risiko dan bahaya lebih dari 50% jaringan menerima transaksi yang tidak valid akan dibahas kemudian di buku ini. Penambangan Anda mungkin pernah mendengar kata "penambangan" yang digunakan ketika berbicara tentang Bitcoin dan *cryptocurrency*.

Permintaan transaksi dikirim ke setiap komputer di jaringan untuk memvalidasi dan memasukkannya ke dalam *blockchain*. Untuk memvalidasi transaksi dan menambahkannya ke *blockchain*, komputer di jaringan harus memecahkan teka-teki yang terhubung ke blok berikutnya untuk ditambahkan ke *blockchain*. Komputer yang memecahkan teka-teki dengan benar terlebih dahulu, dapat menambahkan transaksi ke dalam blok, lalu menambahkan blok transaksi tersebut ke *blockchain*. Untuk memecahkan teka-teki terlebih dahulu, mereka menerima hadiah, biasanya dibayarkan dalam *cryptocurrency* atau token yang digunakan di jaringan itu. Proses ini dikenal sebagai penambangan, karena seperti menambang sejumlah kecil nilai dari sebuah blok.

Bukti kerja

Penambang yang memecahkan teka-teki dan menambahkan blok yang valid ke jaringan dihargai karena menyumbangkan daya komputer, listrik, dan sumber daya ke jaringan karena ini membantu menjaga jaringan tetap berjalan. Teka-teki yang mereka pecahkan dikenal sebagai bukti kerja. Ini adalah teka-teki matematika yang sangat sulit untuk dipecahkan tetapi mudah untuk memverifikasi jawabannya setelah dipecahkan. Anggap saja sebagai kunci kombinasi. Untuk menambahkan blok baru ke *blockchain* dan menerima hadiah, Anda harus memecahkan kombinasi ke kunci.

Anda hanya dapat memecahkan kombinasi kunci ini dengan menebak angkanya. Semua orang di jaringan secara acak menebak nomor kunci kombinasi ini. Orang yang menyelesaiannya terlebih dahulu mendapat hadiah dan dapat menambahkan blok ke *blockchain*. Setelah kombinasi kunci dipecahkan, semua orang di jaringan dapat dengan mudah memasukkan angka-angka itu ke dalam kunci untuk mengonfirmasi bahwa angka-angka tersebut membuka kunci. Dengan memecahkan teka-teki ini, ini bertindak sebagai bukti bahwa daya komputasi, listrik, waktu, dan sumber daya disumbangkan ke jaringan. Hadiahnya adalah kompensasi untuk biaya kontribusi sumber daya ini untuk menjalankan *blockchain*. *Proof of work* membutuhkan banyak daya komputasi dan ada metode lain yang dapat digunakan saat menjalankan *blockchain* yang akan dibahas nanti.

2.6 CARA KERJA *BLOCKCHAIN*

Kami telah membahas bagaimana jaringan *blockchain* dapat digunakan untuk membuat database untuk menggantikan perpustakaan sebagai institusi terpusat. Bagi banyak orang, kegunaan mengganti database perpustakaan mungkin tidak sepenting saat ini ketika hampir semuanya digital. Namun, buku-buku dapat digantikan oleh hampir semua hal yang berharga. Jika kita mengganti buku dengan kepemilikan judul properti dalam contoh, kita dapat melihat bahwa kepemilikan properti dapat ditransfer dan dikelola melalui *blockchain*. Ketika kepemilikan properti ditransfer, semua orang di jaringan menerima pemberitahuan tentang transfer properti, mayoritas di jaringan menyetujui transfer kepemilikan, dan ditambahkan ke *blockchain* sebagai catatan yang dapat dilihat semua orang.

Jika pemilik properti mencoba menjual hak milik mereka kepada 2 orang yang berbeda, semua orang di jaringan akan melihat transfer duplikat dan salah satu transfer akan ditolak oleh jaringan.

Seperti disebutkan dalam bab sebelumnya, di mana jaringan *blockchain* dapat memiliki potensi paling besar adalah negara-negara di mana perusahaan, lembaga bank, dan pemerintah tidak dapat dipercaya dan pencatatannya manual atau tidak dapat diandalkan. Mampu mengganti database dan institusi terpusat dengan jaringan *blockchain* untuk catatan properti dapat memberikan manfaat besar bagi orang-orang di negara-negara ini. Kami terutama melihat bagaimana teknologi *blockchain* bekerja pada tingkat umum dan membahas beberapa contoh di mana itu dapat digunakan. Nanti di buku ini, kami akan membahas lebih banyak contoh area di mana jaringan *blockchain* dapat menggantikan teknologi dan institusi yang ada.

2.7 RINGKASAN

- Agar suatu transaksi dapat diproses dan dianggap sah, maka transaksi tersebut dikelompokkan dengan transaksi lain dan ditambahkan ke blok baru.
- Blok baru ini ditambahkan "di atas" blok sebelumnya di *blockchain*. Setiap blok mengacu pada nomor blok sebelumnya, menghubungkannya bersama seperti rantai, dari situlah nama "*blockchain*" berasal.
- Rantai blok dalam rantai blok menghubungkan semua jalan kembali ke blok pertama pada rantai yang dikenal sebagai "blok genesis."
- Dengan *blockchain* terdesentralisasi, setiap blok transaksi di *blockchain* diverifikasi oleh jaringan. Semua orang di jaringan menerima informasi tentang transaksi di jaringan; tidak dikendalikan oleh database terpusat yang dimiliki oleh satu perusahaan atau institusi.
- Setelah blok transaksi telah ditambahkan ke *blockchain*, sulit untuk membalikkannya. Setiap blok yang ditambahkan di atas adalah konfirmasi bahwa transaksi tidak akan dibatalkan. Semakin banyak blok di atas, semakin sulit untuk dibalik sampai tidak layak. Di jaringan Bitcoin, 6 blok diterima sebagai konfirmasi bahwa transaksi tidak akan dibatalkan.
- Dengan konsensus terdistribusi, mayoritas komputer di jaringan harus setuju bahwa suatu transaksi sah sebelum diterima di *blockchain*.

- Pengeluaran ganda adalah ketika seseorang di jaringan mencoba untuk menduplikasi transaksi. Ini umumnya dilakukan dengan mengirimkan transaksi lebih dari sekali sebelum salah satunya dikonfirmasi dan diterima ke *blockchain*.
- Serangan pengeluaran ganda adalah ketika pengguna mengontrol lebih dari 50% komputer di jaringan. Hal ini memungkinkan pengguna untuk menggandakan transaksi pembelanjaan dengan mengontrol transaksi mana yang diterima dan ditolak.
- Penambangan adalah proses memvalidasi transaksi dan menambahkan blok baru ke *blockchain*. Hadiah kecil diberikan untuk setiap blok baru yang ditambahkan ke *blockchain*, seperti menambah hadiah kecil dari blok besar.
- Bukti kerja melibatkan pemecahan teka-teki komputer untuk menambahkan blok baru ke *blockchain*. Sulit dipecahkan tetapi mudah dibuktikan, seperti kunci kombinasi. Ini memberikan bukti bahwa daya komputasi dan sumber daya digunakan dan berkontribusi ke jaringan.

BAB 3

SEJARAH *BLOCKCHAIN* DAN BITCOIN

"Saya pikir fakta bahwa dalam dunia bitcoin, sebuah algoritme menggantikan fungsi [pemerintah] sebenarnya sangat keren. Saya penggemar berat Bitcoin."

--Al Gore, Wakil Presiden Amerika Serikat ke-45

Blockchain pertama kali disebutkan dalam kode asli untuk Bitcoin. Meskipun sekarang ada pemisahan antara teknologi *blockchain* dan Bitcoin, sejarah *blockchain* terkait dengan sejarah Bitcoin, jadi bab ini akan membahas sejarah yang saling terkait. Kriptografi adalah fondasi utama yang mendasari *blockchain*. Kriptografi memiliki sejarah panjang dalam melindungi rahasia dan pesan yang berasal dari ribuan tahun yang lalu. Contoh kriptografi kuno yang terkenal adalah "Caesar Cipher" yang digunakan oleh Julius Caesar ketika ia mengirim komunikasi tertulis yang berisi informasi sensitif.

Caesar Cipher melibatkan penggantian setiap huruf dalam pesan dengan huruf alfabet yang berbeda dengan jumlah huruf yang ditentukan. Misalnya, semua huruf dapat dimajukan 3 huruf, A menjadi D, B menjadi E, C menjadi F dan seterusnya sampai setiap huruf dalam pesan diganti. Hanya orang yang mengetahui nomor setiap huruf yang telah dipindahkan yang dapat membaca pesan dengan mudah. Tingkat melek huruf rendah pada saat itu dan ada banyak bahasa berbeda yang digunakan di seluruh dunia, sehingga musuh yang mencegat pesan tidak akan dapat membacanya atau menganggap surat-surat itu ditulis dalam bahasa asing. Ini adalah metode sederhana yang mudah diuraikan hari ini; namun, pada saat itu cukup efektif untuk membuat komunikasi sulit dicegat.

Kriptografi modern telah berkembang jauh dari asalnya, tetapi fondasi dasarnya serupa. Pesan atau data ditutup-tutupi dengan mengganti huruf dan angka sehingga pesan asli tidak dapat dibaca kecuali orang tersebut memiliki kode rahasia atau cara untuk mendekripsinya. Melompat maju ke kriptografi yang mendasari teknologi *blockchain*, beberapa penelitian diterbitkan antara tahun 80-an dan 90-an yang mengusulkan data dapat diamankan melalui kriptografi sambil menautkan data itu dengan aman dalam rantai bersama dengan proposal untuk mata uang digital.

Pada tahun 1982, David Chaum menulis penelitian berjudul "Tanda Tangan Buta Untuk Pembayaran yang Tidak Dapat Dilacak". Karena penelitian ini, David Chaum dikreditkan sebagai penemu uang digital dan tanda tangan buta. Tanda tangan buta menyembunyikan isi pesan sebelum ditandatangani, tanda tangan digital dapat diverifikasi terhadap aslinya sementara isinya tetap tersembunyi, yang merupakan versi awal dari tanda tangan kriptografi yang digunakan oleh mata uang kripto. Penelitian ini dan penelitian selanjutnya yang diterbitkan oleh David Chaum mengusulkan agar pengguna dapat memperoleh dan membelanjakan mata uang digital dengan cara yang tidak dapat dilacak oleh bank atau lembaga lain. David Chaum bersama dengan Amos Fiat dan Moni Naor juga mengusulkan transaksi offline yang dapat mendeteksi jika uang tunai sebelumnya telah dibelanjakan, solusi yang mungkin untuk masalah pengeluaran ganda.

Pada tahun 1990, David mendirikan DigiCash untuk menciptakan mata uang digital berdasarkan ide-ide dalam penelitiannya. Kemudian pada tahun 1994, pembayaran elektronik DigiCash pertama dikirim. Awal dari siaran pers DigiCash tahun 1994 di bawah ini:

"Pembayaran tunai elektronik pertama di dunia melalui jaringan komputer. (Tanggal Rilis: 27 Mei 1994) Uang elektronik memiliki privasi uang kertas, sekaligus mencapai keamanan tinggi yang diperlukan untuk lingkungan jaringan elektronik secara eksklusif melalui inovasi dalam kriptografi kunci publik."

Siaran pers ini 14 tahun sebelum penciptaan Bitcoin, namun jika Anda mengganti kata "uang elektronik" dengan "Bitcoin" dalam siaran pers, itu bisa dikeluarkan sebagai siaran pers untuk Bitcoin hari ini. DigiCash menciptakan sistem uang tunai elektronik pertama yang tidak dapat dilacak oleh bank, pemerintah, atau lembaga lain. Itu menggunakan kriptografi, kunci pribadi dan publik, serta tanda tangan untuk menyembunyikan konten pesan dengan cara yang sama seperti yang dilakukan mata uang kripto saat ini. DigiCash mungkin terlalu maju dari masanya karena kebanyakan orang bahkan belum pernah mendengar tentang internet pada tahun 1994. DigiCash menyatakan kebangkrutan pada tahun 1998 dan asetnya dijual ke teknologi eCash, yang merupakan perusahaan lain yang berfokus pada mata uang digital.

Pada hari-hari awal internet, spam email menjadi masalah yang belum ada solusi untuknya. Pada tahun 1997, Adam Back mengusulkan sebuah sistem untuk membatasi spam email bersama dengan serangan penolakan layanan dengan menggunakan algoritma bukti kerja yang dikenal sebagai hashcash. Algoritma *proof-of-work* ini mengharuskan sistem pengiriman email memecahkan teka-teki komputer, kemudian menempatkan jawabannya di header email. Ini mengharuskan pengirim menggunakan daya komputasi dan sumber daya untuk mengirim email, sehingga lebih sulit untuk mengirim email spam massal. Teka-teki ini sulit dipecahkan untuk pengirim tetapi mudah untuk memverifikasi bahwa jawaban benar untuk penerima email, filter-Mg email spam yang tidak melengkapi bukti kerja ini.

3.1 MATA UANG DIGITAL

Pada tahun 1998, Nick Szabo mengusulkan mata uang digital terdesentralisasi yang disebut "bit emas." Dalam proposal untuk bit gold, orang akan mengalokasikan sumber daya komputasi untuk memecahkan teka-teki kriptografi. Mayoritas jaringan harus menerima jawaban sebagai valid sebelum melanjutkan ke teka-teki berikutnya. Setelah teka-teki dipecahkan dan diterima oleh jaringan, itu akan menjadi bagian dari teka-teki berikutnya yang harus dipecahkan oleh jaringan. Teka-teki itu diberi cap waktu dan ketika setiap jawaban menjadi bagian dari teka-teki berikutnya, teka-teki itu dihubungkan bersama seperti rantai.

Pada saat itu, Nick Szabo menyatakan bahwa mata uang digital menghadapi masalah pengeluaran ganda karena mereka hanya dapat disalin dan ditempel kecuali kontrol diberikan kepada bank sentral atau otoritas. Karyanya tentang emas bit adalah upaya untuk memecahkan masalah pengeluaran ganda ini dikombinasikan dengan mata uang digital terdesentralisasi. Bit emas tidak pernah dibuat sebagai mata uang nyata; itu hanya ada dalam teori. Namun, itu dianggap telah meletakkan dasar bahwa teknologi Bitcoin dan *blockchain* kemudian dibangun.

Pada tahun 1998, Wei Dai menerbitkan penelitian lain berjudul "*B-Money, An Anonymous, Distributed Electronic Cash System.*" Penelitian tersebut menguraikan dasar-dasar untuk *cryptocurrency*, termasuk Bitcoin, dan penelitian tersebut dirujuk dalam penelitian Bitcoin Satoshi Nakamoto.

Dalam penelitian oleh Wei Dai, dinyatakan bahwa sistem kas elektronik memerlukan hal-hal di bawah ini untuk berfungsi:

- Sejumlah pekerjaan komputasi dan bukti pekerjaan itu.
- Hadiah yang dialokasikan untuk pekerjaan komputasi yang diselesaikan.
- Buku besar kelompok kolektif yang diverifikasi dan diperbarui oleh semua anggota.
- Transfer dana diselesaikan pada buku besar kelompok kolektif dan diverifikasi dengan hash kriptografi.
- Semua transaksi ditandatangani dengan tanda tangan digital menggunakan kriptografi kunci publik dan diverifikasi oleh jaringan.

Pada tahun 2000, Stefan Konst menerbitkan penelitian yang memberikan solusi praktis untuk mengimplementasikan rantai yang diamankan secara kriptografis. Itu adalah pekerjaan antara tahun 1980-an hingga 2000-an, bersama dengan penelitian akademis yang diterbitkan, yang meletakkan dasar bagi Bitcoin dan *blockchain*. Pada tahun 2008, Satoshi Nakamoto (yang secara luas dianggap sebagai nama samaran) memposting jurnal penelitian di internet berjudul "*Bitcoin: Sistem Uang Elektronik Peer-to-Peer.*" Penelitian ini menguraikan pembuatan Bitcoin dan blok transaksi yang terhubung dalam rantai. Jurnal ini tidak pernah secara langsung menggunakan kata-kata "rantai blok" bersama-sama ketika mengacu pada metode ini. Pada tahun 2009, Bitcoin menjadi lebih dari sekedar ide dalam penelitian akademis ketika Satoshi Nakamoto menciptakan jaringan Bitcoin bersama dengan *blockchain* pertama. Penyebutan pertama *blockchain* adalah sebagai kata terpisah "rantai blok," dalam kode sumber asli untuk Bitcoin. *Blockchain* pertama ini adalah fitur inti Bitcoin, mencegah pengeluaran ganda dan bertindak sebagai buku besar publik terdistribusi untuk semua transaksi di jaringan Bitcoin. Nakamoto dikreditkan dengan penambangan blok pertama di jaringan Bitcoin yang dikenal sebagai "blok genesis." Di "Blok Kejadian," Satoshi Nakamoto meninggalkan pesan:

"The Times 03/Jan/2009 Rektor di ambang bailout kedua untuk bank"

Pesan ini mungkin telah ditinggalkan sebagai bukti bahwa tanggal pemblokiran dibuat pada atau setelah 31 Januari, bersama dengan komentar tentang kegagalan dalam struktur perbankan dan pasar mata uang saat ini. Karena headline ini berasal dari sebuah surat kabar di Inggris, mungkin Satoshi tinggal di Inggris pada saat itu. Kata "blok" dan "rantai" digunakan secara terpisah dengan Bitcoin dan bahkan ketika itu mendapatkan kesadaran arus utama. Tidak sampai bertahun-tahun kemudian menjadi satu kata: *blockchain*. *Blockchain* Bitcoin asli bukan tanpa kesalahan. Seperti kebanyakan teknologi besar dan usaha bisnis, ada masalah di sepanjang jalan. Selama Agustus 2010, masalah besar pertama dengan protokol Bitcoin ditemukan. Transaksi ditemukan yang telah diubah sebelum dicatat di *blockchain*, merusak transaksi resmi. Entah bagaimana orang-orang melewati batasan bawaan Bitcoin dan

menciptakan jumlah tak terbatas dengan mengubah transaksi asli ke atas dan kemudian membaca sepintas dari atas.

Kerentanan dalam sistem dieksplorasi dan lebih dari 184 miliar bitcoin dihasilkan dari satu transaksi dan dikirim hanya ke dua alamat di jaringan. Dalam beberapa jam transaksi telah terlihat, dan kemudian dihapus, dari *blockchain*. Jaringan Bitcoin mengalami perombakan yang diperbarui, dan hingga hari ini masalah seperti itu belum pernah terjadi. Pada tahun 2011, pasar obat "Silk Road" diluncurkan. Itu adalah situs pasar seperti eBay yang memungkinkan orang untuk membeli dan menjual obat secara online. Bitcoin adalah bentuk pembayaran utama di Silk Road, dan meskipun hal ini menyebabkan peningkatan penggunaan Bitcoin, Bitcoin juga mengaitkan Bitcoin dengan perdagangan narkoba dan aktivitas ilegal.

Bitcoin terus mendapatkan popularitas dan kesadaran publik. Pada tahun 2013, Bitcoin mencapai puncaknya sekitar Rp 15.000.000, dan meskipun ada kritik dari penegak hukum dan pemerintah, itu tampaknya tak terbendung. Kemudian pada tahun 2013, Silk Road ditutup oleh FBI dengan semua aset disita dan penciptanya ditangkap menghadapi hukuman penjara seumur hidup. Sekitar waktu yang sama, pertukaran Bitcoin terbesar Mt. Gox, yang menangani 70% dari semua transaksi Bitcoin, menerima surat perintah, denda, dan menghadapi masalah regulasi dari berbagai departemen pemerintah AS. Pada akhir tahun 2013, Mt. Gox telah menangguhkan penarikan ke Dolar AS dan menyatakan kebangkrutan pada awal tahun 2014.

Cryptocurrency lain mulai bermunculan berdasarkan kode sumber Bitcoin menggunakan *blockchain* yang berbeda. Litecoin dipisahkan dari *blockchain* Bitcoin asli sebagai garpu di *blockchain*; itu menjadi *cryptocurrency* dan *blockchain* terpisah dengan waktu yang lebih rendah untuk menambahkan blok ke *blockchain* bersama dengan perubahan lainnya. Satu blok ditambahkan ke *blockchain* Bitcoin sekitar setiap 10 menit, Litecoin menambahkan satu blok ke *blockchain* setiap 2 setengah menit. Setelah Gunung Gox dan Silk Road ditutup, Bitcoin turun dari puncak Rp 15.000.000 menjadi sekitar Rp 3.000.000. *Cryptocurrency* baru dibuat dan banyak orang secara terbuka menyatakan bahwa Bitcoin telah selesai.

