PENERAPAN *BLOCKCHAIN* DENGAN INTEGRASI *SMART CONTRACT* PADA SISTEM *CROWDFUNDING*

TUGAS AKHIR

Disusun dalam rangkai memenuhi salah satu persyaratan

Untuk menyelesaikan program Strata-1 Departemen Informatika

Fakultas Teknik Universitas Hasanuddin

Makassar

Disusun Oleh :

FIQAR ARPIALIM

D42115304

DEPARTEMEN TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS HASANUDDIN

MAKASSAR

2020

LEMBAR PENGESAHAN

"PENERAPAN *BLOCKCHAIN* DENGAN INTEGRASI *SMART CONTRACT* PADA SISTEM *CROWDFUNDING*"

Disusun Oleh :

FIQAR APRIALIM
D421 15 304

Skripsi ini telah dipertahankan pada Ujian Akhir Sarjana tanggal 2 Desember 2020. Diterima dan disahkan sebagai salah satu syarat memperoleh gelar Sarjana Teknik (S.T) pada Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin.

Gowa, 2 Desember 2020

Disetujui Oleh :

Pembimbing I,	Pembimbing II,
Adnan, S.T., M.T., Ph.D.	Dr. Eng. Ady Wahyudi Paundu, S.T., M.T.
NIP. 19740426 200501 1 002	NIP. 19750313 200912 1 003

Diterima dan disahkan oleh:
Ketua Departemen Teknik Informatika

Dr. Amil Ahmad Ilham, S.T.,M.IT
NIP. 19731010 199802 1 001

PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini :

Nama : FIQAR APRIALIM

NIM : D421 15 304

Departemen : S1 Teknik Informatika

Menyatakan dengan sebenar-benarnya bahwa skripsi yang berjudul :

PENERAPAN *BLOCKCHAIN* DENGAN INTEGRASI *SMART CONTRACT* PADA SISTEM *CROWDFUNDING*

Adalah karya ilmiah saya sendiri dan sepanjang pengetahuan saya di dalam naskah skripsi ini tidak terdapat karya ilmiah yang pernah diajukan/ditulis/diterbitkan sebelumnya. Kecuali yang secara tertulis dikutip dalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila dikemudian hari ternyata di dalam naskah skripsi ini terdapat unsur-unsur jiplakan, saya bersedia menerima sanksi atas perbuatan tersebut dan diproses sesuai dengan peraturan perundang-undangan yang berlaku (UU No. 20 Tahun 2000, pasal 25 ayat 2 dan pasal 70)

Gowa, 2 Desember 2020

Yang Membuat Pernyataan

FIQAR APRIALIM

ABSTRAK

Popularitas *crowdfunding* yang semakin berkembang menyebabkan peningkatan persaingan antara berbagai *platform crowdfunding* dalam menyediakan sistem yang baik dan efisien. Sebuah proyek galang dana umumnya melibatkan transaksi keuangan yang jumlahnya tidak sedikit. Dengan demikian, keamanan data dan transparansi dari transaksi keuangan yang terjadi merupakan hal utama yang perlu ditingkatkan. Selain itu, perhitungan biaya pemrosesan proyek galang dana yang umumnya diterapkan pada sistem *crowdfunding* masih terbilang kurang optimal karena ditetapkan dengan tarif berbasis persentase berdasarkan jumlah dana yang diterima oleh setiap proyek. Teknologi *blockchain* kemudian hadir untuk memberikan keamanan dan transparansi pada sistem transaksi keuangan. Walaupun demikian, penerapan teknologi *blockchain* pada sistem *crowdfunding* belum cukup karena proses yang terjadi dalam sistem tidak hanya sekedar proses transaksi keuangan dasar, tetapi terdapat protokol penggalangan dana yang perlu diterapkan dalam proses transaksi tersebut. *Smart contract*, yaitu kontrak berbentuk perangkat lunak yang terotomatisasi, kemudian mulai diintegrasikan ke teknologi *blockchain* untuk dapat memenuhi kebutuhan suatu sistem dalam melakukan berbagai macam bentuk pemrosesan dengan protokol *blockchain*. Integrasi *smart contract* memungkinkan implementasi *blockchain* pada sistem *crowdfunding* dapat dilakukan. Penerapan kedua teknologi ini dilakukan dengan menggunakan *platform blockchain* Ethereum. Sistem *crowdfunding* yang menggunakan arsitektur *blockchain* dapat memberikan transparansi pada setiap kegiatan pemberian dana dan keamanan data transaksi karena aksesibilitas data yang bersifat publik dan sifat terdesentralisasi *blockchain*. Sistem *crowdfunding* yang dibangun dalam studi ini mampu mengoptimalkan biaya pemrosesan proyek galang dana karena setiap pemrosesan dilakukan secara otomatis menggunakan *smart contract* dengan biaya yang ditetapkan berdasarkan tarif sama rata. Hasil perbandingan menunjukkan pengoptimalan biaya pemrosesan pembentukan proyek galang dana tercapai untuk total dana yang besarnya sekitar Rp2.000.000,00 atau lebih dan pengoptimalan biaya pemrosesan pemberian dana tercapai untuk jumlah pemberian dana yang besarnya sekitar Rp500.000,00 atau lebih.