Namun, Bitcoin masih jauh dari selesai. Faktanya, dengan ditutupnya Silk Road, Bitcoin mulai kurang terkait dengan perdagangan narkoba dan kejahatan dan perusahaan mulai memperhatikan teknologi di balik Bitcoin. Masih sulit untuk membuat perusahaan besar, bank, dan perusahaan keuangan untuk menganggap serius Bitcoin karena sulit untuk melupakan kegagalan Gunung Gox, perdagangan narkoba, dan pembunuhan bayaran yang dibayar dengan Bitcoin. Bahkan tanpa kejahatan yang terkait dengannya, banyak orang masih menganggap Bitcoin sebagai uang internet palsu, iseng, gelembung mata uang keuangan, atau penipuan. Kata Bitcoin masih memiliki banyak konotasi negatif di sekitarnya, tetapi kata "*blockchain*" adalah kata yang terhormat untuk digunakan saat membahas teknologi. Menggunakan kata *blockchain* memisahkan teknologi dari mata uang internet Bitcoin atau jaringan Bitcoin. Investor dan lembaga keuangan tidak tertarik dengan Bitcoin, tetapi mereka mulai menjadi sangat tertarik dengan teknologi *blockchain*.

Harga Bitcoin, bersama dengan tingkat minat terhadap Bitcoin rendah pada tahun 2014. Namun, minat terhadap *blockchain* mendapatkan momentum. *Blockchain* mulai digunakan dengan mengacu pada buku besar dan database yang didistribusikan, bukan mata uang. Orang-orang mengusulkan bahwa buku besar manual yang sudah ketinggalan zaman untuk mencatat entri data dapat diganti dengan *blockchain*. Pada tahun 2015, *blockchain* langsung Ethereum diluncurkan. Peluncuran ini membawa kemungkinan teknologi *blockchain* ke tingkat yang lebih tinggi. Jaringan Ethereum memungkinkan aplikasi terdesentralisasi berjalan di *blockchain* bersama dengan kontrak pintar. Kontrak cerdas dan aplikasi terpusat dilihat oleh banyak orang sebagai arah masa depan teknologi *blockchain*, sering disebut sebagai *Blockchain 2.0*.

Sebagian besar bank besar dan perusahaan jasa keuangan di seluruh dunia sedang mengembangkan sistem berbasis *blockchain* untuk menggantikan database atau jaringan yang ada. Dengan kemudahan akses, bersama dengan fungsionalitas yang diberikan oleh aplikasi terdesentralisasi yang dikombinasikan dengan kontrak pintar, ia telah membuka teknologi *blockchain* ke hampir setiap industri. Pemrogram di rumah dapat membangun perangkat lunak yang berjalan di *blockchain* tanpa perlu membuat *blockchain* mereka sendiri. Pada tahun 2017, Harvard Business Review menyatakan bahwa *blockchain* berpotensi menciptakan fondasi baru dalam sistem ekonomi dan sosial.

Pernyataan ini tampaknya adalah bagaimana pengembangan *blockchain* berlangsung; itu mengingatkan pada internet dalam masa pertumbuhan dengan potensi tak terhitung yang baru saja direalisasikan. Perusahaan besar, pemula, pemodal ventura, pemerintah, dan pemrogram semuanya bekerja pada sistem berbasis *blockchain*, basis data, dan aplikasi terdesentralisasi. Sekarang Anda harus memiliki pemahaman tentang apa itu *blockchain* dan sejarah perkembangannya. Dalam bab-bab selanjutnya, kita akan membahas manfaat, kerugian, bahaya, dan potensi masa depan teknologi *blockchain*.

3.2 RINGKASAN

- Kriptografi adalah fondasi yang mendasari *blockchain*. Kriptografi sudah ada sejak ribuan tahun yang lalu ketika pesan ditulis dalam kode untuk melindunginya dari musuh.
- Beberapa penelitian diterbitkan selama 80-an dan 90-an berteori penggunaan kriptografi dikombinasikan dengan rantai data yang aman dan penciptaan mata uang digital.
- 1982 — David Chaum menulis jurnal berjudul "*Blind Signatures For Untraceable Payments*." David Chaum dikreditkan sebagai penemu uang digital dan tanda tangan buta.
- 1990 — David mendirikan DigiCash yang menciptakan mata uang digital yang tidak dapat dilacak menggunakan kriptografi, kunci pribadi dan publik, serta tanda tangan. DigiCash menyatakan kebangkrutan pada tahun 1998 dan asetnya dijual ke teknologi eCash.
- 1997 — Adam Back menciptakan algoritma *proof-of-work* untuk membatasi spam email yang dikenal sebagai hashcash. Itu membutuhkan pengirim email untuk

membuktikan bahwa mereka memecahkan teka-teki komputer sebelum mengirim email. Ini menggunakan daya dan sumber daya komputasi, membuatnya lebih mahal untuk mengirim spam massal

- 1998 — Nick Szabo mengusulkan mata uang digital terdesentralisasi yang disebut "bit emas." Ini menggabungkan bukti kerja yang dikombinasikan dengan jaringan komputer yang menerima bukti kerja sebagai valid dan memasukkannya ke dalam teka-teki berikutnya dengan stempel waktu. Bit emas tidak pernah dibuat sebagai mata uang nyata; itu hanya ada dalam teori.
- 1998 — Wei Dai menerbitkan penelitian lain berjudul, "B-Money, An Anonymous, Distributed Electronic Cash System." Penelitian tersebut tersebut menguraikan dasar-dasar untuk *cryptocurrency*, termasuk Bitcoin, dan penelitian tersebut dirujuk dalam Bitcoin Satoshi Nakamoto.
- Itu adalah pekerjaan selama 1980-an hingga 2000-an, bersama dengan penelitian ini akademis yang diterbitkan, yang meletakkan dasar bagi Bitcoin dan *blockchain*.
- 2008 — Satoshi Nakamoto (yang secara luas dianggap sebagai nama samaran) memposting penelitian di internet berjudul "Bitcoin: Uang Tunai Elektronik Peer-to-Peer *tern." penelitian ini menguraikan pembuatan Bitcoin dan blok transaksi yang terhubung dalam rantai. Penelitian ini tidak pernah secara langsung menggunakan kata-kata "*blockchain*" bersama-sama ketika mengacu pada metode ini.
- 2009 — Bitcoin menjadi lebih dari sekedar ide dalam penelitian akademis ketika Satoshi Nakamoto menciptakan jaringan Bitcoin bersama dengan *blockchain* pertama. Penyebutan pertama *blockchain* adalah sebagai kata terpisah "*Blockchain*" dalam kode sumber asli untuk Bitcoin.
- *Blockchain* pertama ini adalah fitur inti Bitcoin, mencegah pengeluaran ganda dan bertindak sebagai buku besar publik terdistribusi untuk semua transaksi di jaringan Bitcoin.
- Nakamoto dikreditkan dengan penambangan blok pertama di jaringan Bitcoin yang dikenal sebagai "blok genesis" dengan pesan di dalamnya:

"The Times 03/Jan/2009 Kanselir di ambang bailout kedua untuk bank."

Pesan ini mungkin ditinggalkan sebagai bukti bahwa tanggal blok pertama dibuat adalah pada atau setelah 31 Januari, bersama dengan komentar tentang kegagalan dalam struktur perbankan dan pasar mata uang saat ini.

- Pencipta Bitcoin dan *blockchain*, Satoshi Nakamoto, masih belum diketahui. Orang-orang mencurigai Nick Szabo atau Wei Dei sebagai pencipta Bitcoin; Namun, mereka berdua menyangkalnya.
- 2015 — *Blockchain* Ethereum diluncurkan, memungkinkan aplikasi terdesentralisasi dan kontak pintar berjalan di *blockchain*. Fungsionalitas teknologi *blockchain* yang ditingkatkan ini dikenal sebagai *Blockchain 2.0*.

BAB 4

MANFAAT TEKNOLOGI *BLOCKCHAIN*

"Teknologi Blockchain memiliki kemampuan untuk mengoptimalkan infrastruktur global untuk menangani masalah global di ruang ini jauh lebih .. efisien daripada sistem saat ini"

— Marwan Forzley, Pendiri Align Commerce

Dalam beberapa bab pertama, kita telah membahas apa itu blockchain, cara kerjanya, dan beberapa contoh penggunaan potensial. Beberapa manfaat telah disebutkan secara singkat di bab sebelumnya, tetapi dalam bab ini, kita akan membahas lebih detail tentang manfaat teknologi *blockchain*.

4.1 TRANSPARANSI

Sistem berbasis *Blockchain* menawarkan peningkatan transparansi dibandingkan dengan pencatatan dan buku besar yang ada. Perubahan pada buku besar dapat dilihat oleh semua orang di jaringan, dan transaksi tidak dapat diubah atau dihapus setelah dimasukkan ke dalam *blockchain*. Dengan pencatatan yang ada, seseorang dapat pergi dan mengubah database dan menyembunyikan perubahan dari orang lain. Ada banyak contoh di mana kasus penipuan besar-besaran tidak terdeteksi karena buku besar tidak transparan. Kurangnya transparansi ini memungkinkan orang untuk mengubah entri atau memanipulasi data tanpa orang lain mengetahui tentang perubahan tersebut.

Teknologi berbasis *Blockchain* memberikan transparansi kepada semua orang di jaringan, dengan transaksi yang terlihat oleh semua komputer yang terhubung. Majoritas komputer yang terhubung ke *blockchain* harus menyetujui transaksi atau perubahan pada *blockchain* yang mencegah transaksi agar tidak disembunyikan atau dimanipulasi. Semua perubahan hampir real-time; proses ini terjadi saat transaksi disetujui dan ditambahkan ke *blockchain*. Skenario seseorang dalam organisasi yang mencuri uang atau menyembunyikan kerugian perusahaan dengan memanipulasi entri dalam buku besar sangat kecil kemungkinannya terjadi pada buku besar terdistribusi berbasis *blockchain*.

Pindah ke *blockchain* di industri yang berbeda memberikan transparansi di berbagai bidang. Dengan transaksi keuangan, Anda dapat melihat status transfer di *blockchain* secara real time, alih-alih tidak mengetahui status transaksi sampai selesai, yang sering terjadi pada sistem saat ini. Transparansi yang sama ini berlaku untuk apa pun yang bernilai yang dicatat di *blockchain*. Di bab-bab selanjutnya, kita akan melihat industri yang berbeda di mana teknologi *blockchain* sedang dikembangkan dan transparansi yang diberikannya kepada pelanggan dan bisnis dibandingkan dengan sistem yang ada.

4.2 PENGHAPUSAN PERANTARA

Seperti yang dibahas di awal buku ini, sebagian besar transaksi saat ini antara orang-orang membutuhkan perantara seperti bank untuk memberikan kepercayaan dan keamanan untuk transaksi. Keuntungan dari teknologi *Blockchain* dibandingkan sistem yang ada adalah

kemampuan untuk menghapus perantara yang memungkinkan transaksi terjadi secara langsung antara orang-orang alih-alih melibatkan pihak ketiga. Ini sangat menguntungkan miliaran orang di dunia yang tinggal di negara-negara di mana mereka tidak dapat mempercayai perantara pihak ketiga karena pemerintahan yang korup, tingkat kejahatan yang tinggi, peraturan perusahaan yang buruk, pencatatan manual atau pilihan hukum yang terbatas untuk mengajukan klaim. *Blockchain* sangat berguna dalam kasus ini di mana kepercayaan pada perantara tidak ada dan bertransaksi langsung dengan orang-orang juga sulit atau berisiko. *Blockchain* memberikan kepercayaan dan transparansi sekaligus mengurangi risiko yang terlibat dalam transaksi, tanpa perlu pihak ketiga untuk bertindak sebagai perantara dalam transaksi.

4.3 DESENTRALISASI

Desentralisasi database *blockchain* adalah komponen kunci tentang bagaimana perantara dapat dihapus sementara pada saat yang sama meningkatkan transparansi dan kepercayaan. *Blockchains* dipertahankan pada satu buku besar bersama, bukan beberapa buku besar yang dikelola secara pribadi oleh lembaga yang berbeda. Orang dan perusahaan tidak harus menyerahkan kendali kepada satu institusi saat menggunakan *blockchain*. Hal ini membuat kolaborasi antar pihak lebih cepat dan lebih mudah untuk dikelola. Untuk menggunakan contoh sekelompok bank yang mentransfer aset antara satu sama lain, dalam struktur dan sistem saat ini, setiap bank akan memelihara buku besar dan catatan transaksi mereka sendiri secara terpisah. Dengan menggunakan buku besar berbasis *blockchain*, mereka hanya perlu merekonsiliasi transaksi ke satu buku besar bersama yang dapat diakses oleh semua bank dan menyetujui catatan transaksi yang benar.

Struktur *blockchain* yang terdesentralisasi merupakan keuntungan bagi perusahaan yang mungkin menjadi pesaing tetapi bekerja sama sebagai bagian dari kelompok industri atau konsorsium. Sebuah perusahaan mungkin berhati-hati dalam menyerahkan data atau berkolaborasi pada database yang dimiliki oleh pesaing. Pesaing bekerja sama, di mana satu pihak memiliki semua data dapat melibatkan kontrak hukum yang panjang dan perjanjian non pengungkapan yang melindungi privasi dan akses data. Namun, dengan sistem berbasis *blockchain*, pesaing dapat bekerja sama dalam database bersama yang mereka semua memiliki akses dan kendali penuh. Basis data terpusat rentan terhadap peretasan, kehilangan data, dan korupsi. *Blockchain* tidak memiliki database pusat yang merupakan titik kegagalan, manipulasi, atau kerusakan data. Semua komputer di jaringan *blockchain* memiliki salinan *blockchain*, mengurangi risiko kehilangan data. Untuk memanipulasi data pada *blockchain* membutuhkan "peretasan" lebih dari 50% komputer di jaringan pada saat yang sama, yang hampir sepenuhnya tidak layak.

Seperti yang disebutkan sebelumnya dalam buku ini, metode saat ini untuk bertransaksi antar orang membutuhkan kepercayaan pada perantara untuk memfasilitasi prosesnya. *Blockchain* memungkinkan perantara untuk dihapus sambil tetap menjaga kepercayaan dan keamanan antara orang-orang yang terlibat dalam transaksi. Kepercayaan ditempatkan di jaringan *blockchain* alih-alih pihak ketiga. Jaringan *Blockchain* umumnya terdesentralisasi, dengan semua orang yang terhubung ke jaringan memiliki akses ke

blockchain. Penghapusan perantara, peningkatan transparansi, dan struktur desentralisasi *blockchain* telah dibahas di atas. Ini adalah peningkatan kepercayaan antara entitas dalam transaksi yang merupakan manfaat penting yang tidak nyata dari perubahan ini.

Keamanan

Data yang dimasukkan ke dalam *blockchain* tidak dapat diubah, artinya tidak dapat diubah atau diubah. Setiap blok data di *blockchain* juga dapat ditelusuri kembali ke "blok genesis" pertama. Kekekalan data yang dimasukkan blok gabungan yang terhubung sepanjang jalan kembali ke blok pertama di *blockchain*, menciptakan jejak audit yang mudah diikuti dari setiap transaksi di *blockchain*. Sepanjang sejarah, tidak terhitung banyaknya kasus penipuan dan manipulasi data. Seringkali ketika penipuan dilakukan, jejak yang mengarah pada terjadinya penipuan diubah sehingga sulit dan memakan waktu untuk menyelidiki. Jejak data mungkin telah diubah sedemikian rupa sehingga tidak mungkin untuk melacak transaksi dan penipuan.

Dengan sistem berbasis *blockchain*, transaksi masa lalu tidak dapat diubah dengan meninggalkan jejak yang jelas tentang apa yang telah terjadi di *blockchain*. Seperti yang disebutkan di bagian terdesentralisasi dari *blockchain*, mengubah transaksi yang ada akan memerlukan pengendalian lebih dari 50% komputer di jaringan pada saat yang sama, yang hampir sepenuhnya tidak layak. Jika ini memang terjadi, itu juga akan segera terlihat oleh komputer lain yang terhubung ke jaringan. Keamanan *blockchain* tidak sempurna, tetapi sistem yang ada saat ini telah terbukti jauh dari aman berkali-kali. Ini memecahkan banyak masalah keamanan dalam sistem konvensional. Sementara penipuan mungkin tidak akan pernah sepenuhnya dihilangkan, *blockchain* memberikan jejak audit yang jelas kembali ke awal yang memungkinkan upaya penipuan untuk dengan mudah diidentifikasi.

4.4 BERBAGAI POTENSI PENGGUNAAN

Hampir semua hal yang berharga dapat direkam di *blockchain*, frasa "segala sesuatu yang berharga," tidak selalu berarti nilai finansial. Di bab pertama, contoh yang diberikan adalah buku, tetapi ini bisa berupa catatan kepemilikan, identitas digital, lisensi hak cipta, file digital, atau apa pun yang saat ini dapat direkam dalam database. Dengan contoh lisensi hak cipta, ini adalah aset nilai namun lisensi hanya data atau angka yang disimpan dalam database. Nilai berasal dari lisensi yang melindungi kepemilikan dan pendapatan yang diperoleh dari apa yang dilindungi hak cipta.

Ada organisasi dan asosiasi yang mengontrol dan mengelola lisensi hak cipta dalam database terpusat. Lisensi ini adalah aset nilai yang dapat disimpan di *blockchain* menghilangkan kebutuhan organisasi yang mengontrol lisensi. Aset bernilai seperti *cryptocurrency*, lisensi, dan aset digital lainnya hanya dapat ada di *blockchain* sebagai aset *blockchain* asli yang membuatnya lebih mudah untuk dikelola daripada catatan kepemilikan yang ada. Teknologi *Blockchain* adalah teknologi baru yang mudah diakses, terutama dengan inovasi terbaru seperti platform Ethereum dan kontrak pintar. Ini memungkinkan siapa saja untuk mengembangkan aplikasi yang memanfaatkan teknologi *blockchain*.

Blockchain memiliki potensi untuk mengubah hampir setiap industri di dunia. Proyek yang sedang dikembangkan menunjukkan dampak teknologi *blockchain* pada kehidupan sehari-hari dengan banyak perusahaan telah mengembangkan sistem *blockchain* mereka sendiri. Nanti di buku ini, kita akan membahas lebih detail tentang berbagai industri dan penggunaan teknologi *blockchain* dengan contoh proyek yang saat ini sedang dikembangkan.

Mengurangi biaya

Teknologi *Blockchain* dapat secara signifikan mengurangi biaya di banyak industri dengan menghilangkan perantara yang terlibat dalam proses pencatatan dan transfer aset. Setiap perantara atau lapisan yang terlibat dalam transaksi menambah biaya untuk mencatat dan mentransfer aset. Dalam sistem saat ini, saat mentransfer aset atau mencatatnya, seringkali ada beberapa buku besar dan database yang dikelola oleh setiap organisasi. Buku besar terdistribusi memungkinkan pihak untuk mentransfer aset pada satu buku besar bersama, mengurangi biaya pemeliharaan beberapa buku besar di setiap organisasi.

Memelihara buku besar atau database mahal dan seringkali merupakan proses yang sangat manual dengan banyak orang yang terlibat dalam memeriksa integritas setiap buku besar. Buku besar terdistribusi berbasis *Blockchain* mengurangi biaya dengan mengganti buku besar individu dengan satu buku besar bersama, memberikan penyelesaian dan audit nyata dari semua pihak yang terhubung ke jaringan setiap kali terjadi transaksi.

4.5 PENINGKATAN KECEPATAN TRANSAKSI

Sistem berbasis *Blockchain* tidak hanya mengurangi biaya yang terlibat dalam transaksi tetapi juga secara dramatis meningkatkan kecepatan. Dengan menghapus perantara dan menyelesaikan transaksi pada buku besar terdistribusi bersama, buku besar berbasis *blockchain* dapat menyelesaikan transaksi hampir secara instan. Jika Anda telah mentransfer uang dari rekening bank, Anda mungkin memperhatikan bahwa dana tersebut telah dihapus dari rekening Anda; namun, mereka tidak diterima di akun lain sampai beberapa hari kemudian.

Demikian juga, dengan pembelian kartu kredit, transaksi mungkin ditampilkan sebagai tertunda selama beberapa hari pada laporan kartu kredit. Untuk pemilik toko, mereka memberikan barang kepada pembeli tetapi tidak menerima pembayaran hingga beberapa hari kemudian ketika perusahaan kartu kredit menyelesaikan transaksi. Dalam contoh di atas, sistem berbasis *blockchain* sedang dikembangkan untuk meningkatkan kecepatan transaksi ini. Namun, tidak terbatas pada contoh-contoh ini saja, semua jenis transaksi atau transfer nilai berpotensi menggunakan teknologi *blockchain* untuk meningkatkan kecepatan transaksi.

Nanti di buku ini, kita akan membahas contoh dunia nyata dari perusahaan yang mengembangkan sistem berbasis *blockchain* untuk meningkatkan kecepatan transaksi di bidang keuangan dan industri lainnya.

4.6 RINGKASAN

Sebagian besar informasi yang dipublikasikan tentang teknologi *blockchain* berkaitan dengan manfaat, keuntungan, dan hype di sekitar potensinya. Meskipun bab ini telah

membahas banyak manfaat menggunakan sistem berbasis *blockchain*, itu tidak berarti itu sempurna atau jawaban untuk semua masalah dalam suatu industri.

Di bab berikutnya, kita akan membahas beberapa kerugian dan bahaya menggunakan sistem berbasis *blockchain*.

Poin Utama:

- **Transparansi** — *Blockchain* menawarkan peningkatan transparansi yang signifikan dibandingkan dengan pencatatan dan buku besar yang ada untuk banyak industri.
- **Penghapusan Perantara** — Sistem berbasis *Blockchain* memungkinkan penghapusan perantara yang terlibat dalam pencatatan dan transfer aset.
- **Desentralisasi** — Sistem berbasis *Blockchain* dapat berjalan di jaringan komputer yang terdesentralisasi, mengurangi risiko peretasan, waktu henti server, dan kehilangan data.
- **Kepercayaan** — Sistem berbasis *Blockchain* meningkatkan kepercayaan antara pihak-pihak yang terlibat dalam transaksi melalui peningkatan transparansi dan jaringan terdesentralisasi bersama dengan penghapusan perantara pihak ketiga di negara-negara di mana kepercayaan pada perantara tidak ada.
- **Keamanan** — Data yang dimasukkan pada *blockchain* tidak dapat diubah, mencegah penipuan melalui manipulasi transaksi dan riwayat data. Transaksi yang dimasukkan di *blockchain* memberikan jejak yang jelas ke awal *blockchain* yang memungkinkan transaksi apa pun dengan mudah diselidiki dan diaudit.
- **Berbagai kegunaan** — Hampir semua hal yang bernilai dapat direkam di *blockchain*, dan ada banyak perusahaan dan industri yang telah mengembangkan sistem berbasis *blockchain*. Contoh-contoh ini dibahas kemudian dalam buku ini.
- **Teknologi yang mudah diakses** — Seiring dengan penggunaan yang luas, teknologi *blockchain* memudahkan pembuatan aplikasi tanpa investasi infrastruktur yang signifikan dengan inovasi terbaru seperti platform Ethereum. Aplikasi terdesentralisasi, kontrak pintar, dan platform Ethereum dibahas nanti dalam buku ini.
- **Pengurangan biaya** — Buku besar berbasis *Blockchain* memungkinkan penghapusan perantara dan lapisan konfirmasi yang terlibat dalam transaksi. Transaksi yang mungkin memerlukan beberapa buku besar individu dapat diselesaikan pada satu buku besar bersama, mengurangi biaya validasi, konfirmasi dan audit setiap transaksi di beberapa organisasi.
- **Peningkatan kecepatan transaksi** — Penghapusan perantara dan penyelesaian pada buku besar yang didistribusikan, memungkinkan kecepatan transaksi yang meningkat secara dramatis dibandingkan dengan berbagai sistem yang ada.
- **Kekurangan** — Ada berbagai alasan kuat untuk berubah dari sistem yang ada ke sistem berbasis *blockchain*. Namun, ada juga kerugian dan risiko yang tidak boleh diabaikan.

BAB 5

BAHAYA MENGGUNAKAN *BLOCKCHAIN*

Blockchain dirancang khusus untuk satu tujuan utama: mencegah "pengeluaran ganda" koin elektronik, tanpa otoritas pusat. Beberapa kasus penggunaan yang diperdebatkan rentan terhadap pengeluaran ganda atau apa pun yang serupa. Pada saat yang sama, banyak tujuan keamanan penting yang tidak disediakan oleh blockchain sama sekali.

Thud blockchain tidak diperlukan atau tidak cukup untuk banyak aplikasi yang disarankan; dalam praktiknya itu direkayasa secara besar-besaran, atau tidak lengkap, atau keduanya.

--Steve Wilson, *Beyond the Hype: Memahami Tautan Lemah di Blockchain*

Teknologi *Blockchain* disebut-sebut oleh banyak orang sebagai solusi untuk semua masalah di industri dan dunia saat ini. Ada *start-up blockchain* baru dan *cryptocurrency* yang diluncurkan setiap hari menjanjikan untuk melakukan segalanya mulai dari mengganggu sistem perbankan hingga menghilangkan kemiskinan dunia. Banyak klaim yang mengingatkan kita pada internet di masa-masa awalnya. Sementara internet memang mengubah dunia, banyak klaim yang dilebih-lebihkan, kerangka waktu yang tidak realistik, dan banyak perusahaan rintisan yang diprediksi akan sukses bangkrut. Dalam bab ini, kita akan melihat beberapa masalah dan kerugian dari teknologi *blockchain*.

5.1 KURANGNYA PRIVASI

Blockchain yang terdesentralisasi tidak memiliki privasi, yang akan membuat penerimaan penuh menjadi sulit. Tidak hanya informasi yang tidak bersifat pribadi, tetapi juga dapat diakses kapan saja oleh siapa saja yang menggunakan sistem. Relatif mudah untuk mengetahui identitas akun di *blockchain* Bitcoin setelah menerima pembayaran dari orang itu. Jika Anda pergi ke toko dan melakukan pembayaran, pemilik toko akan dapat melihat transaksi itu di *blockchain*. Informasi dalam transaksi akan menunjukkan dompet dari mana dana dikirim, mereka kemudian dapat memeriksa akun itu dan dapat melihat berapa banyak uang yang Anda miliki dan semua transaksi Anda masuk dan keluar dari akun itu.

Gagasan bahwa *blockchain* terdesentralisasi secara efektif mempublikasikan setiap transaksi yang mereka lakukan ke jaringan publik mengkhawatirkan banyak orang. Terutama dalam kasus pembelian di dalam toko di mana identitas dapat diarahkan ke akun dan transaksi. Ini juga memprihatinkan mengingat komputer yang menjalankan sejumlah besar jaringan *blockchain* berada di negara-negara seperti Rusia dan China di mana kejahatan komputer tinggi dan informasi pribadi dapat digunakan terhadap orang yang tinggal atau bepergian ke negara-negara tersebut.

Ada *blockchain* terdesentralisasi yang memberikan lebih banyak privasi dengan transaksi atau membatasi orang yang memiliki akses untuk melihat informasi. Namun, Bitcoin, Ethereum, dan banyak *cryptocurrency* *blockchain* terbesar tidak beroperasi dengan cara ini dan saat ini tidak memiliki rencana untuk menerapkan privasi lebih lanjut seputar transaksi atau akun.

5.2 MASALAH KEAMANAN

Aset berbasis *Blockchain* seperti uang tunai, jika uang tunai di dompet Anda dicuri atau hilang, maka hilang. Sistem berbasis *blockchain* menggunakan kriptografi dan enkripsi canggih yang lebih aman daripada kata sandi internet standar atau kode akses nomor. Namun, lebih aman terkadang dapat mengakibatkan sistem menjadi kurang aman. Ada banyak contoh dengan *cryptocurrency* di mana seseorang telah melupakan kunci pribadi mereka dan tidak dapat mengakses uang mereka. Anda hanya perlu melihat utas forum di internet dari orang-orang yang menyatakan peringatan untuk tidak kehilangan kunci pribadi Anda bersama dengan cerita tentang bagaimana mereka kehilangan kunci mereka dan sekarang tidak dapat mengakses uang di dompet mereka.

Kasus-kasus ini sering terjadi ketika seseorang telah membeli *cryptocurrency* tertentu dengan harga murah tetapi tidak terlalu memperhatikannya. Mereka kemudian mengetahui bahwa mata uangnya telah naik banyak dan bahwa investasi kecil awal bernilai ribuan dolar sekarang dan mencoba mengaksesnya lagi. Bitcoin senilai Rp 750.000 pada tahun 2009 akan bernilai lebih dari satu juta dolar 8 tahun kemudian, jadi mudah untuk melihat bagaimana hal ini dapat terjadi dengan kenaikan harga yang begitu besar pada jumlah uang yang awalnya kecil. Kasus yang dipublikasikan dengan baik adalah James Howells di Inggris, yang membuang laptopnya yang berisi 7.500 bitcoin di dalamnya. Pada harga hari ini, ini bernilai lebih dari Rp 225.000.000.000.

Karena transparansi *blockchain*, jika orang memiliki kunci publik mereka, mereka dapat melihat saldo mereka dan berapa nilainya tetapi tidak memiliki cara untuk mengaksesnya. Ini setara dengan bank yang dapat memberi tahu Anda saldo di rekening bank Anda, tetapi Anda tidak memiliki cara untuk mengaksesnya. Dengan rekening bank tradisional, jika Anda kehilangan kata sandi untuk internet banking, kartu kredit Anda atau lupa nomor rekening bank Anda, Anda dapat pergi ke bank dan membuktikan identitas Anda untuk mendapatkan akses lagi. Ini tidak terjadi dengan *cryptocurrency* berbasis *blockchain* yang terdesentralisasi seperti Bitcoin. Ada miliaran dolar dalam *cryptocurrency* yang dicuri melalui peretasan, penipuan, atau keamanan yang buruk selama beberapa tahun terakhir.

Jika seseorang mendapatkan akses ke kartu kredit Anda dan menarik dana, Anda dapat menelepon bank dan meminta mereka membatalkan kartu Anda sehingga pencuri tidak dapat menarik dana lagi. Bank kemungkinan akan memiliki perlindungan penipuan dan dapat membalikkan transaksi dan melacak pembayaran. Dengan sistem berbasis *blockchain*, transaksi tidak dapat diubah atau dibatalkan, dan tidak ada perantara untuk membantu Anda jika terjadi penipuan pada akun Anda. Jika Anda mengirim dana ke nomor rekening (dompet) yang salah di *blockchain*, maka dana tersebut hilang. Jika seseorang mendapatkan akses ke kunci pribadi Anda, mereka dapat menarik semua uang di akun Anda, dan tidak ada cara untuk membalikkan transaksi itu atau mengklaim kompensasi.

Pertanyaan pertama pada halaman pertanyaan yang paling sering diajukan dari sistem berbasis *blockchain* adalah "bagaimana cara mereset kata sandi saya jika saya lupa atau kehilangannya?" Jawabannya adalah "Anda tidak bisa." Saran yang diberikan kepada orang-orang saat menyiapkan kunci pribadi di *blockchain* adalah untuk "menuliskannya di suatu tempat." Semua kriptografi dan keamanan yang canggih itu mengakibatkan orang-orang

menuliskan kunci pribadi dan menyimpannya di rumah atau di komputer mereka, mengurangi keamanan jika dibandingkan dengan metode keamanan tradisional. Ketika berhadapan dengan implementasi arus utama sistem berbasis *blockchain*, banyak metode keamanan yang membuat aset *blockchain* lebih aman akan membuat adopsi arus utama lebih sulit. Dompet *blockchain* berbasis web sangat populer, di mana orang menyimpan *cryptocurrency* dengan perusahaan pihak ketiga. Saat menggunakan dompet berbasis web pihak ketiga, orang mengorbankan manfaat keamanan dari *blockchain* seperti kunci pribadi demi kata sandi tradisional yang dapat diatur ulang jika mereka tetap melupakannya.

5.3 TIDAK ADA KONTROL TERPUSAT

"Di pasar keuangan selalu ada mekanisme untuk memperbaiki serangan. Di blockchain tidak ada mekanisme untuk memperbaikinya — orang harus menerimanya."
- Robert Sams, pendiri dan kepala eksekutif Clearrnatics yang berbasis di London.

Sistem berbasis *Blockchain* dirancang untuk mengantikan perantara pihak ketiga, menempatkan tanggung jawab dan kontrol kembali dengan individu yang terlibat dalam transaksi. Kontrol ini ditempatkan pada sebagian besar orang di jaringan, menciptakan masalah terkait dengan kontrol *blockchain*. Sifat terdesentralisasi dari banyak *blockchain* berarti bahwa jaringan harus menyetujui dan memutuskan arah masa depan jaringan dan *blockchain*. Dengan jaringan dan perangkat lunak tradisional, jika suatu organisasi ingin membuat perubahan, mereka dapat membuat perubahan itu setelah mendapat persetujuan dari departemen terkait di dalam organisasi. Dengan jaringan *blockchain* terdesentralisasi seperti Bitcoin, perubahan harus disetujui oleh sebagian besar jaringan, ini mungkin lebih dari 50% tetapi bisa setinggi 70% hingga 80% dari jaringan.

Contoh terbaru dari hal ini adalah divisi dalam jaringan Bitcoin tentang penerapan SegWit (Segregated Witness) atau Bitcoin Unlimited. Sejumlah besar jaringan mendukung perubahan yang berbeda untuk jaringan Bitcoin dan tidak ada pihak yang bisa mendapatkan majoritas yang diperlukan untuk membuat perubahan. Ketidaksepakatan itu berarti *cryptocurrency* lain dan jaringan *blockchain* telah mampu bergerak di depan Bitcoin dalam hal perubahan teknologi. Ketidaksepakatan telah menyebabkan jaringan Bitcoin mandek dengan waktu transaksi yang lambat, waktu konfirmasi yang lambat, dan masalah skalabilitas yang berkelanjutan.

Teknologi seperti perangkat lunak terus berubah dari waktu ke waktu. Jaringan *blockchain* yang terdesentralisasi dapat mengakibatkan pembagian arah perubahan, terutama jika ada kegagalan untuk mencapai kesepakatan mayoritas. Jika kesepakatan mayoritas tercapai, masih akan ada banyak orang di jaringan yang tidak setuju dengan perubahan yang telah dilakukan. Ini membuat jaringan terdesentralisasi berisiko bagi organisasi untuk digunakan. Sebuah perusahaan dapat membangun bisnis atau perangkat lunak di sekitar jaringan di mana mereka tidak memiliki kendali atas perubahan yang secara dramatis dapat berdampak pada perangkat lunak dan bisnis mereka.

5.4 RISIKO SERANGAN 51%

Melanjutkan dari masalah kontrol, jika seseorang dapat mengontrol lebih dari 50% komputer di jaringan *blockchain*, mereka akan mengontrol transaksi di *blockchain*. Pengguna jahat yang mengendalikan lebih dari 50% komputer di jaringan *blockchain* dikenal sebagai "serangan 51%."

Memanfaatkan kontrol ini atas jaringan *cryptocurrency*, mereka secara teoritis akan dapat memblokir transaksi baru dari konfirmasi, membalikkan transaksi, dan memungkinkan "pengeluaran ganda" koin yang ditakuti.

Serangan 51% pada jaringan *blockchain* bersifat teoretis karena akan sulit untuk mengontrol jaringan dalam jumlah besar. Namun, ada peternakan pertambangan besar yang didirikan di Cina, Rusia, dan bagian lain dunia yang mengendalikan sebagian besar kekuatan komputasi jaringan *blockchain*. Jika peternakan pertambangan besar ini berkolaborasi, mereka berpotensi mengambil alih jaringan *blockchain* dan memanipulasinya untuk keuntungan mereka. Bahkan tanpa mengendalikan 51% dari jaringan, mereka masih dapat memanipulasi jaringan dengan mengalokasikan daya komputasi mereka dengan cara yang mempengaruhi perkembangan jaringan di masa depan. Inilah yang terjadi dengan divisi mengenai jaringan Bitcoin yang disebutkan sebelumnya.

5.5 TEKNOLOGI BARU YANG BELUM TERBUKTI

Sistem berbasis *blockchain* adalah teknologi baru yang belum terbukti yang terutama diterapkan pada *cryptocurrency*. Ada kekurangan aplikasi dunia nyata yang saat ini ada untuk membuktikan keefektifan teknologi. Teknologi ini baru dengan banyak potensi, tetapi sebagian besar aplikasi potensial bersifat teoritis. Pepatah "Buat perangkap tikus yang lebih baik dan dunia akan membuka jalan ke pintu Anda" adalah kesalahan bisnis yang umum hanya karena teknologinya mungkin lebih baik daripada sistem yang ada dalam banyak hal, itu tidak berarti bahwa orang ingin menggunakan daripada sistem yang sudah ada.

Seperti disebutkan sebelumnya, keamanan kriptografi lebih unggul dari metode keamanan yang ada; namun, jika Anda kehilangan kunci ke banyak sistem berbasis *blockchain*, Anda tidak dapat memulihkannya. Orang-orang memilih untuk menuliskan kunci pribadi mereka di atas kertas atau menyimpannya di komputer mereka, sehingga mereka tidak melupakannya, sehingga menghilangkan manfaat dari keamanan tambahan dan berpotensi membuat sistem menjadi kurang aman. Manfaat lain dari jaringan *blockchain* adalah menghapus perantara pihak ketiga. Proses menghubungkan ke jaringan *blockchain*, mengirim transaksi, menyiapkan kunci pribadi rumit dan berisiko bagi banyak orang. Banyak orang lebih suka memberikan akses ke kunci pribadi mereka ke perantara pihak ketiga dengan dompet web atau perangkat lunak serupa, yang menghilangkan manfaat utama lain dari jaringan *blockchain*.

5.6 BIAYA

Algoritma *proof-of-work* yang digunakan banyak jaringan *blockchain* memerlukan bukti bahwa daya komputasi dan sumber daya dikontribusikan ke jaringan sebelum blok ditambahkan ke jaringan. Bukti ini berupa jawaban atas teka-teki yang ditempelkan pada blok

tersebut untuk jaringan untuk memastikan kebenarannya. Memecahkan teka-teki ini membutuhkan sejumlah besar daya komputasi dan listrik. Profesor John Quiggin dari University of Queensland telah menghitung bahwa setiap setengah jam jaringan Bitcoin menggunakan jumlah listrik yang sama dengan rata-rata rumah tangga AS dalam satu tahun penuh.

Rata-rata rumah tangga AS menggunakan 10 hingga 12.000 kWh listrik setiap tahun, hampir sama dengan yang dibutuhkan untuk menghasilkan empat Bitcoin senilai sekitar Rp 15.000.000. Karena tingginya biaya listrik untuk menjalankan komputer di jaringan *blockchain* menggunakan algoritma bukti kerja ini, ada keuntungan bagi negara-negara di mana listriknya murah atau untuk organisasi yang memiliki kesepakatan khusus dengan perusahaan energi. Karena kesulitan teka-teki pada *blockchain* Bitcoin meningkat, konsumsi listrik juga akan meningkat, membuatnya lebih mahal dan intensif sumber daya untuk menjalankan *blockchain* dengan algoritma *proof-of-work* dalam skala besar.

5.7 KURANGNYA SKALABILITAS

Pada tingkat konsumsi energi saat ini, biaya listrik untuk menjalankan *blockchain* menggunakan algoritma *proof-of-work* membuatnya tidak layak untuk menangani jumlah transaksi oleh perusahaan kartu kredit seperti Visa dan MasterCard. Ini adalah salah satu faktor yang saat ini mempengaruhi skalabilitas jaringan *blockchain*. Satu blok ditambahkan ke *blockchain* Bitcoin setiap 10 menit, setiap blok saat ini berisi sekitar 2.000 transaksi, artinya jaringan Bitcoin memproses sekitar 3 transaksi per detik. Karena batasan ukuran blok, jaringan Bitcoin hanya mampu menangani sekitar 7 transaksi per detik. Visa telah melakukan tes dengan IBM yang menyimpulkan bahwa jaringan Visa mampu menangani lebih dari 20.000 transaksi per detik.

Jika Anda pergi ke toko dan menggunakan kartu kredit Anda tetapi tidak memiliki cukup uang untuk melakukan pembelian, sistem kartu kredit akan menolak transaksi tersebut. Bitcoin *blockchain* tidak memiliki mekanisme seperti ini. Transaksi di *blockchain* Bitcoin akan memakan waktu minimal 10 menit untuk ditambahkan ke *blockchain* dan perusahaan dapat menunggu beberapa blok lagi untuk ditambahkan sebelum menerima transaksi, untuk memastikan transaksi tidak akan dibalik.

Membandingkan perbedaan antara kedua metode tersebut, jika Anda pergi ke toko untuk membayar dengan Bitcoin, pemilik toko mungkin harus menunggu satu jam untuk memastikan transaksi dikonfirmasi dengan beberapa blok yang ditambahkan ke *blockchain* di atas blok yang berisi transaksi. Ada jaringan *blockchain* yang jauh lebih cepat daripada jaringan Bitcoin. Namun, tidak ada yang memiliki tingkat popularitas atau penerimaan yang sama sebagai bentuk pembayaran seperti Bitcoin. Bahkan *blockchain* dan *cryptocurrency* yang memiliki waktu konfirmasi transaksi lebih cepat masih tidak memiliki kapasitas untuk menskalakan ke tingkat jaringan pembayaran keuangan yang ada seperti Visa atau MasterCard. Karena masalah skalabilitas ini, banyak orang melihat implementasi *blockchain* dalam skala besar sebagai tidak lebih dari buku besar resmi informasi yang dicap waktu.