Kata kunci: *crowdfunding*, *blockchain*, *smart contract*, Ethereum, transaksi.

KATA PENGANTAR

Puji dan syukur penulis panjatkan atas kehadirat Allah SWT karena berkat rahmat dan karunia-Nya sehingga tugas akhir yang berjudul "*Penerapan Blockchain Dengan Integrasi Smart Contract Pada Sistem Crowdfunding*" ini dapat diselesaikan sebagai salah satu syarat dalam menyelesaikan jenjang Strata-1 (S-1) pada Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin.

Penulis menyadari bahwa dalam penyusunan dan penulisan laporan tugas akhir ini tidak lepas dari bantuan, bimbingan serta dukungan dari berbagai pihak, dari masa perkuliahan sampai dengan masa penyusunan tugas akhir. Oleh karena itu, penulis dengan senang hati menyampaikan terima kasih kepada:

1. Orang tua penulis, Bapak Dr. dr. Arifin Seweng, MPH dan Ibu Dra. Nurbaeti, M.Kes. serta Saudara kandung penulis, Fadil Apriawan dan Nurfina Yuniar, yang selalu memberikan dukungan, doa, semangat dan kekuatan kepada penulis dalam menjalani masa perkuliahan, terlebih pada saat pengerjaan tugas akhir;
2. Bapak Adnan, S.T., M.T., Ph.D. selaku dosen pembimbing I dan Bapak Dr.Eng. Ady Wahyudi Paundu, S.T., M.T. selaku dosen pembimbing II yang selalu menyediakan waktu, tenaga, pikiran dan perhatian yang besar untuk mengarahkan penulis dalam penyusunan tugas akhir;
3. Bapak Dr. Amil Ahmad Ilham, S.T., M.IT. dan Bapak Iqra Aswad, S.T., M.T. selaku dosen penguji yang telah memberikan saran sehingga laporan tugas akhir ini menjadi lebih baik;

4. Bapak Dr. Amil Ahmad Ilham, S.T., M.IT. selaku Ketua Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin atas bimbingan yang diberikan selama masa perkuliahan penulis;
5. Segenap Staf Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin yang telah membantu segala urusan administrasi yang diperlukan selama masa perkuliahan penulis;
6. Teman-teman dan kakak-kakak Laboratorium UBICON, yang telah memberikan dukungan dan semangat;
7. Teman-teman Laboratorium IOT, yang telah memberikan dukungan dan semangat;
8. Teman-teman HYPERV15OR atas dukungan dan semangat yang telah diberikan.
9. Seluruh pihak yang tidak sempat penulis sebutkan satu persatu, yang telah meluangkan waktu, tenaga dan pikiran selama penyusunan laporan tugas akhir ini.

Akhir kata, penulis berharap semoga Allah SWT berkenan membalas segala kebaikan dari semua pihak yang telah banyak membantu. Semoga tugas akhir ini dapat bermanfaat bagi para pembacanya.