5.8 KEPERCAYAAN, REPUTASI, DAN PEMAHAMAN TENTANG BLOCKCHAINS

Masih kurangnya pemahaman tentang bagaimana *blockchain* bekerja bersama dengan reputasi yang ternoda dari koneksi dengan Bitcoin. Bitcoin adalah penggunaan *blockchain* yang paling umum dikenal; banyak orang memiliki hubungan yang kuat dengan Bitcoin dan kejahatan. Meskipun semakin diterima arus utama sebagai metode pembayaran yang sah, teroris, dan kejahatan komputer membawa Bitcoin kembali ke berita yang mengulangi tautan itu.

Contoh terbaru adalah jaringan komputer di National Health Service di Inggris. Virus komputer mengunci komputer NHS, mencegahnya diakses kecuali sejumlah uang tebusan dibayarkan dalam Bitcoin. Ini membawa Bitcoin menjadi berita utama di Inggris, dengan surat kabar menghubungkan Bitcoin dengan kejahatan komputer anonim, peretas, dan teroris. Rumah sakit tidak dapat mengakses catatan pasien, berpotensi mengancam nyawa orang yang membutuhkan perawatan medis selama ini.

Blockchain mengklaim untuk menciptakan kepercayaan di antara orang-orang tanpa perlu mempercayai perantara pihak ketiga untuk transaksi. Namun, orang masih perlu percaya pada jaringan *blockchain* dan komputer anonim yang menjalankannya. Sulit untuk membuat orang mempercayai sistem yang digunakan secara terbuka oleh penjahat terutama karena banyak komputer yang menjalankan jaringan berada di luar negeri yang tidak diatur atau dikendalikan oleh pemerintah mereka.

Insiden kejahatan yang terkait dengan Bitcoin adalah alasan mengapa perusahaan yang mengembangkan sistem berbasis *blockchain* mencoba untuk menjauhkan hubungan antara Bitcoin dan *blockchain*. Istilah "buku besar terdistribusi" telah menjadi lebih populer baru-baru ini, untuk lebih menciptakan kesenjangan antara Bitcoin dan teknologi berbasis *blockchain* baru. Manfaat sistem berbasis *blockchain* sulit dipahami banyak orang. Seperti disebutkan sebelumnya, banyak orang sudah memilih perantara pihak ketiga untuk mengakses *blockchain*, dan mereka menggunakan kata sandi standar untuk masuk ke situs web yang menghilangkan manfaat utama dari teknologi *blockchain*. Banyak orang tidak suka orang lain dapat melihat saldo atau transaksi mereka atau aspek lain dari *blockchain* dan lebih memilih sistem yang ada. Pemahaman publik, kepercayaan, dan persepsi jaringan *blockchain* akan menjadi penting untuk mengarusutamakan penerimaan teknologi. Mungkin butuh waktu lama bagi masyarakat umum untuk mempercayai jaringan *blockchain* dan bertransaksi dengan nyaman di jaringan tersebut.

5.9 REGULASI DAN INTEGRASI

"Pemain dan analis keuangan terbesar di dunia sibuk membicarakan penemuan yang menjadi terkenal sebagian dengan berjanji untuk menghancurkannya."

- Mike Gault-

Aset berbasis *blockchain* menghadapi proses regulasi dan masalah integrasi yang panjang dengan sistem yang ada. Pemerintah dan bank menolak perubahan karena skala dan biaya penggantian sistem yang ada. Kecuali sistem berbasis *blockchain* dapat membuktikan bahwa mereka akan memberikan penghematan biaya atau manfaat yang signifikan untuk

membenarkan penggantian sistem yang ada, kecil kemungkinan institusi besar seperti pemerintah atau bank akan menggunakannya dalam waktu dekat. Pemerintah Estonia sedang menguji sistem berbasis *blockchain*, tetapi Estonia memiliki populasi kurang dari 1,5 juta. Ada kota-kota di Amerika Serikat, Cina, dan negara-negara lain dengan 10 kali populasi ini. Sementara sistem berbasis *blockchain* dapat bekerja dalam skala kecil, tidak mudah untuk mengintegrasikannya pada skala yang dibutuhkan untuk pemerintah seperti AS atau bank besar.

Konsorsium dan riak R3 adalah contoh buku besar berbasis *blockchain* atau terdistribusi yang terintegrasi dengan banyak perusahaan keuangan dari berbagai negara. Ada perusahaan keuangan yang menahan transisi mereka untuk menggunakan buku besar berbasis *blockchain* karena skala "kecil" di mana *blockchain* telah diuji. Jika sejumlah besar lembaga keuangan pindah ke teknologi baru yang belum teruji dan menggunakannya ketika masalah ditemukan, itu bisa menimbulkan risiko yang sangat signifikan terhadap pasar keuangan dan data pelanggan.

Ada juga kekhawatiran dari *Financial Stability Oversight Counsel* (FSOC) bahwa beberapa sistem berbasis *blockchain* bisa lebih rentan terhadap penipuan daripada yang saat ini dipahami dengan pengujian skala kecil. Masalah lain dengan beberapa lembaga keuangan yang mengadopsi sistem berbasis *blockchain* bersama atau buku besar terdistribusi adalah area di mana regulator bekerja. Sistem berbasis *blockchain* secara teoritis dapat menjangkau banyak yurisdiksi peraturan dan batas-batas nasional yang berbeda, semakin menggelapkan perairan antara regulator dan yurisdiksi mana transaksi harus ditangani.

Lembaga keuangan besar akan berhati-hati untuk pindah ke sistem di mana peraturan pemerintah tidak jelas. Risiko keuangan dan bisnis terlalu tinggi jika pemerintah tidak memiliki peraturan yang jelas tentang bagaimana aset berbasis *blockchain* diperlakukan. Kekhawatiran regulasi, biaya integrasi bersama dengan kurangnya aplikasi skala besar dari sistem berbasis *blockchain* akan menyebabkan lambatnya penyerapan teknologi dari lembaga keuangan besar dan pemerintah.

5.10 PROMOSI SENSASIONAL

Banyak tulisan tentang teknologi *blockchain* bisa disebut evangelis atau overhyped, dengan klaim bahwa teknologi berbasis *blockchain* akan mengubah dunia, mengganggu pemerintah, menghilangkan bank, memecahkan kemiskinan dunia, dan mungkin memberi Anda otot-otot keras tanpa berolahraga. Klaim terakhir tentang otot perut itu tidak benar, tetapi mengingat hype seputar *blockchain*, tidak mengherankan jika ada perusahaan baru di Silicon Valley yang mengajukan ide itu ke perusahaan modal ventura sekarang. Sangat mudah untuk terjebak dalam hype teknologi baru; internet tidak berbeda. Itu adalah teknologi revolusioner yang telah mengubah dunia, tetapi banyak prediksi di masa-masa awal internet adalah "kegembiraan yang tidak rasional".

Perkiraan kerangka waktu tentang dampak teknologi baru sangat bervariasi dan seringkali sangat diremehkan. Seperti disebutkan dalam sejarah bab *blockchain*, DigiCash dan uang digital lainnya serta teknologi berbasis kriptografi ada sekitar beberapa dekade sebelum Bitcoin tetapi terlalu dini dalam prediksi adopsi pasar terhadap teknologi tersebut. Bahkan jika

banyak prediksi tentang dampak teknologi *blockchain* akurat, mereka tidak akan memiliki dampak arus utama pada masyarakat selama bertahun-tahun yang akan datang. Perusahaan rintisan yang mempelopori teknologi sekarang, mungkin tidak dapat bertahan cukup lama untuk melihat teknologi mereka mencapai pasar massal. Seperti yang disebutkan sebelumnya dalam bab ini, bahkan ketika orang ingin menggunakan Bitcoin dan sistem berbasis *blockchain*, banyak yang masih memilih metode yang diklaim sebagai pengganti *blockchain*. Ini menghilangkan kebutuhan akan sistem berbasis *blockchain* di tempat pertama jika orang lebih memilih sistem yang ada daripada manfaat yang diharapkan dari *blockchain*. Teknologi *blockchain* hanyalah cara baru untuk menyimpan dan mengelola data. Itu bukan jawaban untuk semua masalah dunia, jadi jangan percaya semua hype.

5.11 RINGKASAN:

- **Kurangnya Privasi** - Banyak *blockchain* yang terdesentralisasi tidak bersifat pribadi. Saldo akun dan transaksi dapat diakses oleh siapa saja di jaringan untuk melihatnya.
- **Masalah Keamanan** - Aset berbasis *blockchain* seperti uang tunai—jika Anda kehilangan uang tunai di dompet Anda atau dicuri, uang itu hilang. Banyak metode keamanan di *blockchain* akan membuat adopsi arus utama lebih sulit dan mungkin kurang aman daripada metode yang ada saat orang menuliskan kunci pribadi sehingga mereka tidak melupakannya.
- **Tanpa Kontrol Terpusat** - Dengan jaringan *blockchain* yang terdesentralisasi seperti Bitcoin, perubahan harus disetujui oleh sebagian besar jaringan, ini mungkin lebih dari 50% tetapi bisa mencapai 70% hingga 80% dari jaringan. Tidak ada satu organisasi pun yang memiliki kendali atas perubahan atau arah *blockchain* terdesentralisasi yang membuatnya berisiko bagi bisnis untuk digunakan karena mereka tidak dapat mengontrol perubahan apa pun pada sistem.
- **Risiko serangan 51%** - Banyak komputer yang menjalankan *blockchain* di seluruh dunia akan berada di negara-negara yang secara historis tidak nyaman bagi orang-orang karena kejahatan, sistem hukum yang lemah, atau kurangnya regulasi. Biaya listrik dan komputer yang rendah di negara-negara ini telah menyebabkan pusat-pusat besar menambang blok di *blockchain*. Jika pusat data ini berkolaborasi, mereka dapat berpotensi awalnya mengontrol lebih dari 50% jaringan dan mengambil alih kendali itu.
- **Teknologi baru yang belum terbukti** - Teknologi *blockchain* adalah teknologi baru yang belum terbukti yang terutama diterapkan pada mata uang kripto. Masih ada perangkat lunak atau perusahaan dunia nyata yang terbatas yang menggunakan teknologi *blockchain* untuk membuktikan bahwa itu bermanfaat bagi sistem yang ada.
- **Biaya** - Dibutuhkan sejumlah besar energi untuk menyalakannya. Diperkirakan bahwa setiap setengah jam jaringan Bitcoin menggunakan jumlah listrik yang sama dengan rata-rata rumah tangga AS dalam satu tahun penuh.
Catatan: Perhitungan tentang konsumsi listrik didasarkan pada konsumsi rumah rata-rata di Amerika Serikat sebesar 10.000 hingga 12.000 kWh listrik. Ini setara dengan jumlah listrik untuk menghasilkan 4 blok pada *blockchain* Bitcoin.

- **Masalah skalabilitas** - Jaringan *blockchain* belum terbukti mampu menskalakan secara efektif ke tingkat yang sama dari sistem yang ada. Jaringan Bitcoin hanya mampu menangani sekitar 7 transaksi per detik. Namun, jaringan Visa mampu menangani lebih dari 20.000 transaksi per detik.
- **Reputasi dan kepercayaan** - Bitcoin adalah penggunaan *blockchain* yang paling umum dikenal, yang memiliki hubungan kuat dengan terorisme, perdagangan narkoba, dan kejahatan. Orang perlu percaya pada jaringan *blockchain* yang mereka gunakan, terutama jika itu mengantikan perantara yang dapat dipercaya. Banyak orang akan ragu-ragu mempercayai jaringan *blockchain* yang juga terkait dengan kegiatan kriminal.
- **Kurangnya pemahaman tentang teknologi blockchain** - Cara kerja *blockchain* dan manfaatnya sulit dipahami banyak orang. Orang-orang juga memiliki kekhawatiran tentang aspek jaringan *blockchain* seperti saldo dan transaksi mereka menjadi publik. Meski manfaatnya sudah dipahami, banyak orang masih lebih memilih sistem yang sudah ada.
- **Regulasi dan integrasi** - Sistem berbasis *blockchain* akan menghadapi masalah regulasi bersama dengan biaya dan memakan waktu masalah integrasi dengan sistem yang ada. Pemerintah dan bank menolak perubahan karena skala dan biaya penggantian sistem yang ada.
- **Hype** - Ada banyak hype seputar kemampuan sistem berbasis *blockchain*. *Blockchain* hanyalah tipe database baru; itu bukan solusi ajaib yang sering digembar-gemborkan. Itu juga masih belum terbukti dalam skala besar atau dengan banyak aplikasi praktis di luar *cryptocurrency*.

BAB 6

BLOCKCHAIN DAN INDUSTRI KEUANGAN

"Teknologi Blockchain terus mendefinisikan ulang tidak hanya bagaimana sektor pertukaran beroperasi, tetapi ekonomi keuangan global secara keseluruhan."

— Bob Greifilci, Kepala Eksekutif NASDAQ

Bitcoin adalah penggunaan teknologi *blockchain* pertama yang stabil di seluruh dunia dan dengan cepat menarik perhatian industri keuangan. Banyak perusahaan jasa keuangan tidak melihat banyak potensi dalam Bitcoin sampai mereka memeriksanya lebih lanjut dan memahami teknologi *blockchain* di baliknya. Begitu mereka menyadari apa yang mampu dilakukan oleh teknologi *blockchain*, mereka menuangkan jutaan dolar ke dalam penelitian, pengembangan, dan akuisisi untuk mengembangkan *blockchain* mereka sendiri. Memanfaatkan teknologi berbasis *blockchain* dalam dunia keuangan memiliki banyak keuntungan. Kemampuan *blockchain* untuk memproses informasi lebih cepat dengan menghilangkan perantara berpotensi menurunkan biaya sekaligus meningkatkan kecepatan. Ini dapat diterapkan pada transfer mata uang, perdagangan saham, pembayaran, penyelesaian, dan banyak kegiatan yang merupakan operasi inti dari lembaga keuangan.

Mentransfer nilai adalah proses yang lambat dibandingkan dengan rata-rata lama transaksi keuangan. Terkadang diperlukan waktu berminggu-minggu untuk mentransfer uang ke negara tertentu dengan nilai tukar yang seringkali tidak pasti pada saat transfer. Buku besar berbasis *blockchain* tidak hanya dapat mengurangi biaya biaya transfer nilai, tetapi juga dapat mempercepat proses secara signifikan karena penghapusan saluran perantara yang harus dilalui informasi untuk memvalidasi transaksi. Untuk bank, teknologi *blockchain* menawarkan peningkatan kecepatan transaksi sambil mengganti lapisan otentikasi dengan transparansi transaksi. Bank menyelesaikan transfer pada buku besar internal; ini dapat dilakukan pada waktu pemrosesan yang berbeda untuk setiap bank. Hal ini sering mengakibatkan transfer dana dihapus dari buku besar satu bank tetapi tidak muncul di buku besar bank lain selama beberapa hari kemudian.

Di negara berkembang di mana pemukiman mungkin lebih manual, ini bisa memakan waktu lebih lama dan rentan terhadap kesalahan. Mengganti proses ini dengan *blockchain* akan memungkinkan bank untuk segera menyelesaikan transfer pada buku besar yang didistribusikan dengan semua orang di jaringan dapat melihat transaksi. Perdagangan saham beroperasi dengan cara yang hampir sama. *blockchains* dapat digunakan untuk mengurangi waktu yang dibutuhkan dalam proses penyelesaian serta meningkatkan akurasi perdagangan. Faktanya, NASDAQ telah membuat *blockchain* untuk perdagangan saham. Saat ini, *blockchain* yang dijalankan NASDAQ sedang digunakan untuk perdagangan saham pra-IPO, mentransfer kepemilikan saham perusahaan swasta antara investor sebelum mereka terdaftar di bursa saham. NASDAQ *blockchain* beroperasi sekarang, menunjukkan seberapa dekat dunia untuk memiliki sistem *blockchain* di banyak industri.

Setelah transaksi pertama yang mengalihkan kepemilikan saham antar investor, Bob Greifeld menyatakannya sebagai momen penting dalam penerapan teknologi *blockchain* dan kemajuan besar di sektor keuangan global.

Tidak peduli seberapa besar potensi manfaat dari teknologi *blockchain*, apakah lembaga keuangan siap untuk menerapkan teknologi ini? Apakah mereka bersedia mempercayai jutaan dan berpotensi miliaran dolar transaksi untuk diproses menggunakan teknologi *blockchain*? Jawaban singkatnya adalah, ya. Industri jasa keuangan adalah salah satu industri pertama yang menerima manfaat yang datang dengan memanfaatkan teknologi *blockchain*. Banyak perusahaan sudah menggunakan teknologi *blockchain*, seperti contoh NASDAQ yang disebutkan sebelumnya. Hampir setiap lembaga keuangan besar di dunia saat ini terlibat dalam pengembangan teknologi *blockchain* melalui pengembangan internal atau joint venture dengan perusahaan lain. Nasdaq, Visa, Citibank, Capital One telah menginvestasikan lebih dari Rp 450 juta di chain.com untuk membangun buku besar terdistribusi untuk transaksi antar lembaga keuangan.

6.1 Ripple

Ripple adalah jaringan pembayaran yang dapat digunakan untuk mentransfer berbagai mata uang, komoditas, atau apa pun yang bernilai menggunakan buku besar yang didistribusikan. Jaringan pembayaran Ripple sedang digunakan oleh bank-bank besar dan lembaga keuangan di seluruh dunia sebagai jaringan penyelesaian, memungkinkan bank untuk mengirim pembayaran internasional waktu nyata dengan biaya yang jauh lebih rendah daripada metode yang ada. Saat ini, 15 dari 50 bank teratas dunia bekerja dengan Ripple dalam mengembangkan platform *blockchain*.

Paolo Cederle, CEO UniCredit, dikutip mengatakan: "*Blockchain* dan teknologi terkait adalah perubahan paradigma dari status quo dan semakin menjadi fokus utama inovasi bagi kami. Melalui kemitraan kami dengan Ripple, kami mengoptimalkan pembayaran global kami sebagai salah satu bank besar pertama yang menerapkan teknologi keuangan terdistribusi dalam pengaturan komersial."

Perusahaan teknologi R3 telah bekerja dengan 25 bank besar termasuk Wells Fargo, JP Morgan, dan Citibank. Perusahaan yang terlibat dalam proyek ini dikenal sebagai konsorsium R3. R3 adalah teknologi basis data terdistribusi yang memiliki beberapa pengembang profil tinggi dari inti bitcoin, kriptografi, dan industri teknologi yang mengerjakannya. Buku besar terdistribusi yang mereka buat berbeda dari *blockchain* tetapi memiliki banyak kesamaan. Sebelas bank dalam konsorsium R3 telah terhubung ke buku besar terdistribusi R3.

Nama menonjol lainnya yang mengembangkan teknologi *blockchain* adalah The Bank of England. Mereka mengatakan akan berkomitmen untuk merombak fondasi basis data mereka dan menerapkan *blockchain*. Bank of England memiliki tim yang didedikasikan untuk *blockchain*, menyatakannya sebagai inovasi teknologi utama. Bank of England berharap dapat memanfaatkan teknologi untuk membantu pertahanannya terhadap serangan siber yang semakin meningkat, membantu sistem mereka dalam memungkinkan pembayaran nonbank untuk menyelesaikan transaksi lebih cepat, dan membuatnya lebih kompatibel dengan teknologi yang terus berubah. Bank of England awalnya berencana untuk menggunakan

secara internal, tetapi mereka telah berjanji untuk membuka teknologi tersebut ke lebih banyak bisnis pada tahun 2020. Jika mereka tetap setia pada kata-kata mereka, maka teknologi berbasis *blockchain* akan diuji pada sistem penyelesaian kotor waktu nyata, menangani ratusan miliar transaksi perbankan setiap hari.

Estonia adalah negara lain yang menerapkan teknologi *blockchain*. Pemerintah Estonia memelopori teknologi digital untuk pemerintah dengan mengembangkan *blockchain* untuk identifikasi dan catatan kesehatan dengan area lain seperti pengumpulan pajak dengan pemungutan suara yang direncanakan untuk berpotensi dibangun di atas fondasi ini. Teknologi *blockchain* dengan cepat diadopsi oleh industri keuangan dan bank sentral, tetapi juga menjadi lebih populer dengan lembaga di luar keuangan. Bab berikutnya membahas perusahaan di luar keuangan yang memanfaatkan teknologi baru ini untuk mengubah industri mereka.

6.2 RINGKASAN

- Mentransfer nilai antara perusahaan dan negara saat ini merupakan proses yang lambat. Teknologi *blockchain* menawarkan peningkatan kecepatan transaksi dengan potensi transfer instan *real-time*.
- Teknologi *blockchain* dapat menggantikan lapisan otentikasi dengan transparansi transaksi.
- Banyak bank, bank sentral, pemerintah, dan perusahaan keuangan telah memanfaatkan teknologi *blockchain* atau sedang meneliti dan mengembangkannya.
- Perdagangan saham melibatkan transfer kepemilikan antara orang-orang. *Blockchain* dapat digunakan untuk menggantikan perantara aries dan proses perdagangan dengan Nasdaq sudah menerapkan *blockchain* yang berfungsi.
- Banyak fungsi administrasi dan penyelesaian yang dilakukan oleh lembaga keuangan sudah ketinggalan zaman dan manual. Fungsi-fungsi ini berpotensi diganti dengan *blockchain* dan buku besar yang didistribusikan.

BAB 7

BLOCKCHAIN DAN INDUSTRI SELAIN KEUANGAN

"Blockchain dan teknologi terkait adalah perubahan paradigma dari status quo dan semakin menjadi fokus utama inovasi bagi kami.

Paolo Cederle, CEO Solusi Terintegrasi Bisnis UniCredit

Pada bab sebelumnya, kita melihat bagaimana industri keuangan dengan cepat mengadopsi teknologi *blockchain*. Sementara *blockchain* memiliki hubungan yang kuat dengan pembayaran dan transaksi, sebagian besar karena dimulai dengan Bitcoin, potensi teknologi *blockchain* jauh lebih besar dari sekedar pembayaran dan sektor keuangan. *blockchain* memiliki potensi untuk mengubah hampir setiap industri di dunia. Proyek dalam pengembangan menunjukkan dampak teknologi *blockchain* pada kehidupan sehari-hari. Dalam bab ini, kita akan membahas potensi penggunaan *blockchain* dengan contoh perusahaan yang saat ini membangun sistem berbasis *blockchain*.

7.1 MANAJEMEN IDENTITAS DAN IDENTITAS DIGITAL

Manajemen identitas yang memanfaatkan teknologi *blockchain* adalah inovasi utama yang dapat membuka jalan bagi keamanan dan fondasi industri lain. Jika Anda dapat mempercayai seseorang yang mereka klaim, maka Anda dapat menghubungkannya ke berbagai aplikasi lain. Teknologi *blockchain* memecahkan banyak masalah yang ada dengan identitas digital. Saat ini, relatif mudah untuk membuat identitas palsu atau mencuri identitas orang lain secara online. Kata sandi tidak aman, dan basis data terpusat rentan terhadap serangan. Setelah database terpusat diserang, mungkin menyediakan akses ke semua data pelanggan yang tersimpan di sistem. Sistem identifikasi berbasis *blockchain* menyediakan tanda tangan digital menggunakan kriptografi.

Mereka unik, tak terbantahkan, aman, dan hampir tidak mungkin diduplikasi atau diakses tanpa otorisasi. Identifikasi berbasis *blockchain* adalah kemungkinan nyata di masa depan dengan pemerintah Estonia dan perusahaan seperti ShoCard telah membangun sistem identitas di *blockchain*. Kedepannya, ini dapat digunakan untuk Identitas digital, paspor, SIM, izin tinggal, akta kelahiran, akta nikah, dan bentuk identifikasi lainnya.

7.2 PEMUNGUTAN SUARA DIGITAL

Setelah membangun teknologi yang memungkinkan identitas digital dan tanda tangan digital, mudah untuk mengotentikasi identitas seseorang untuk berbagai transaksi dan tindakan online lainnya. Pemungutan suara digital adalah teknologi yang gagal diterapkan dengan sukses di seluruh negara karena risiko keamanan dan masalah privasi. Estonia, Denmark, dan Norwegia telah bereksperimen dengan pemungutan suara digital; namun, hanya Estonia yang berhasil menjalankan pemungutan suara digital skala besar.

Denmark telah menggunakan teknologi *blockchain* untuk pemungutan suara skala kecil dengan Aliansi Liberal, sebuah partai politik di Denmark yang menggunakan sistem

pemungutan suara *blockchain* pada tahun 2014. Dengan menggunakan sistem pemungutan suara berbasis *blockchain*, pemilih dapat memeriksa apakah suara mereka berhasil dikirim, sambil tetap menjaga privasi dan menyembunyikan identitas mereka. Ini juga akan membuat pemungutan suara lebih mudah diakses oleh banyak orang, yang berpotensi meningkatkan partisipasi pemilih dalam pemilihan.

7.3 PERAWATAN KESEHATAN DAN REKAM MEDIS

Blockchain menyediakan buku besar terdistribusi di mana ketika perubahan dibuat dalam satu buku besar, semua salinan lainnya diperbarui secara bersamaan. Ini memastikan bahwa setiap orang memiliki data valid terbaru yang cocok dengan semua salinan di jaringan. Banyak potensi telah diterapkan dalam industri kesehatan. Jika Anda pernah mengunjungi lebih dari satu dokter atau rumah sakit, Anda akan menyadari bahwa setiap kali Anda mengunjungi dokter atau rumah sakit baru, itu melibatkan banyak dokumen tentang riwayat kesehatan Anda, alergi, dan pertanyaan medis lain yang mungkin Anda miliki diselesaikan beberapa kali sebelumnya di lokasi lain.

Menyimpan informasi ini pada database bersama catatan kesehatan berarti bahwa dokter, rumah sakit, ahli bedah, perawat, dan profesional kesehatan akan memiliki akses ke data bersama tentang pasien. Mereka akan memiliki rincian lengkap dari catatan medis, menghemat waktu dan membantu mereka untuk membuat keputusan yang lebih komprehensif ketika merawat pasien. Ini bisa berpotensi menyelamatkan nyawa dalam kasus pasien yang dilarikan ke operasi. Catatan dari setiap masalah kesehatan yang mendasari, golongan darah, alergi terhadap obat-obatan tertentu, kontak darurat, obat-obatan saat ini yang mungkin mereka pakai atau perincian lainnya akan langsung dapat diakses bila diperlukan.

Rincian riwayat penyakit pasien sebelumnya juga akan membantu menyelesaikan teka-teki tentang apa yang mungkin menyebabkan masalah kesehatan pada pasien. Kunjungan ke dokter untuk satu kondisi mungkin tidak memicu alasan untuk khawatir, tetapi bila dikombinasikan dengan kunjungan ke dokter lain atau profesional kesehatan untuk kondisi yang tampaknya tidak terkait, ini mungkin menandakan gejala masalah yang belum terdiagnosis. Setiap profesional kesehatan mungkin hanya memiliki satu gejala yang memberikan mereka hanya sebagian dari gambarannya, tetapi dengan informasi tambahan, mereka dapat mendiagnosis pasien dengan lebih baik.

Perusahaan asuransi kesehatan dapat menghemat banyak uang dan waktu dengan memiliki akses ke database ini juga. Jika Anda melamar asuransi kesehatan, saat ini membutuhkan banyak pertanyaan dan tes medis yang bisa sangat invasif, memakan waktu, dan tidak nyaman. Dengan memberikan akses ke catatan kesehatan Anda ke perusahaan asuransi, mereka akan memiliki gambaran lengkap tentang riwayat kesehatan Anda dan dapat membuat keputusan asuransi berdasarkan informasi ini tanpa perlu tes dan pertanyaan ekstensif.

Perusahaan seperti Gem, Tieroim, dan Philips Healthcare saat ini sedang mengerjakan *blockchain* untuk catatan kesehatan. Estonia memimpin di antara negara-negara di bidang ini. Otoritas eHealth Estonia telah bekerja dengan perusahaan teknologi *Blockchain Guardtime*

untuk memasukkan data medis warga ke dalam database *blockchain* yang aman. Otoritas Administrasi Jalan Estonia telah menerima sertifikat medis digital untuk memastikan seseorang dalam keadaan sehat untuk mengemudi sebelum memperbarui lisensi mereka. Ini sebelumnya merupakan proses manual untuk warga negara tetapi menjadi digital dan otomatis. Di masa depan, catatan kesehatan di *blockchain* dapat diperbarui dengan informasi seperti apakah seseorang sehat untuk mengemudi. Departemen pemerintah akan memiliki akses ke informasi ini dan sistem akan secara otomatis mengeluarkan pembaruan berdasarkan informasi dalam catatan kesehatan *blockchain*.

Blockchain catatan kesehatan menawarkan manfaat bagi individu maupun profesional kesehatan. Individu akan memiliki pandangan yang lebih transparan dan akurat tentang catatan medis dan data kesehatan mereka. Tidak ada pemerintah atau perusahaan yang dapat mengubah informasi ini tanpa pasien, bersama dengan semua orang di jaringan, menyadarinya. Estonia telah membuat portal pasien, di mana warga memiliki akses penuh ke riwayat medis, resep, perincian rujukan, dan informasi asuransi mereka. Di portal pasien, mereka juga dapat menyatakan apakah akan menjadi donor organ dan membuat keputusan tentang perawatan mereka selama operasi. Di masa depan, basis data catatan kesehatan ini mungkin ada di *blockchain*. Dengan Estonia yang memimpin dengan cepat, ini mungkin hanya beberapa tahun lagi untuk menjadi kenyataan.

7.4 SERTIFIKAT AKADEMI

Sekolah Holbertson di California berencana menggunakan teknologi *blockchain* untuk mengotentikasi sertifikat akademiknya. Memalsukan transkrip dan sertifikat akademik adalah praktik umum dengan siswa yang mengklaim kualifikasi yang tidak mereka peroleh. *Blockchain* akan menciptakan transparansi seputar catatan dan kualifikasi akademik siswa. Memungkinkan mereka untuk diverifikasi dengan mudah, menghilangkan penipuan sambil menghemat waktu dan uang untuk memeriksa atau membuktikan kualifikasi secara manual.

7.5 MUSIK

Industri musik sudah mengembangkan teknologi berbasis *blockchain* untuk digunakan dalam berbagai cara yang berbeda. Ada beberapa perusahaan yang mengembangkan aplikasi berbasis *blockchain* untuk mengubah cara musik didistribusikan, dibagikan, dibeli, dan bagaimana royalti penjualan akan dibayarkan kepada artis. Peertracks, Uio Music, dan Mycelia hanyalah beberapa perusahaan rintisan yang bekerja pada platform berbasis *blockchain* bagi artis untuk menjual musik mereka langsung ke penggemar mereka tanpa perlu label rekaman atau perantara. Spotify baru-baru ini membeli Mediachain, yang mengembangkan sistem berbasis *blockchain* yang memungkinkan artis membuat rekaman digital untuk lagu di *blockchain* Bitcoin dan Sistem File InterPlanetary. Spotify bertujuan untuk memanfaatkan platform *blockchain* dari Mediachain untuk menciptakan pembayaran yang lebih adil dan lebih transparan kepada artis untuk musik mereka.

7.6 PENYIMPANAN CLOUD

Perusahaan penyimpanan cloud seperti Google Drive, Dropbox, dan Microsoft OneDrive telah menjadi standar untuk menyimpan data dan file. Banyak orang menggunakan penyimpanan cloud untuk menyimpan semua jenis data pribadi dan bisnis. Penyimpanan cloud saat ini membutuhkan banyak kepercayaan pada perusahaan pihak ketiga. Orang sering meletakkan semua data mereka di satu tempat, dengan satu perusahaan penyimpanan cloud yang hanya memerlukan kata sandi dengan keamanan rendah untuk mengaksesnya. Sistem penyimpanan cloud terpusat rentan terhadap serangan dan kata sandi dapat dengan mudah diperoleh melalui metode peretasan atau penipuan dasar.

Ada beberapa *start-up* yang memberikan alternatif dengan menggabungkan penyimpanan cloud dengan teknologi *blockchain*. Perusahaan seperti Storj telah menciptakan penyimpanan cloud terdesentralisasi yang tidak terlalu rentan terhadap serangan dan peretasan. Penyimpanan cloud didistribusikan di ruang penyimpanan yang tidak digunakan pada komputer yang terhubung ke jaringan, dienkripsi dan hanya dapat diakses oleh pemiliknya. Siacoin dan Filecoin adalah perusahaan rintisan yang juga bekerja untuk menggabungkan penyimpanan cloud dan *blockchain* seperti Storj.

7.7 RENTAL MOBIL

Industri mobil adalah industri lain yang dapat diubah oleh teknologi *blockchain*. Visa dan DocuSign telah menjalin kemitraan untuk mengembangkan sistem berbasis *blockchain* untuk penyewaan mobil. Ini akan memotong banyak dokumen dan perantara yang terlibat dalam penyewaan mobil. Pelanggan memilih mobil yang ingin mereka sewa, identitas digital mereka sudah berisi informasi keuangan dan lisensi, mereka menyetujui polis asuransi untuk sewa dan blok rantai diperbarui dengan perjanjian sewa baru.

Penyewaan mobil jangka pendek di bandara bergerak ke arah yang lebih otomatis menghilangkan kebutuhan akan dokumen dan proses yang panjang sebelum menyewa mobil. Teknologi yang dikembangkan untuk penyewaan mobil dan identitas digital juga dapat diterapkan pada penyewaan mobil. Rekam medis banyak warga di Estonia sudah didigitalkan dan diteruskan ke Otoritas Jalan untuk memperbarui lisensi secara otomatis. Penautan informasi *blockchain* dan identitas digital ini juga dapat digunakan untuk menyetujui persewaan mobil secara otomatis di masa mendatang.

7.8 BERBAGI PERJALANAN

Aplikasi berbagi perjalanan seperti Uber telah mengganggu industri taksi dan mengubah transportasi bagi jutaan orang di seluruh dunia. Perusahaan taksi memiliki monopoli atas transportasi mobil di banyak kota di seluruh dunia dengan satu organisasi mengendalikan semua lisensi taksi untuk sebuah kota. Sementara Uber dan aplikasi berbagi perjalanan lainnya menyediakan alternatif untuk Taksi, mereka masih merupakan basis data terpusat dengan sistem yang semuanya dikendalikan oleh satu perusahaan.

Berbagi tumpangan adalah antara pengemudi dan penumpang; namun, dengan platform berbagi perjalanan saat ini, masih ada perantara antara semua interaksi dan transaksi perjalanan. Teknologi *blockchain* akan memungkinkan untuk menghapus perantara

apa pun dan membuat aplikasi berbagi perjalanan yang terdesentralisasi. Perusahaan rintisan La'zooz saat ini sedang mengerjakan platform berbagi perjalanan terdesentralisasi berbasis *blockchain*. *Ride-sharing* adalah industri yang akan menjadi penyesuaian mudah untuk menggantikan platform yang ada dengan *blockchain*. Keamanan pengemudi akan menjadi perhatian; namun, begitu identitas digital yang terkait dengan *blockchain* otoritas jalan atau leasing mobil dan *blockchain* sewa adalah praktik umum, berbagi perjalanan dapat berintegrasi dengan baik dengan *blockchain* tersebut.

7.9 PROPERTI

Penjualan properti, real estat, dan tanah adalah area yang saat ini melibatkan banyak dokumen manual dan perantara untuk memfasilitasi transaksi. Transaksi properti melibatkan catatan yang seringkali sulit diperoleh, rentan terhadap kesalahan, salah tempat, atau proses yang lambat. Catatan dan transaksi properti berbasis *blockchain* dapat secara dramatis meningkatkan kecepatan dan transparansi transaksi properti sekaligus mengurangi biaya transaksi. Platform berbasis *blockchain* real estat dapat merekam kepemilikan tanah, mentransfer akta properti, melacak perubahan zonasi atau rencana pembangunan dan hampir semua properti yang saat ini dicatat oleh perusahaan atau pemerintah daerah. Ubiquity adalah perusahaan rintisan yang saat ini membangun platform properti berbasis *blockchain* untuk bank, lembaga keuangan, pialang hipotek, dan orang biasa untuk melacak dokumen yang terkait dengan transaksi properti.

7.10 SEWA APARTEMEN

Airbnb adalah contoh lain dari platform seperti Uber yang mendisrupsi industri dengan menyediakan platform yang memungkinkan orang untuk menyewakan apartemen mereka kepada orang lain di kota-kota di seluruh dunia. Airbnb menghapus perantara seperti hotel dan agen perjalanan, menyatukan orang untuk bertransaksi satu sama lain. Meskipun ini merupakan langkah ke arah menghilangkan perantara, itu masih hanya menggantikan perantara dengan platform lain untuk memfasilitasi transaksi antar orang. Platform penyewaan hotel dan apartemen berbasis *blockchain* dapat beroperasi seperti Airbnb tetapi tanpa perantara yang memfasilitasi semua transaksi dan pemesanan. Ini akan dilakukan secara langsung antara orang-orang di *blockchain*.

7.11 INDUSTRI PERJALANAN

Bahkan platform pemesanan hotel yang lebih tradisional dapat digantikan oleh sistem pemesanan berbasis *blockchain*. John Guscic, direktur pelaksana Webjet, menyatakan bahwa 'Sekitar 1 dari 25 transaksi pemesanan hotel di seluruh dunia berakhir di mana seseorang menyediakan layanan tetapi tidak dibayar.'

Hal ini disebabkan oleh banyaknya perantara yang terlibat dalam industri pemesanan hotel dan perjalanan di mana pemesanan hilang atau salah bayar. Sistem pemesanan berbasis *blockchain* akan menciptakan sistem pemesanan yang lebih transparan dan tidak rentan terhadap kesalahan. Webjet saat ini bekerja dengan Microsoft untuk mengembangkan sistem

berbasis *blockchain* untuk industri perjalanan; namun, saat ini tidak ada kerangka waktu untuk rilis tersebut.

7.12 PROGRAM LOYALITAS / HADIAH

Program Loyalitas / Imbalan adalah hal yang umum di sebagian besar industri, mulai dari kedai kopi lokal hingga maskapai besar. Namun, program hadiah seringkali mahal untuk dijalankan, rentan terhadap penipuan, dan pelanggan sering merasa tidak puas dengan hadiah yang diterima atau proses untuk memeriksa saldo dan menukar hadiah. Teknologi *blockchain* menawarkan solusi untuk banyak masalah yang dihadapi program loyalitas / penghargaan yang ada. Perusahaan jasa keuangan Deloitte menerbitkan sebuah penelitian berjudul "Menjadikan *blockchain* Nyata Untuk Program Hadiah Loyalitas Pelanggan" yang meneliti bagaimana program loyalitas berbasis *blockchain* dapat menguntungkan perusahaan dan pelanggan.

Penelitian tersebut menyatakan bahwa program loyalitas pelanggan yang ada menderita dari partisipasi klien yang rendah, waktu pemrosesan yang lambat, penipuan, dan biaya tinggi untuk dijalankan. Program loyalitas berbasis *blockchain* akan lebih transparan sekaligus secara signifikan mengurangi waktu pemrosesan, biaya, dan meningkatkan keamanan. Ketika sebuah transaksi terjadi di mana pelanggan akan mendapatkan poin loyalitas, itu akan terjadi secara real time sebagai lawan dari waktu pemrosesan yang lambat untuk mengkredit saldo ke pelanggan sekarang. Perusahaan dapat lebih mulus mengintegrasikan program loyalitas yang memungkinkan peluang nilai tambah bagi pelanggan dan peluang bisnis potensial dengan berbagi program dengan perusahaan pelengkap.

Sebuah perusahaan start-up bernama Loyyal telah bekerja dengan teknologi besar, akuntansi, dan perusahaan lain dalam membangun program loyalitas berbasis *blockchain*. Dengan transparansi, pengurangan biaya, dan peningkatan kecepatan, hadir program loyalitas dan penghargaan yang lebih baik bagi perusahaan dan pelanggan mereka.

7.13 PREDIKSI DAN PERJUDIAN

Industri perjudian diatur untuk diubah oleh startup *blockchain* yang muncul. Bukan hanya perjudian di acara olahraga yang akan berubah tetapi seluruh industri prediksi, termasuk prediksi pasar keuangan dan prediksi. Salah satu *cryptocurrency* yang tumbuh paling cepat adalah Augur, yang mengembangkan pasar prediksi di mana orang dapat memprediksi dan mendapat untung dari hasil peristiwa. Augur akan menjadi platform terdesentralisasi untuk memperkirakan kemungkinan terjadinya peristiwa apa pun. Sistem ini didasarkan pada penelitian yang menunjukkan bahwa pasar prediksi telah terbukti lebih akurat dari waktu ke waktu daripada analis individu, pakar, survei, atau jajak pendapat.

Dalam jajak pendapat, banyak orang menanggapi dengan apa yang mereka inginkan terjadi sebagai hasil dari suatu peristiwa, bukan apa yang mereka pikir akan terjadi. Inilah sebabnya mengapa hasil pemilu dan jajak pendapat bisa sepenuhnya tidak akurat dengan hasil yang sangat berbeda dari prediksi jajak pendapat. Pasar prediksi meminta orang untuk "menempatkan uang mereka di tempat mereka berada," seperti kata pepatah, dan

mempertaruhkan uang pada hasil dari peristiwa yang terjadi yang mengarah ke hasil yang lebih akurat dari waktu ke waktu.