Makassar, Juli 2020

Penulis

DAFTAR ISI

PENERAPAN *BLOCKCHAIN* DENGAN INTEGRASI *SMART CONTRACT*

PADA SISTEM *CROWDFUNDING* ..... **i**

LEMBAR PENGESAHAN ..... **ii**

PERNYATAAN KEASLIAN ..... **iii**

ABSTRAK ..... **iv**

KATA PENGANTAR ..... **v**

DAFTAR ISI ..... **vii**

DAFTAR TABEL ..... **x**

DAFTAR GAMBAR ..... **xi**

BAB I PENDAHULUAN **1**

1.1. Latar Belakang 1

1.2. Rumusan Masalah 4

1.3. Tujuan Penelitian 4

1.4. Manfaat Penelitian 5

1.5. Batasan Masalah 5

1.6. Sistematika Penulisan 5

BAB II TINJAUAN PUSTAKA **7**

2.1. *Crowdfunding* 7

2.2. *Blockchain* 9

2.3. *Smart Contract* 20

2.4. Ethereum 22

2.4.1. *Account* 24

2.4.2. Transaksi 25
2.4.3. *Block* 27
2.4.4. Eksekusi Transaksi 30
2.4.5. Arsitektur *Blockchain* 31
BAB III METODOLOGI PENELITIAN 33
3.1. Waktu dan Lokasi Penelitian 33
3.2. Instrumen Penelitian 33
3.3. Gambaran Umum Sistem 35
3.3.1. *Activity Diagram* Sistem 36
3.3.2. Desain *Smart Contract* 45
3.3.3. Detail Perancangan Sistem 47
3.4. Skenario Analisis dan Pengujian 49
3.4.1. Pengujian Fungsionalitas Sistem 49
3.4.2. Analisis Keamanan & Transparansi Sistem 50
3.4.3. Pengujian Besar Biaya Transaksi Sistem 50
BAB IV HASIL DAN PEMBAHASAN 53
4.1. *Cryptocurrency* 53
4.2. Pengujian Fungsionalitas Sistem 54
4.2.1. Pembentukan Proyek 54
4.2.2. Pemberian Dana pada Proyek 56
4.2.3. Pengambilan Dana Proyek 57
4.2.4. Pengembalian Dana Proyek 58
4.3. Analisis Keamanan dan Transparansi Sistem 59

4.3.1. Dasar Teoritis 59
4.3.2. Pengujian *Blockchain* Ethereum..... 64
4.3.2.1. Pengujian Mayoritas Node Jujur (Kondisi Pertama)..... 66
4.3.2.2. Pengujian *Double Spending* (Kondisi Kedua)..... 68
4.3.2.3. Pengujian Rantai *Block* Tidak Valid (Kondisi Ketiga)..... 71
4.3.3. Analisis Terhadap Serangan Digital Lainnya..... 74
4.4. Pengujian Besar Biaya Transaksi..... 77
4.4.1. Pemrosesan Pembentukan Proyek..... 77
4.4.2. Pemrosesan Pemberian Dana pada Proyek..... 80
4.4.3. Evaluasi Hasil Pengujian Besar Biaya Pemrosesan 84
BAB V PENUTUP..... 90
5.1. Kesimpulan..... 90
5.2. Saran..... 91
DAFTAR PUSTAKA..... 92
LAMPIRAN..... 94

DAFTAR TABEL

Tabel 2. 1 Jenis *Blockchain* 15

Tabel 2. 2 Bidang Aplikasi Blockchain 18

Tabel 2. 3 Komponen Transaksi (Kasireddy 2017) 26

Tabel 3. 1 *Input* dan *Output* Pembentukan Proyek 38

Tabel 3. 2 *Input* dan *Output* Pemberian Dana pada Proyek 41

Tabel 3. 3 *Input* dan *Output* Pengambilan Dana Proyek 42

Tabel 3. 4 *Input* dan *Output* Pengembalian Dana Proyek 44

Tabel 3. 5 *Variable* dan *Function* dari Contract Crowdfunding 45

Tabel 3. 6 *Variable* dan *Function* dari Contract Project 46

Tabel 4. 1 Hasil *Black Box Testing* Pembentukan Proyek 55

Tabel 4. 2 Hasil *Black Box Testing* Pemberian Dana pada Proyek 56

Tabel 4. 3 Hasil *Black Box Testing* Pengambilan Dana Proyek 58

Tabel 4. 4 Hasil *Black Box Testing* Pengembalian Dana Proyek 58

Tabel 4. 5 Jenis Serangan yang Teratasi 74

Tabel 4. 6 Hasil Pengujian Nilai *gasUsed* untuk Lima Kondisi Pemrosesan Pembentukan Proyek 78

Tabel 4. 7 Hasil Pengujian Nilai *gasUsed* untuk Tiga Kondisi Pemrosesan Pemberian Dana pada Proyek 81