7.14 RINGKASAN

Contoh dalam bab ini menunjukkan bahwa teknologi *blockchain* mungkin merupakan inovasi besar berikutnya di berbagai industri. Contoh-contoh ini hanyalah puncak gunung es dalam hal kemampuan teknologi *blockchain*. Banyak aplikasi teknologi *blockchain* akan dikelola menggunakan kontrak pintar. Di bab selanjutnya, kita akan melihat kontrak pintar, aplikasi terdesentralisasi, platform Ethereum, dan contoh lain dari kemampuan teknologi *blockchain*.

Poin Utama

- Bukan hanya perusahaan jasa keuangan yang menerapkan sistem berbasis *blockchain*. Teknologi Blockchain memiliki berbagai kegunaan di berbagai industri.
- Teknologi berbasis *blockchain* dapat digunakan untuk mentransfer dan merekam hampir semua hal yang berharga.
- Banyak perusahaan telah mengembangkan sistem *blockchain* mereka sendiri, dengan beberapa sistem berbasis *blockchain* yang sudah bekerja dan tersedia sekarang.
- Di masa depan, perantara dan platform dapat digantikan oleh platform *blockchain*.
- Teknologi *blockchain* adalah kenyataan yang jauh lebih dekat daripada yang mungkin disadari banyak orang. Dalam beberapa tahun ke depan, kemungkinan akan ada berbagai industri yang menerapkan teknologi *blockchain*.

BAB 8

ETHEREUM, KONTRAK CERDAS, DAN APLIKASI TERDESENTRALISASI

"Memberi pengguna akses mudah ke berbagai jenis aset digital di blockchain, terutama token yang terkait dengan aset di dunia nyata, sangat penting untuk melihat adopsi blockchain mencapai tingkat berikutnya..."

Vitalik Buterin Chief Scientist Ethereum

8.1 PENGANTAR ETHEREUM

Ethereum adalah langkah selanjutnya di masa depan teknologi *blockchain*. Itu dibangun dari teknologi dasar yang sama dengan *blockchain* Bitcoin; namun, dibutuhkan kemungkinan teknologi *blockchain* ke tingkat yang lebih tinggi. Ethereum adalah *blockchain* dengan bahasa pemrograman yang memungkinkan aplikasi dan kontrak pintar berjalan di atas *blockchain* yang mendasarinya. Ini memungkinkan pengembang untuk membuat program yang berjalan di *blockchain* dan menggunakan kekuatan komputasi dari ribuan komputer yang terhubung ke jaringan *blockchain*. Hampir semua aplikasi yang berjalan di komputer saat ini berpotensi berjalan di *blockchain*. Dengan memanfaatkan jaringan Ethereum, pengembang dapat dengan cepat membuat aplikasi dengan mudah tanpa perlu membuat *blockchain* dan *cryptocurrency* mereka sendiri.

Jaringan Ethereum menggunakan *cryptocurrency* "Ether," which bertindak sebagai mata uang di jaringan. Ether ditukar sebagai pembayaran untuk menjalankan aplikasi terdesentralisasi di jaringan. *cryptocurrency* Ether adalah *cryptocurrency* terbesar kedua berdasarkan kapitalisasi pasar setelah bitcoin dengan kapitalisasi pasar lebih dari Rp10 miliar.

8.2 PERBEDAAN ANTARA ETHEREUM DAN BITCOIN

Perbedaan utama antara Bitcoin dan Ethereum adalah bahwa Bitcoin terutama digunakan sebagai buku besar terdistribusi untuk transaksi keuangan, tetapi Ethereum dirancang untuk digunakan sebagai platform komputasi terdistribusi untuk menjalankan aplikasi. Bitcoin dapat digunakan untuk membayar barang dan jasa di mana pun mereka diterima, mata uang jaringan Ethereum "Ether" dirancang untuk digunakan oleh pengembang untuk membayar daya komputasi pada jaringan saat menjalankan aplikasi terdesentralisasi. Bitcoin dan Ethereum keduanya memiliki mata uang digital tetapi dari sudut pandang keseluruhan, mereka berbeda dalam tujuan. Inti dari Ether bukanlah untuk memantapkan dirinya sebagai alternatif pembayaran tetapi untuk mendorong pengembang untuk membuat dan menjalankan aplikasi dalam Ethereum.

Sederhananya: Bitcoin terutama merupakan mata uang untuk transaksi keuangan. Ethereum memiliki banyak aspek. Meskipun memiliki *cryptocurrency* sendiri ("ether"), tidak hanya itu yang dimilikinya. Mata uang adalah salah satu bagian kecil dari jaringan karena Ethereum juga memiliki seluruh platform komputasi di atas *blockchain*.

8.3 MANFAAT ETHEREUM

Karena jaringan *blockchain* Ethereum dijalankan oleh ribuan komputer di seluruh dunia, aplikasi dapat dijalankan menggunakan kekuatan komputasi dari jaringan komputer global yang sangat besar. Salah satu masalah dengan jaringan Bitcoin adalah bahwa ia lebih kuat daripada gabungan superkomputer teratas di dunia, namun kekuatan pemrosesan itu terbuang sia-sia untuk menghasilkan angka acak untuk menambahkan blok ke *blockchain*. Ethereum menempatkan semua komputer yang terhubung ke jaringan dan kekuatan pemrosesannya untuk penggunaan yang lebih baik yang memungkinkan pengembang untuk membuat aplikasi yang berjalan menggunakan kekuatan pemrosesan gabungan jaringan bersama dengan teknologi *blockchain*.

Pengembang tidak perlu membuat *blockchain* mereka sendiri dan menghubungkan komputer dengannya. Ethereum memiliki jaringan komputer yang sudah mapan di *blockchain* Ethereum. Platform Ethereum juga memiliki bahasa pemrograman Ethereum Virtual Machine dan Solidity. Soliditas dapat digunakan untuk membuat aplikasi terdesentralisasi atau kontrak pintar yang kemudian dikompilasi oleh Mesin Virtual Ethereum dan dijalankan di *blockchain*.

8.4 APLIKASI TERDESENTRALISASI (DAPPS)

Aplikasi Terdesentralisasi adalah aplikasi yang bersifat open source, tidak dikendalikan oleh satu orang atau entitas dan dijalankan melintasi *blockchain* atau jaringan komputer yang terdistribusi, dApps tidak memiliki server pusat. Sebagai gantinya, pengguna terhubung satu sama lain melalui koneksi *peer to peer*.

Dengan aplikasi standar, mereka dikendalikan oleh satu entitas, berjalan di server terpusat yang rentan terhadap peretasan atau downtime karena server offline. Aplikasi terdesentralisasi tidak memiliki server atau entitas tunggal yang mengendalikannya. Ini berjalan di jaringan komputer dan perubahan diputuskan oleh pengguna. Tidak ada titik sentral bahwa server bisa crash atau diretas. Jika satu komputer di jaringan offline, aplikasi tidak terpengaruh karena ada ribuan komputer lain yang menjalankan aplikasi secara bersamaan. Bahkan jika satu komputer di jaringan diretas, itu tidak dapat membuat perubahan yang tidak sah pada aplikasi karena sebagian besar jaringan harus menyetujui perubahan tersebut.

8.5 KONTRAK PINTAR

Kontrak pintar adalah kontrak yang ditulis dalam kode komputer dan beroperasi pada *blockchain* atau buku besar yang didistribusikan. Mereka secara otomatis memverifikasi, melaksanakan, dan menegakkan kontrak berdasarkan ketentuan yang tertulis dalam kode. Kontrak pintar dapat sebagian atau seluruhnya dijalankan sendiri dan ditegakkan sendiri. Kontrak pintar dapat digunakan untuk menukar apa pun yang bernilai, seperti yang disebutkan dalam bab tentang potensi penggunaan *blockchain*, banyak industri yang menggunakan teknologi *blockchain* akan menggunakan kontrak pintar.

Ketika kontrak pintar dijalankan di *blockchain*, kontrak itu beroperasi secara otomatis. Jika kondisi kontrak terpenuhi, pembayaran atau nilai dipertukarkan berdasarkan persyaratan kontrak. Demikian juga, jika kondisi dalam kontrak tidak terpenuhi, pembayaran dapat ditahan

jika ditulis ke dalam kontrak pintar. Kontrak pintar berjalan saat diprogram pada jaringan komputer terdesentralisasi di *blockchain* yang menghilangkan risiko seputar perubahan yang tidak sah, penipuan, kegagalan server, atau ketidakpatuhan terhadap ketentuan kontrak. Kontrak dijalankan secara otomatis, pertukaran nilai dan pembayaran antara orang-orang tanpa perlu pengacara atau pengadilan untuk menegakkannya.

Entri di *blockchain* diberi stempel waktu dan tidak dapat diubah. Ini menciptakan platform yang ideal untuk kontrak karena setiap perubahan pada kontrak diberi stempel waktu, sementara versi sebelumnya dipertahankan di *blockchain*. Kontrak dapat disimpan (dan versi baru dibuat) sambil mempertahankan salinan sebelumnya (serta stempel waktu yang akurat pada semua pengeditan dan revisi). Ini tidak hanya memberikan garis besar yang lebih akurat tentang proses yang terjadi tetapi juga membuat semua pihak yang terlibat lebih jujur tentang transaksi yang terjadi karena buku besar tidak dapat diubah. Jaringan *blockchain* menghilangkan kebutuhan akan perantara pihak ketiga untuk mengelola kontrak.

Penggunaan kontrak pintar

Risiko dengan jaringan Bitcoin adalah jika Anda membeli barang menggunakan Bitcoin, setelah melakukan pembayaran tidak ada jaminan Anda akan menerima barang yang dibeli. Orang lain yang terlibat dapat memutuskan untuk tidak mengirimkan barang atau mengklaim bahwa mereka tidak menerima pembayaran. Karena tidak ada perantara pihak ketiga untuk transaksi di jaringan Bitcoin, tindakan tradisional seperti memperdebatkan transaksi, meminta pengembalian dana, atau menghubungi perantara tidak dimungkinkan.

Dompet Bitcoin juga anonim, jadi Anda mungkin tidak memiliki informasi tentang ke mana transaksi itu dikirim. Jika transaksi dikirim ke alamat yang salah, maka transaksi tersebut hilang dan uangnya hilang. Kontrak pintar memecahkan banyak risiko yang terkait dengan bertransaksi di jaringan *blockchain*. Kontrak pintar dapat digunakan untuk apa pun yang bernilai yang dapat ditukar, dan ada banyak perusahaan yang mengembangkan aplikasi terdesentralisasi berbasis *blockchain* yang memanfaatkan kontrak pintar. Ascribe adalah perusahaan rintisan di industri seni yang memungkinkan banyak seniman berbeda untuk mengklaim kepemilikan atas karya mereka dan menerbitkan cetakan edisi terbatas. Platform mengeluarkan karya seni bernomor dalam bentuk digitalnya dan menggunakan *blockchain* untuk melacak kembali semua kreasi dan transaksi asli dalam kreasi tersebut. Ini memiliki pasar tempat seniman dapat beriklan, dan orang dapat membeli dan menjual karya seni melalui situs web mereka.

UProov adalah perusahaan hukum dan media yang menyediakan prangko waktu nyata yang dapat diverifikasi pada setiap dan setiap video dan gambar yang diambil pada perangkat elektronik apa pun. Gambar dan video dengan stempel waktu yang tidak dapat diubah dapat lebih diandalkan sebagai bukti dalam kasus pengadilan. BitProof, perusahaan lain yang menggunakan *blockchain* untuk membuat cap waktu, memiliki aplikasi yang mudah diunduh ke telepon. Ini memungkinkan stempel waktu yang dapat diverifikasi ke setiap bagian dokumentasi yang Anda jalankan. Itu dapat ditelusuri kembali ke pembuatannya di *blockchain* yang tidak dapat diubah. Teknologi ini berpotensi menghilangkan kebutuhan akan notaris di masa depan. Warranteer adalah perusahaan lain yang sudah memiliki ikatan dengan GoPro dan LG. Mereka menggunakan kontrak pintar untuk memindahkan jaminan produk ke

blockchain yang mudah diakses, dapat ditransfer, dan dipertahankan. Semua jejak suntingan, perubahan, pembaruan, dan pergeseran dicatat ke dalam *blockchain* yang dapat diakses oleh pemberi jaminan dan penerima jaminan pada saat tertentu.

Peertracks, Mycelia, dan Ujo Music adalah perusahaan terpisah yang semuanya berfokus pada penggunaan teknologi *blockchain* dalam industri musik. Ketiga perusahaan tersebut menggunakan kontrak pintar dengan cara yang berbeda dengan tujuan utama menghilangkan perantara seperti label rekaman, sehingga memudahkan musisi untuk menjual langsung kepada penggemar dan mendapatkan bayaran untuk musik mereka. Keuangan mikro melibatkan pinjaman sejumlah kecil uang, terutama di negara-negara miskin di seluruh dunia. Jumlah ini kecil untuk bank; namun, mereka penting bagi peminjam, karena memungkinkan mereka untuk memulai bisnis, mendapatkan penghasilan, dan menghidupi keluarga mereka.

Keuangan mikro telah mengangkat jutaan orang di seluruh dunia keluar dari kemiskinan, dibantu oleh Mohamed Yunus, yang memenangkan Hadiah Nobel untuk karyanya dengan keuangan mikro. Sebelum modernisasi keuangan mikro oleh Mohamed Yunus, sebagian besar bank tidak akan membiayai pinjaman kecil karena biaya administrasi lebih besar daripada keuntungan dari pinjaman. Asuransi Mikro adalah bidang yang belum melihat perubahan dramatis seperti pinjaman mikro. Perusahaan start-up Stratumn bertujuan untuk mengubah asuransi mikro dengan bekerja sama dengan Lemonway dalam pembuatan sistem berbasis *blockchain* asuransi mikro yang disebut "LenderBot." LenderBot akan menggunakan kontrak pintar di atas *blockchain* untuk membuat dan mengelola kontrak asuransi mikro.

Saat membahas masa depan *blockchain*, istilah "*Blockchain 2.0*" biasanya digunakan untuk menggambarkan langkah selanjutnya dalam evolusi teknologi *blockchain*. Aplikasi terdesentralisasi bersama dengan kontrak pintar membawa kemampuan teknologi *blockchain* ke tingkat baru yang menarik. Masa depan *blockchain* akan berkisar pada kontrak pintar dan dApps. *blockchain* 2.0 berpotensi berdampak pada dunia secara eksponensial lebih besar daripada dampak yang dimiliki Bitcoin dan teknologi *blockchain* asli.

8.6 RINGKASAN:

- Ethereum adalah platform di atas *blockchain* dengan bahasa pemrograman yang memungkinkan pengembang untuk membuat dan menjalankan aplikasi terdesentralisasi dan kontrak pintar pada platform komputasi terdistribusi yang kuat dan *blockchain* yang mendasari platform Ethereum.
- Mata uang dan jaringan Bitcoin terutama digunakan untuk transaksi keuangan. Ethereum memiliki mata uang "Ethel;" tetapi dirancang untuk ditukar dengan daya komputasi, bukan untuk transaksi keuangan di luar platform Ethereum.
- Aplikasi terdesentralisasi (dApps) tidak memiliki saluran pembuangan tunggal atau entitas yang mengendalikannya; dApps berjalan di jaringan komputer.
- Kontrak pintar adalah kontrak yang ditulis ke dalam kode komputer dan beroperasi pada *blockchain* atau buku besar yang didistribusikan.

- Kontrak pintar secara otomatis memverifikasi, melaksanakan, dan menegakkan kontrak berdasarkan ketentuan yang tertulis dalam kode tanpa perlu perantara pihak ketiga seperti pengacara atau pengadilan untuk menegakkan kontrak.
- Apa pun yang bernilai dapat ditukar menggunakan kontrak pintar; mereka tidak hanya mengacu pada kontrak hukum. Kontrak pintar mengurangi risiko yang terkait dengan transaksi di jaringan *blockchain*, karena transaksi dan pembayaran ditangani secara otomatis oleh jaringan.
- Ada banyak perusahaan yang sudah mengembangkan aplikasi terdesentralisasi berbasis *blockchain* dan kontrak pintar di platform Ethereum.
- Platform Ethereum adalah langkah selanjutnya di masa depan teknologi *blockchain* yang mencakup kontrak pintar dan aplikasi terdesentralisasi—teknologi ini sering disebut sebagai "*blockchain 2.0*."

BAB 9

MASA DEPAN *BLOCKCHAIN*

"Pada saatnya, saya melihat blockchain publik - apakah itu Bitcoin atau yang lain terbuka di masa depan, yang merupakan cara mendaftarkan kepemilikan semua jenis aset dan ini adalah cara mentransfer kepemilikan aset tersebut dalam satu sistem yang dapat dibaca oleh semua orang yang tepat dan tidak ada orang yang salah.

Menjadi sangat sederhana bagi saya untuk menukar dolar saya dengan saham IBM Anda, atau pound Anda untuk rumah Anda. Aset apa pun yang kami beri nilai dan ingin memastikan siapa pemiliknya dapat didaftarkan menggunakan teknologi ini"
-James Smith, CEO of Elliptic

Seperti yang dibahas dalam buku ini, teknologi *blockchain* memiliki potensi untuk menjangkau setiap negara, industri, dan orang di planet ini dalam beberapa dekade mendatang. Banyak prediksi tentang masa depan teknologi *blockchain* adalah asumsi; namun, ini bukan prediksi seperti "di masa depan, akan ada mobil terbang." Ada banyak sistem berbasis *blockchain* yang sudah dikembangkan di banyak industri. Momentum yang diperoleh teknologi *blockchain* selama beberapa tahun terakhir dalam hal investasi dalam proyek perusahaan dan pemerintah membuat prediksi masa depan dengan teknologi *blockchain* yang dimasukkan ke dalam kehidupan kita sehari-hari menjadi sangat realistik.

Jika kita melihat sistem berbasis *blockchain* saat ini yang sedang dibuat, industri yang digunakan dan tren yang muncul, kita dapat memperluas tren tersebut ke masa depan untuk mendapatkan gambaran tentang arah masa depan sistem berbasis *blockchain*.

9.1 SUMBER TERBUKA TERDESENTRALISASI VS SUMBER TERTUTUP TERPUSAT

Kesenjangan saat ini dalam pengembangan *blockchain* adalah apakah *blockchain* harus didesentralisasi dengan kode sumber yang tersedia untuk umum (*open source*) atau terpusat dengan kode sumber yang dipegang secara pribadi oleh organisasi atau kelompok kolaborator (*sumber tertutup*). Komponen asli dari teknologi *blockchain* percaya bahwa *blockchain* harus *open source* dan terdesentralisasi. Perusahaan dan pemerintah melihat teknologi *blockchain* *open source* yang terdesentralisasi dan menganggapnya brilian, namun mereka hanya menginginkannya tanpa aspek desentralisasi dan *open source*.

Ini seperti hari-hari awal komputasi pribadi di mana sebagian besar programmer percaya bahwa perangkat lunak harus *open source* dan gratis untuk semua orang. Bill Gates menerima banyak kritik karena menentang pola pikir ini dengan mengubah perangkat lunak menjadi bisnis yang dilisensikan dan dijual. Meskipun perangkat lunak *open source* masih populer, sebagian besar perusahaan perangkat lunak saat ini tidak membagikan kode mereka secara terbuka. Ripple adalah salah satu proyek *blockchain* paling terkenal dan saat ini *cryptocurrency* terbesar ketiga berdasarkan kapitalisasi pasar. Ripple adalah sumber tertutup dan terpusat; itu didistribusikan di antara kelompok lembaga keuangan tertentu sebagai buku besar yang didistribusikan untuk menyelesaikan transaksi di antara mereka. Ripple menerima banyak kritik dari komunitas *open source* yang tidak ingin masa depan teknologi *blockchain* terdiri dari *blockchain* tertutup dan terpusat yang dimiliki oleh lembaga keuangan besar.

Ethereum adalah *cryptocurrency* terbesar kedua berdasarkan kapitalisasi pasar dan salah satu jaringan *blockchain* terbesar. Ethereum adalah open source dan terdesentralisasi; ini menyediakan platform bagi pengembang untuk membangun aplikasi terdesentralisasi dengan token di *blockchain* menggunakan platform Ethereum. Tampaknya tidak ada pemenang yang jelas bahwa sistem berbasis *blockchain* akan mengambil antara desentralisasi open source dan open source didistribusikan / *blockchain* terpusat. Ada pekerjaan pengembangan dan pendanaan yang signifikan untuk kedua metode karena masing-masing memiliki manfaat yang sesuai dengan kebutuhan, organisasi, dan komunitas yang berbeda. Teknologi *blockchain* kemungkinan akan terus bergerak di kedua arah jaringan desentralisasi open source bersama dengan jaringan terpusat sumber tertutup secara bersamaan. Pemerintah dan perusahaan besar akan memilih satu metode sementara pemrogram individu, proyek skala kecil, dan perusahaan rintisan akan memilih yang lain.

9.2 BUKU BESAR TERDISTRIBUSI

Konsorsium R3 lembaga keuangan besar adalah arah lain yang diambil perusahaan. Konsorsium ini awalnya mengembangkan *blockchain*; Namun, itu telah pindah ke buku besar yang didistribusikan. Sementara buku besar terdistribusi konsorsium R3 memiliki banyak manfaat dari *blockchain*, itu bukan *blockchain*. Buku besar terdistribusi saat ini sangat terkait dengan *blockchain*, dan diasumsikan bahwa buku besar terdistribusi berbasis *blockchain*. Namun, buku besar terdistribusi dapat beroperasi tanpa menggunakan *blockchain*. Sebagian besar pekerjaan pengembangan dan start-up berbasis *blockchain* namun buku besar terdistribusi yang tidak didasarkan pada *blockchain* bisa menjadi tren yang muncul di masa depan.

Lebih sedikit *cryptocurrency*

Pada awal setiap industri berkembang, ada banyak perusahaan. Namun, seiring berkembangnya industri dan pasar, jumlah ini berkurang hingga hanya tersisa beberapa perusahaan atau merek besar saja. Pada awal tahun 1900-an ketika mobil merupakan teknologi baru, ada ribuan produsen mobil di AS, sekarang hanya ada beberapa perusahaan besar yang memproduksi mobil.

Tingkat pengurangan produsen mobil ini umum di sebagian besar industri dan kemungkinan akan terbukti menjadi tren di antara *cryptocurrency* di masa depan. Saat ini, ada ribuan *cryptocurrency* dengan lebih banyak yang dibuat setiap hari. Di masa depan, kemungkinan hanya beberapa *cryptocurrency* utama yang akan tetap ada dan menerima penerimaan arus utama sebagai bentuk pembayaran. Tren ini sudah terjadi saat proyek *blockchain* baru diluncurkan menggunakan token pada *blockchain* yang ada seperti Ethereum alih-alih membuat *cryptocurrency* mereka sendiri.

Lebih banyak token *blockchain*

Meskipun kemungkinan akan ada pengurangan jumlah *cryptocurrency*, jumlah token pada platform *blockchain* akan meningkat. Token seperti *cryptocurrency* karena ditukar di *blockchain* untuk pembelian. Namun, mereka berjalan di atas *blockchain* yang ada, dengan token yang mewakili nilai yang dikeluarkan di atas mata uang *blockchain* lain. Ethereum adalah *blockchain* paling populer untuk konsep ini. *Blockchain* Ethereum menggunakan mata uang

asli yang disebut "Eter." Siapa pun dapat mengeluarkan token di atas *blockchain* Ethereum, token mewakili nilai dan digunakan sebagai alat untuk pertukaran tetapi menggunakan *blockchain* Ethereum dan mata uang Eter yang ada. Token memungkinkan pengembang dan organisasi untuk membuat aplikasi yang berjalan di *blockchain* tanpa harus membuat dan memelihara *Blockchain* atau *cryptocurrency* mereka sendiri.

9.3 BLOCKCHAIN 2.0 - APLIKASI TERDESENTRALISASI (DAPPS) DAN KONTRAK CERDAS

Blockchain 2.0 adalah istilah untuk menggambarkan fungsionalitas baru dari *blockchain* yang ada sekarang dibandingkan dengan kode sumber aslinya. Platform Ethereum memungkinkan untuk membuat dan menjalankan aplikasi terdesentralisasi dan kontrak pintar di *blockchain*. dApps, Kontrak Cerdas, dan platform Ethereum dibahas secara rinci sebelumnya dalam buku ini. dApps dan kontrak pintar yang dibangun di jaringan Ethereum atau *blockchain* lain yang ada yang menggunakan token alih-alih *cryptocurrency* adalah tren baru yang berkembang pesat yang tidak menunjukkan tanda-tanda melambat.

Lebih banyak regulasi dan penerimaan

Masih ada kritik dan kekhawatiran yang signifikan tentang teknologi *blockchain*. Bitcoin adalah contohnya; pemerintah mengklaim transaksi terlalu pribadi, sehingga mudah digunakan untuk kegiatan kriminal, pencucian uang, dan penghindaran pajak. Di sisi lain dari argumen itu, orang mengklaim bahwa database terdesentralisasi seperti Bitcoin, keterbukaan untuk dapat melihat dompet siapa pun, saldo saat ini, dan transaksi membuatnya terlalu transparan dan tidak cukup pribadi. Banyak kritik karena Bitcoin menjadi aplikasi teknologi *blockchain* yang paling terkenal, di seluruh dunia, arus utama dan layak. *Blockchain* masih dalam masa-masa awal. Ini sangat terkait dengan Bitcoin dan *cryptocurrency*, dan ada ratusan *cryptocurrency open source* yang dibuat setiap bulan.

Pemerintah sebelumnya menolak Bitcoin melihatnya hanya digunakan oleh penjahat dan pencucian uang. Pandangan itu mulai berubah karena teknologi *blockchain* lebih dipahami dan lembaga keuangan mengintegrasikan teknologi ke pasar keuangan. Pemerintah sekarang mendorong perusahaan Teknologi Finansial (FinTech) untuk melakukan bisnis di negara mereka, menerima *cryptocurrency* sebagai bentuk pembayaran baru dan memastikannya diatur dengan benar di dalam negeri. Jepang baru-baru ini melegalkan Bitcoin sebagai bentuk pembayaran yang sah, Australia baru-baru ini menghapus pajak atas *cryptocurrency* bersama dengan mendorong perusahaan yang terlibat dengan teknologi berbasis *blockchain* untuk melakukan bisnis di Australia. Pemerintah akan terus mencoba menarik perusahaan rintisan di bidang FinTech yang bekerja dengan bank, perusahaan, dan lembaga keuangan untuk menciptakan lapangan kerja, mempromosikan perdagangan, dan menumbuhkan ekonomi melalui teknologi berbasis *blockchain* baru.

9.4 BLOCKCHAIN DALAM KEHIDUPAN SEHARI-HARI

Apakah aplikasi desentralisasi open source dibangun di atas *blockchain* yang ada atau *blockchains* konsorsium swasta baru dibuat, akan ada peningkatan jumlah *blockchain* yang digunakan di setiap area kehidupan kita. Banyak database perusahaan dan pemerintah yang menggunakan spreadsheet usang atau buku besar manual akan digantikan oleh *blockchain*.

Bank-bank besar di seluruh dunia sudah mengembangkan *blockchain* mereka sendiri untuk menangani transaksi, entri buku besar, pertukaran antar mata uang dan banyak lagi.

Pemanfaatan teknologi *blockchain* dapat terus berkembang hingga menjadi umum seperti teknologi database saat ini yang digunakan oleh perusahaan dan pemerintah. Juga akan ada tren alternatif *blockchain* untuk opsi industri yang ada dalam kehidupan sehari-hari. Contoh yang menunjukkan tren alternatif *blockchain* yang ada di samping opsi yang ada adalah penyimpanan cloud. Storj dan Siacoin adalah perusahaan yang menciptakan penyimpanan berbasis cloud terdesentralisasi di *blockchain*. Meskipun kemungkinan besar mereka tidak akan menggantikan Google Drive atau Dropbox dalam waktu dekat, mereka telah memberikan opsi alternatif saat memutuskan tempat menyimpan file di cloud.

Hype tentang sistem berbasis *blockchain* yang mengganggu industri yang ada dan mengganti perusahaan mungkin tidak menjadi kenyataan dalam jangka pendek, tetapi ada tren yang jelas bahwa di banyak industri alternatif berbasis *blockchain* akan ada di samping opsi yang ada. Teknologi *blockchain* mungkin tidak menggantikan perantara yang ada seperti bank atau perusahaan seperti Google atau Uber seperti yang diprediksi beberapa orang, terutama dalam jangka pendek. Namun, bahkan jika perantara tidak diganti, Anda pada akhirnya akan menemukan teknologi *blockchain* melalui buku besar *blockchain* terdistribusi di tempat kerja, kontrak pintar, aplikasi terdesentralisasi atau dapat memilih alternatif berbasis *blockchain* untuk opsi saat ini di banyak bidang kehidupan sehari-hari.

9.5 RINGKASAN:

- **Sumber terbuka terdesentralisasi vs. sumber tertutup terpusat** - Belum ada pemenang yang jelas untuk arah pengembangan di masa depan. Kedua *blockchain* terdesentralisasi open source akan dikembangkan bersama dengan *blockchain* terpusat/konsorsium sumber tertutup untuk memenuhi kebutuhan yang berbeda.
- **Buku besar terdistribusi:** Buku besar terdistribusi yang tidak menggunakan *blockchain* tetapi memiliki banyak manfaat dari *blockchain* adalah tren yang dapat bersaing dengan Buku Besar berbasis *blockchain* di masa depan.
- **Lebih sedikit cryptocurrency dan lebih banyak token blockchain:** Tren yang saat ini terjadi adalah perusahaan yang menggunakan token pada platform Ethereum daripada *blockchain* dan cryptocurrency mereka sendiri. Tren ini tampaknya akan berlanjut karena fungsionalitas platform Ethereum memungkinkan pengembangan Aplikasi Terdesentralisasi dan Kontrak Cerdas.
- **Blockchain 2.0:** Teknologi *Blockchain* sekarang telah meningkatkan fungsionalitas secara signifikan seperti Aplikasi terdesentralisasi (dApps) dan Kontrak Cerdas yang bukan merupakan bagian dari kode *blockchain* asli. *Blockchain* 2.0 digunakan untuk merujuk ke masa depan teknologi *blockchain* termasuk peningkatan ini untuk memisahkannya dari kemampuan *blockchain* asli.
- **Lebih banyak regulasi dan penerimaan:** Pemerintah dan perusahaan telah bergerak untuk menerima cryptocurrency sebagai bentuk pembayaran yang sah bersama dengan investasi besar-besaran dalam infrastruktur dan teknologi *blockchain*.

- **Blockchain dalam kehidupan sehari-hari:** Bahkan jika teknologi berbasis *blockchain* tidak serevolusioner seperti yang diperkirakan, ia masih terlihat menjadi bagian dari setiap kehidupan melalui buku besar yang didistribusikan, opsi pembayaran, atau alternatif perangkat lunak untuk opsi yang ada.

BAB 10

PANDUAN TEKNIS UNTUK *BLOCKCHAIN*

10.1 PENGANTAR PANDUAN TEKNIS UNTUK *BLOCKCHAIN*

Panduan teknis tentang cara kerja *blockchain* ini ada di akhir buku karena mungkin tidak menarik bagi banyak pembaca. Detik ini akan mencakup aspek yang lebih maju seperti hash dan kriptografi yang terlibat dalam *blockchain*. Jika Anda tidak tertarik dengan kriptografi di balik *blockchain*, Anda dapat melewati bagian ini atau kembali lagi nanti. Ada beberapa sumber dan daftar istilah setelah bab ini yang memberikan rincian lebih lanjut tentang *blockchain*, Bitcoin, Ethereum, dan kontrak pintar yang mungkin juga menarik baginya.

10.2 PANDUAN TEKNIS TENTANG CARA KERJA *BLOCKCHAIN*

Panduan ini akan fokus pada bagaimana *blockchain* Bitcoin bekerja karena ini adalah *blockchain* asli dan semua *blockchain* lainnya didasarkan pada fondasi ini sehingga akan bekerja dengan cara yang sama. *Blockchain* Bitcoin menggunakan algoritma SHA-256. Algoritme SHA-256 menghasilkan hash 256-bit berukuran tetap yang unik. Hash seperti kode rahasia yang menggunakan metode enkripsi yang menyembunyikan data sedemikian rupa sehingga hampir tidak mungkin untuk didekripsi tanpa otorisasi. Hash yang dihasilkan selalu sama panjangnya. Tidak masalah apakah Anda memasukkan satu kata atau seluruh buku, Anda masih akan mendapatkan hash dengan panjang yang sama untuk jumlah data yang dimasukkan. Jika Anda mengubah salah satu huruf maka hash akan benar-benar berubah. Hash tampaknya acak tanpa koneksi ke data yang dimasukkan. Hampir tidak mungkin untuk mengetahui pesan asli dari hash kecuali Anda mengetahui pesan asli atau memiliki kunci pribadi.

Beberapa contoh hash yang dihasilkan dari berbagai kata dan frasa di bawah ini:

Hash dari kata "Blockchain" dengan huruf besar B:

b3f4e968455ea3ea20e60aae2cad91d8412a53bc4f3834e31521776eb4b44d4c

Hash dari kata "blockchain" dengan huruf kecil b:

154a5318f688615ba779541d8753e0b704715ba4b5cd7676d124008201803e73

Hash dari kata "rantai blok" dengan spasi di antara kata "blok" dan "rantai":

7ef554758e1810bldeclf43ef6c2d0ff105b6398756 1 fdb41352d9433d231457

Ini adalah keseluruhan lakon "Romeo dan Juliet" karya Shakespeare yang berisi lebih dari 20.000 kata:

e807d23c1f18e4ba4aa1542d35082e28f9f580407ca6031a34bcleff424fd37a

Dari contoh di atas, Anda dapat melihat bahwa tidak mungkin untuk memberi tahu data input dari hash yang dihasilkan. Jelas juga bahwa perubahan kecil, seperti mengubah huruf dari

huruf besar ke huruf kecil, atau menambahkan spasi akan secara signifikan mengubah hash yang dihasilkan.

10.3 HASHING TRANSAKSI MENJADI BLOK

Contoh sebelumnya adalah untuk menunjukkan bagaimana hash yang dihasilkan tidak memiliki pola yang dapat dideteksi terhadap panjang teks atau jenis data yang dimasukkan. Contoh di atas tidak mengandung transaksi, jadi untuk contoh berikutnya kita akan menggunakan transaksi dan mengubahnya menjadi hash. Setelah hash dibuat, kami akan menautkannya dalam blockchain.

Blok pertama di blockchain adalah blok 0, juga dikenal sebagai blok genesis.

Blok 0

Blok transaksi pertama akan berisi teks:

John menerima 100 bitcoin

Sally menerima 50 bitcoin

Sam menerima 10 bitcoin”

Hash 0 = 0000641727781545e50c0235823c9ae0785d419499cc5a5dcdf12332a53f0f7f

Blok 1

Blok transaksi kedua akan berisi transaksi di bawah ini:

John mengirim Sally 50 bitcoin

Sally mengirim Sam 10 bitcoin

Setiap transaksi akan ditandatangani dengan kunci pribadi oleh pemilik alamat Bitcoin pengirim. Jaringan tidak akan dapat melihat kunci pribadi tetapi mereka dapat memverifikasi kunci pribadi yang benar yang diotorisasi untuk mengirim bitcoin telah digunakan.

Blok juga akan berisi hash dari blok sebelumnya:

0000641727781545e50c0235823c9ae0785d419499cc5a5dcdf12332a53f0f7f

Nomor yang dikenal sebagai "nonce" (Nomor yang digunakan Sekali) juga akan disertakan. Nonce adalah jawaban atas teka-teki yang harus dipecahkan oleh penambang untuk menambahkan blok yang valid ke blockchain dan mendapatkan hadiah.

Hash 1 =

0000ed29ee4097b79e194adb355b18c500a900fib3a1670dec4673eac2abdd07 Blok 2

Blok transaksi ketiga akan berisi transaksi yang ditandatangani di bawah ini, bersama dengan hash dari blok sebelumnya dan nonce:

Sally mengirim Sam 20 bitcoin

John mengirim Sally 20 bitcoin

Hash 2 =

0000d5cada28a39cb0511cc871d550fe0c4ba704a93ad33db378936c6ab40caf

Blok 3:

Blok keempat transaksi akan berisi transaksi yang ditandatangani di bawah ini, bersama dengan hash dari blok sebelumnya dan nonce:

Sam mengirim John 10 bitcoin

Sally mengirim John 20 bitcoin

Hash 3=

00001bbd6491304360d142bd5f32610214937c263b0bc6c44b3ac04574b62d4c

10.4 MEMBUAT BLOCKCHAIN

Dengan menggunakan contoh-contoh di atas, kami memiliki 4 buah data yang telah diubah menjadi hash. Sekarang kita dapat menambahkan hash tersebut ke dalam blok dan membuat blockchain yang menghubungkannya.

Blok pertama di blockchain akan memiliki hash:

0000641727781545e50c0235823c9ae0785d119499cc5a5dcdf12332a53f0f7f

Ini adalah "blok 0" atau "blok genesis", tidak ada blok sebelumnya di blockchain yang perlu dirujuk oleh blok ini. Blok kedua di blockchain akan menjadi "Blok 1" dan akan mereferensikan hash dari blok genesis. Setiap blok yang ditambahkan ke blockchain akan mereferensikan hash dari blok sebelumnya di header, menghubungkannya bersama seperti rantai. Dengan menggunakan contoh transaksi di atas, kita dapat membuat blockchain yang terlihat seperti di bawah ini:

Blok 0 — Blok Genesis:

Hash dari blok sebelumnya: 0 — tidak ada blok sebelumnya

Hash dari blok 0:

0000641727781545e50c0235823c9ae0785d419499cc5a5dcdf12332a53f0f7f

Blok 1:

Hash dari blok sebelumnya (Blok 0):

0000641727781545e50c0235823c9ae0785d419499cc5a5c1cdf12332a53f0f7f

Hash dari blok 1:

0000ed29ee4097b79e194adb355b18c500a900flb3a1670dec4673eac2abdd07

Blok 2:

Hash dari blok sebelumnya (Blok 1):

0000ed29ee4097b79e194adb355b18c500a900f1b3a1670dec4673eac2abdd07

Hash dari blok 2:

0000d5cada28a39cb0511cc871d550fe0c4ba704a93ad33db378936c6ab40caf

Blok 3:

Hash dari blok sebelumnya (Blok 2):

0000d5cada282.39cb0511cc871d550fe0c4ba704a93ad33db378936c6ab40caf

Hash dari blok 3:

00001bbd6491304360d142bd5f32610214937c263b0bc6c44b3ac04574b62d4c

Itulah contoh dasar pembuatan *blockchain*. Setiap kelompok transaksi diubah menjadi hash, digabungkan dengan hash dari blok sebelumnya dan nomor yang dipecahkan oleh penambang. Hash disertakan dalam header blok berikutnya yang menghubungkan setiap blok baru ke blok sebelumnya. Kita dapat mengikuti transaksi dari blok saat ini, sampai ke blok pertama untuk memahami apa yang telah terjadi di *blockchain*.

10.5 MENGUBAH BLOCKCHAIN

Seperti yang kita lihat pada contoh pertama menghasilkan hash, setiap perubahan kecil pada teks akan menghasilkan hash yang sama sekali berbeda. Beginilah cara *blockchain* membuatnya hampir tidak mungkin untuk melakukan penipuan dengan mengubah transaksi di blok sebelumnya.

Di blok 1, berisi transaksi di bawah ini:

John mengirim Sally 50 bitcoin

Sally mengirim Sam 10 bitcoin

Jika Sam ingin memanipulasi *blockchain* dan mengubah transaksi itu, maka Sally mengiriminya 20 bitcoin, bukan 10. Itu hanya akan menjadi perubahan kecil dengan mengubah 1 angka dalam transaksi itu. Perubahan semacam ini dapat dengan mudah terjadi dalam database keuangan saat ini, di mana satu nomor secara tidak sengaja atau sengaja dimasukkan secara tidak benar dan tidak diperhatikan. Dengan *blockchain*, mengubah satu nomor ini menciptakan hash yang sama sekali baru untuk blok transaksi itu.

Hash asli dari blok adalah:

0000ed29ee4097b79e194adb355b18c500a90Offb3a1670dec4673eac2abdd07

Hash baru dari blok tersebut adalah:

0000f3e9eda5e3f8782c5051068935abcd710ffd5fecb7fe7eaa6a57f8aa 1 208

Karena setiap blok di *blockchain* terhubung ke blok sebelumnya, hash header di blok 2 perlu diubah sehingga menyertakan hash baru dari blok 1 dengan transaksi yang diubah. Ini akan mengubah hash dari blok 2, yang berarti hash header dari blok 3 perlu diubah untuk mereferensikan hash baru dari blok 2. Ini akan berlanjut sampai ke blok terbaru di *blockchain* sampai semua hash dari blok telah diubah.

Konfirmasi di *blockchain*

Blok baru ditambahkan setiap 10 menit di *blockchain* Bitcoin. Banyak *blockchain* lain menambahkan blok lebih cepat dari ini. Untuk mengubah transaksi yang termasuk dalam blok, setiap blok harus ditambang ulang dengan hash baru lebih cepat daripada jaringan lainnya yang menambahkan blok. Ini mungkin untuk beberapa blok terbaru, namun secara umum diterima bahwa setelah 6 blok ditambahkan di atas blok transaksi, menjadi tidak mungkin secara komputasi untuk mengubah transaksi di blok itu. Blok baru yang ditambahkan di atas blok sebelumnya, dianggap sebagai konfirmasi bahwa blok transaksi sebelumnya valid dan tidak akan berubah. 6 blok di atas akan menjadi 6 konfirmasi dan keyakinan yang cukup bahwa transaksi sebelum 6 blok tersebut tidak akan diubah atau dibalik.

Target kesulitan jaringan *Blockchain*

Hash yang diberikan dalam contoh transaksi memiliki beberapa nol di depannya. Sebuah blok hanya dapat ditambahkan ke Bit *blockchain* koin jika hash lebih rendah dari hash target jaringan.

Contoh di bawah ini mungkin sedikit teknis, tetapi anggap saja seperti melempar dadu secara acak. Sebuah dadu memiliki angka 1 sampai 6 di atasnya, jika Anda memilih angka 6 sebagai target, maka jika ada yang melempar dadu dan mendapatkan di bawah angka 6 maka mereka dapat menambahkan blok ke *blockchain*. Semakin rendah angka target, semakin sulit untuk menggulung angka yang lebih rendah secara acak karena ada pilihan yang kurang

diterima. Jika nomor target adalah 2, maka hanya seseorang yang melempar nomor 1 yang dapat menambahkan blok ke *blockchain*. Ini akan memakan waktu lebih lama untuk melempar angka ini secara acak, jadi dengan bertambahnya jumlah orang yang melempar dadu, angkanya akan berubah dibuat untuk menjaga tingkat penambahan blok ke *blockchain* tetap konsisten.

Dalam contoh *blockchain* yang dibuat sebelumnya, hash dari blok 3 memiliki empat nol di depannya seperti yang ditunjukkan di bawah ini:

00001bbd6491304360d142bd5f32610214937c263bObc6c44b3ac04574b62d4c

Jika target jaringan adalah lima nol dan angka 5, mis. 000005, maka hash hanya valid jika lebih rendah dari 000005, jika tidak maka tidak akan diterima sebagai blok yang valid di *blockchain*.

Contoh hash Target:

000005d6b56a86dd37a43d070fe7eb7e59cf6026f7f1f5f14286flla3abl5lc9

Contoh hash yang dapat diterima:

Lima nol dan angka 4:

000004e13ccc4e31d500b52bc226dc4abb1627c383beaef6f4da90a61b7994f0

Tujuh nol dan satu angka:

000000022b64fdf3Odd4f28a50b542345b9750ee24a3467423acdb66dea27e4ff55

Delapan nol dan satu angka:

000000004a4a2e623f745df50e97e62c9e854-d07b0eef79a07ddad848c780133

Contoh hash yang ditolak:

Tiga nol dan satu angka:

0005f765f3c32e5e911ca 1 8e136746daa0beffP8a6d7aa48fal87debd959a69d507f

Empat nol dan satu angka:

00001c8d7349aeaOdd4acf2d16cb5f575035a9ca80b080175 l c832dfb97223043ab3f

Lima nol dan angka 6:

000006a38420742929149840eb l 318343bb9c332a1c95e9e20f9e20692fe45e2,Jika

Ini adalah versi yang lebih maju dari contoh melempar dadu, tetapi logika yang sama berlaku dengan kumpulan angka yang jauh lebih besar.

Blok Nonce

Nonce adalah angka yang termasuk dalam blok yang ketika di-hash akan menghasilkan hash yang lebih rendah dari target sehingga dapat diterima untuk dimasukkan ke dalam *blockchain*. Angka yang menciptakan hash valid yang lebih rendah dari target jaringan saat ini adalah teka-teki yang coba dipecahkan oleh penambang untuk menambahkan blok ke *blockchain* dan mendapatkan hadiah. Para penambang memilih transaksi luar biasa untuk dimasukkan dalam blok berikutnya untuk ditambahkan ke *blockchain* bersama dengan input dan output transaksi yang cocok. Juga termasuk hash dari blok sebelumnya, target kesulitan jaringan saat ini, akar pohon merkle, alamat *blockchain* untuk membayar hadiah dan cap waktu.

Saat menambahkan transaksi ke blok, penambang dapat memilih kombinasi transaksi luar biasa yang menunggu untuk ditambahkan ke *blockchain*. Biasanya mereka akan memilih transaksi dengan biaya tertinggi yang melekat padanya sebagai penambang menerima biaya bersama dengan hadiah blok jika mereka berhasil menambahkan blok ke rantai blok. Seperti

yang ditunjukkan pada contoh di atas, hash yang dihasilkan tampak acak dan tampaknya tidak memiliki koneksi ke data yang dimasukkan. Para penambang tidak tahu apa itu hash sampai mereka menghasilkan hash. Mereka hanya dapat menambahkan blok ke *blockchain* jika hash yang mereka hasilkan lebih rendah dari target hash jaringan. Untuk mencapai ini, mereka menambahkan nomor bersama dengan transaksi dan hash dari blok sebelumnya kemudian menghasilkan hash.

Jika hash yang dihasilkan lebih rendah dari target jaringan, mereka dapat menambahkannya ke *blockchain*. Jika lebih tinggi dari target jaringan, mereka mengubah nonce (angka) dan coba lagi. Tidak ada cara untuk menentukan apa hashnya, jadi proses menghasilkan angka hanyalah tebakan acak. Penambang yang menemukan nomor yang bila digabungkan dengan transaksi yang luar biasa membuat hash lebih rendah dari target jaringan dapat menambahkan blok ke *blockchain*. Penambang yang menambahkan blok yang valid ke *blockchain*, menerima biaya transaksi dan hadiah blok.

Setelah nomor tersebut ditemukan, semua komputer lain di jaringan dapat menambahkan nomor tersebut ke data transaksi dan mengonfirmasi bahwa itu benar. Nomor acak ini sulit ditemukan, tetapi mudah untuk memverifikasi kebenarannya setelah ditemukan. Blok yang valid ditambahkan ke *blockchain* dan kemudian semua komputer di jaringan memperbarui sistem mereka dengan versi terbaru dari *blockchain* termasuk blok baru. Penambang kemudian mengulangi proses ini untuk mencoba dan menambahkan blok berikutnya ke *blockchain* lebih cepat daripada penambang lain di jaringan.

10.6 MENINGKATKAN KESULITAN JARINGAN

Proses menemukan angka yang benar yang menghasilkan hash yang valid adalah permainan peluang acak, seperti contoh melempar dadu. Kecepatan pemrosesan memainkan faktor besar karena semakin cepat komputer dapat menebak angka, semakin cepat ia dapat menemukan jawaban yang benar. Jaringan Bitcoin dirancang untuk menambahkan blok ke *blockchain* setiap 10 menit. Karena lebih banyak komputer ditambahkan ke jaringan, ada lebih banyak kekuatan pemrosesan pada jaringan yang membuat lebih banyak tebakan pada kemungkinan nomor yang benar untuk setiap blok. Untuk memastikan waktu blok tetap sekitar 10 menit, target kesulitan disesuaikan setiap 2.016 blok menyesuaikan jumlah minimum dan maksimum untuk menambahkan blok yang valid. Untuk kembali ke contoh dadu, blok yang valid hanya dapat ditambahkan jika seseorang melempar dadu di bawah angka 3. Jika satu orang melempar dadu, mereka memiliki peluang 2 dalam 6 untuk melempar angka di bawah 3 yang akan di bawah target jaringan 3 dan memungkinkan mereka untuk menambahkan blok ke *blockchain*.

Misalnya, ini mungkin membutuhkan waktu sekitar 10 menit untuk memutar nomor 1 atau 2, sehingga target jaringan untuk menambahkan blok setiap 10 menit dipertahankan. Namun, jika orang lain ditambahkan ke jaringan, juga melempar dadu untuk mendapatkan di bawah angka 3, mungkin separuh waktu yang dibutuhkan untuk melempar angka 1 atau 2 secara acak, juga mengurangi separuh waktu yang dibutuhkan untuk menambahkan blok ke *blockchain*. Untuk menyesuaikan peningkatan orang di jaringan yang menambahkan blok lebih cepat dari setiap 10 menit, jaringan akan menyesuaikan target dari 3 menjadi 2, jadi blok

yang valid hanya diterima jika di bawah angka 2. Ada peluang 2 dari 6 untuk mendapatkan nomor yang valid, tetapi jumlah orang berlipat ganda di jaringan, sehingga kesulitannya diturunkan dan sekarang peluang 1 dari 6 untuk mendapatkan nomor yang valid. Ini akan menggandakan waktu yang diperlukan untuk mendapatkan target ini, yang akan menyesuaikan waktu blok yang ditambahkan ke jaringan kembali ke 10 menit. *blockchain* Bitcoin beroperasi dengan cara yang sama, karena lebih banyak komputer ditambahkan ke jaringan, kesulitannya disesuaikan dengan menurunkan target jaringan. Artinya ada hash yang kurang valid yang akan diterima dan rentang angka yang lebih luas yang perlu ditebak untuk membuat blok dengan hash yang valid.

10.7 PERMASALAHAN YANG DIHADAPI

Metode penghitungan angka yang benar yang membuat hash valid ini dikenal sebagai "bukti kerja", karena menunjukkan bahwa daya komputasi dan sumber daya dikontribusikan ke jaringan saat menambahkan blok. Penambang dihargai karena menyumbangkan daya komputer, listrik, dan sumber daya ke jaringan dengan pembayaran untuk setiap blok yang berhasil mereka tambahkan ke jaringan. Ini dikenal sebagai "hadiah blok", para penambang juga menerima biaya transaksi untuk setiap blok yang mereka tambahkan, itulah sebabnya mereka cenderung memilih transaksi dengan biaya lebih tinggi. Metode proof-of-work membutuhkan sejumlah besar daya komputasi dan listrik. Jaringan Bitcoin lebih dari 10.000 kali lebih kuat daripada gabungan 500 superkomputer top dunia, namun sebagian besar kekuatan komputasi itu diarahkan untuk tujuan menghasilkan angka acak.

Masalah utama dengan metode ini adalah pemborosan sumber daya yang besar untuk melakukan fungsi yang tampaknya tidak ada gunanya dan tidak diperlukan untuk menjalankan jaringan *blockchain*. Pikirkan sejenak, ada jaringan komputer yang lebih kuat daripada gabungan superkomputer paling kuat di dunia. Alih-alih mengerjakan masalah yang berpotensi mengubah dunia, ini digunakan untuk menghasilkan angka secara acak. Tampaknya agak konyol itulah sebabnya banyak orang mengkritik pemborosan "bukti kerja" yang digunakan oleh *blockchain* Bitcoin.

Ada metode lain seperti "*proof-of-stake*", "*proof-of-capacity*", "*proof-of-activity*" dan "*proof-of-burn*" yang dapat digunakan sebagai gantinya. Metode ini tidak akan dibahas secara lebih rinci, tetapi penting untuk diketahui bahwa ada alternatif untuk *proof-of-work* yang digunakan oleh *blockchain* lain. Platform Ethereum menggunakan jaringan untuk menjalankan aplikasi terdesentralisasi, menempatkan daya komputasi untuk penggunaan yang lebih baik. Ethereum juga beralih dari *proof-of-work* dan menuju *proof-of-stake* di *blockchain* Ethereum.

Keamanan jaringan *blockchain*

Salah satu fitur keamanan penting dari *blockchain* terdesentralisasi adalah bahwa setiap orang memiliki akses dan semua salinan diperbarui di seluruh jaringan. Ini memainkan peran besar dalam memastikan bahwa tidak ada database pusat di mana *blockchain* dapat dimanipulasi oleh seseorang yang ingin melakukan penipuan. Siapa pun dapat menambahkan blok ke *blockchain* tetapi mayoritas pengguna di jaringan harus menerimanya sebagai valid. Setelah blok baru diterima sebagai valid, itu ditambahkan ke *blockchain*, semua salinan *blockchain* diperbarui di seluruh jaringan dan blok berikutnya akan ditambahkan di atas itu.

Jika seseorang mencoba memanipulasi transaksi, itu tidak akan cocok dengan salinan *blockchain* lainnya dan karenanya tidak akan diterima oleh jaringan.

51% serangan dan garpu di *blockchain*

Serangan 51% telah disebutkan sebelumnya dalam buku ini, ini adalah kasus teoretis di mana pengguna berhasil mengontrol lebih dari 50% jaringan. Dengan mengendalikan lebih dari 50%, mereka kemudian dapat memutuskan transaksi dan blok mana yang valid dan jaringan lainnya akan diperbarui dengan versi *blockchain* mereka. Garpu adalah situasi di mana sejumlah besar pengguna di jaringan tidak setuju dengan perubahan dalam jaringan, ini bisa berupa transaksi dan blok yang ditambahkan atau fungsionalitas jaringan. Ketidaksepakatan ini menciptakan garpu di *blockchain* di mana beberapa pengguna berpisah dan mengalokasikan daya komputasi mereka untuk menjalankan *blockchain* baru yang terpisah dari *blockchain* asli. Garpu utama dalam *blockchain* telah terjadi dengan Ethereum dan *cryptocurrency* lainnya. "Ether" dan "Ether classic" adalah dua *blockchain* terpisah yang dibuat dari *blockchain* Ethereum asli, namun karena ketidaksepakatan, bagian dari jaringan Ethereum terpecah dan mengalokasikan sumber daya ke versi *blockchain* yang berbeda.

10.8 RINGKASAN

Bab ini seharusnya memberikan pemahaman yang lebih teknis tentang cara kerja *blockchain*. Ada beberapa informasi lanjutan tambahan tentang jaringan *blockchain* yang tersedia di bagian sumber daya.

DAFTAR PUSTAKA

- Aini, Q., Rahardja, U., Moeins, A., & Apriani, D. M. (2018). Penerapan Gamifikasi pada Sistem Informasi Penilaian Ujian Mahasiswa Untuk Meningkatkan Kinerja Dosen. *Jurnal Informatika Upgris*, 4(1).
- Al Fatta, H., & Marco, R. (2015). Analisis pengembangan dan perancangan sistem informasi akademik smart berbasis cloud computing pada sekolah menengah umum negeri (smun) di daerah istimewa yogyakarta. *Telematika*, 8(2).
- Anggoro, B. S., & Sulistyo, W. (2019, November). Implementasi Intrusion Prevention System Suricata dengan Anomaly-Based untuk Keamanan Jaringan PT. Grahamedia Informasi. In *SEMINAR NASIONAL APTIKOM (SEMNASTIK) 2019* (pp. 280-288).
- Aripin, A. A. (2018). Potensi pemanfaatan teknologi Blockchain terhadap ketepatan waktu, efisiensi dan keamanan proses operasi pada subsektor perbankan.
- D. Ariyus, Pengantar Ilmu Kriptografi: Teori, Analisis, dan Implementasi. Yogyakarta: Andi, 2008.
- E. Barker, Recommendation for Key Management, Part 1: General, Revision 4. Gaithersburg: Gaithersburg National Institute of Standards and Technology, 2016.
- Febriyanto, E., Rahardja, U., Faturahman, A., & Lutfiani, N. (2019). Sistem Verifikasi Sertifikat Menggunakan Qrcode pada Central Event Information. *Techno. Com*, 18(1), 50-63.
- Forte, P., Romano, D., & Schmid, G. (2015). Beyond Bitcoin-Part I: A critical look at blockchain-based systems. *IACR Cryptology ePrint Archive*, 2015, 1164.
- Grech, A., & Camilleri, A. F. (2017). Blockchain in education.
- Handayani, I., Aini, Q., & Sari, N. (2018). Pemanfaatan Sistem iJC Berbasis OJS Sebagai Media E-Journal Pada STISIP YUPPEN TEK. *Technomedia Journal*, 2(2), 94-106.
- Handayani, I., Febriyanto, E., & Bachri, E. W. (2018). Aplikasi Stat Counter Sebagai Alat Monitoring Aktivitas Website PESSTA+ Pada Perguruan Tinggi. *SISFOTENIKA*, 8(2), 188-197.
- Huckle, S., Bhattacharya, R., White, M., & Beloff, N. (2016). Internet of things, blockchain and shared economy applications. *Procedia computer science*, 98, 461-466.
- Iswari, D. A., Arkeman, Y., & Muslich, M. (2019). ANALISIS DAN DESAIN RANTAI PASOK KAKAO BERBASIS BLOCKCHAIN. *JURNAL AGRI-TEK: Jurnal Penelitian Ilmu-Ilmu Eksakta*, 20(2), 41-47.

- J. Gao et al., "GridMonitoring: Secured Sovereign Blockchain Based Monitoring on Smart Grid," IEEE Access, vol. 4, pp. 2292–2303, 2018.
- K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.
- Kristanto, V. H. (2018). Metodologi Penelitian Pedoman Penulisan Karya Tulis Ilmiah (KTI). Yogyakarta: CV Budi Utama.
- Kurniawan, M. L., & Erna Dewi, F. (2018). PERAN KEPOLISIAN DALAM PENYIDIKAN TINDAK PIDANA PENYALAHGUNAAN IJAZAH PALSU. JURNAL POENALE, 6(3).
- Liu, L., Chen, Y., & Liu, D. (2019). U.S. Patent No. 10,313,870. Washington, DC: U.S. Patent and Trademark Office.
- Malson, H. (2019). Akibat Hukum Penggunaan Sertifikat Elektronik pada Admissibility dan Kekuatan Mengikat Alat Bukti Elektronik dalam Sistem Pembuktian Perdata (Studi Perbandingan: Indonesia dan Singapura) (Doctoral dissertation, Universitas Gadjah Mada).
- Nafizah, N. S., & Winoto, Y. (2018). Pekerjaan Pustakawan di Bagian Layanan Teknis Pada Era Teknologi Digital. Jurnal Pustaka Budaya, 5(1), 19-28.
- Njatrijani, R. (2019). PERKEMBANGAN REGULASI DAN PENGAWASAN FINANCIAL TECHNOLOGY DI INDONESIA. Diponegoro Private Law Review, 4(1).
- Nugraha, A. C., 2020, Penerapan Teknologi Blockchain dalam Lingkungan Pendidikan: Studi Kasus Jurusan Teknik Komputer dan Informatika POLBAN. Produktif: Jurnal Ilmiah Pendidikan Teknologi Informasi.
- Nugrahanto, S., & Zuchdi, D. (2019, April). Indonesia PISA Result and Impact on The Reading Learning Program in Indonesia. In International Conference on Interdisciplinary Language, Literature and Education (ICILLE 2018). Atlantis Press.
- Ouaddah, A., Elkalam, A. A., & Ouahman, A. A. (2017). Towards a novel privacy-preserving access control model based on blockchain technology in IoT. In Europe and MENA Cooperation Advances in Information and Communication Technologies (pp. 523-533). Springer, Cham.
- Peniarsih, P., 2020, Sistem Keamanan Data Dengan Metode Cryptography, Jurnal Mitra Manajemen, 4(2).
- R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Commun. ACM, vol. 21, pp. 120–126, 1978.

- Rahardja, U., Handayani, I., & Wijaya, R. (2018). Penerapan Viewboard Technomedia Journal menggunakan sistem iLearning Journal Center pada Perguruan Tinggi. *Technomedia Journal*, 2(2), 78-89
- Rahardja, U., Harahap, E. P., & Christianto, D. D., 2020, Pengaruh Teknologi Blockchain Terhadap Tingkat Keaslian Ijazah, *Technomedia Journal*.
- S. V. Nandury and B. A. Begum, "Big Data for Smart Grid Operation in Smart Cities," in IEEE International Conference on Wireless Communications Signal Processing and Networking (WiSPNET), 2017.
- Sutrisno, B. (2018). Blockchain dan Cryptocurrency: Peran Teknologi Menuju Inklusi Keuangan?.
- The Research Perspective Ltd, "Smart Meter Electricity Trial Data Manifest," 2012.
- Tho'in, M. (2017). Pembiayaan Pendidikan Melalui Sektor Zakat. *Al-Amwal: Jurnal Ekonomi dan Perbankan Syari'ah*, 9(2).
- W. Stallings, *Cryptography and Network Security: Principles and Practice*. Boston: Prentice Hal, Inc, 2011.
- W. Stallings, *Data and Computer Communications*, 10th ed. New Jersey: Prentice Hal, Inc, 2015.
- Widaningsih, I. (2019). Strategi dan inovasi pembelajaran bahasa indonesia di era revolusi industri 4.0. *Uwais Inspirasi Indonesia*.
- Winarno, A. (2019, April). DESAIN e-TRANSKRIP DENGAN TEKNOLOGI BLOCKCHAIN. In *Prosiding Seminar Nasional Pakar* (pp. 1-37).
- Yatim, A., Nurkholis, F. M., & Setiawan, A. (2018). Innovation in University in the era of Industry 4.0.