Tabel 4. 8 Pembebanan Biaya pada Beberapa Sistem *Crowdfunding* 84

DAFTAR GAMBAR

Gambar 2. 1 Ilustrasi *Blockchain* 11

Gambar 2. 2 Detail *Block* pada *Blockchain* 12

Gambar 2. 3 Komputasi *Block Hash* 13

Gambar 2. 4 Arsitektur *Decentralized Application* 22

Gambar 2. 5 *Block Header* 30

Gambar 3. 1 Gambaran Umum Sistem 35

Gambar 3. 2 *Use Case Diagram* Sistem 36

Gambar 3. 3 *Activity Diagram* Pembentukan Proyek 38

Gambar 3. 4 *Activity Diagram* Pemberian Dana pada Proyek 40

Gambar 3. 5 *Activity Diagram* Pengambilan Dana Proyek 42

Gambar 3. 6 *Activity Diagram* Pengembalian Dana Proyek 43

Gambar 3. 7 Pengembangan Aplikasi *Web* Sistem *Crowdfunding* 48

Gambar 3. 8 Pengembangan *Smart Contract* Sistem *Crowdfunding* 49

Gambar 4. 1 Prosedur Transaksi Mata Uang Fiat 53

Gambar 4. 2 Prosedur Transaksi *Cryptocurrency* 53

Gambar 4. 3 Proses Pencatatan Data *Blockchain* 62

Gambar 4. 4 Struktur Rantai *Block* 62

Gambar 4. 5 Konfigurasi *Genesis Block* 65

Gambar 4. 6 Konfigurasi *Node* Pengujian 66

Gambar 4. 7 Gambaran Pengujian Mayoritas *Node* Jujur (Kondisi Pertama) 67

Gambar 4. 8 Rantai *Block* Setelah Proses *Mining* (Pengujian Kondisi Pertama) . 67

Gambar 4. 9 Sinkronisasi Rantai *Block Node* 3 (Pengujian Kondisi Pertama) 68

Gambar 4. 10 Pembentukan Double Spending (Pengujian Kondisi Kedua) 69
Gambar 4. 11 *Block Data* Transaksi 1 di Node 2 (Pengujian Kondisi Kedua) 70
Gambar 4. 12 *Block* Data Transaksi 2 di Node 3 (Pengujian Kondisi Kedua)..... 70
Gambar 4. 13 Sinkronisasi Rantai *Block* (Pengujian Kondisi Kedua)..... 71
Gambar 4. 14 *Block* Data Transaksi *Double Spending* Setelah Sinkronisasi (Pengujian Kondisi Kedua)..... 71
Gambar 4. 15 Penghapusan Data Chaindata Geth (Pengujian Kondisi Ketiga) ... 72
Gambar 4. 16 Jumlah *Block Node* 2 Setelah Penghapusan Data (Pengujian Kondisi Ketiga)..... 73
Gambar 4. 17 *Output Command Peer* Pada Node 2 (Pengujian Kondisi Ketiga) 73
Gambar 4. 18 Besar Biaya Transaksi (*transactionFee*) Eksekusi Pemrosesan Pembentukan Proyek dalam *Ether*..... 80
Gambar 4. 19 Besar Biaya Transaksi (*transactionFee*) Eksekusi Pemrosesan Pemberian Dana pada Proyek dalam *Ether*..... 83
Gambar 4. 20 Perbandingan Biaya Pemrosesan Pembentukan Proyek Galang Dana 87
Gambar 4. 21 Perbandingan Biaya Pemrosesan Pemberian Dana pada Proyek Galang Dana..... 88

BAB I

PENDAHULUAN

1.1. Latar Belakang

Crowdfunding merupakan suatu metode baru dalam melakukan pengumpulan dana yang diperoleh dari kontribusi masyarakat dalam memenuhi suatu tujuan tertentu. *Crowdfunding* memberikan kesempatan kepada masyarakat dalam menyalurkan bantuan uang ataupun materi untuk suatu kepentingan yang dianggap sedang membutuhkan. Kepentingan ini dapat berupa kepentingan yang bersifat personal dan kepentingan umum yang mencakup banyak orang.

Platform crowdfunding mulai dikembangkan oleh berbagai instansi untuk memudahkan masyarakat dalam melakukan penyaluran donasi untuk suatu kepentingan yang dianggap membutuhkan. Beberapa contoh *platform crowdfunding* yang ada saat ini yaitu Kickstarter, GoFundMe, dan Kitabisa.

Popularitas *crowdfunding* yang semakin berkembang menyebabkan peningkatan persaingan antara berbagai *platform crowdfunding* untuk menyediakan sistem yang baik dan efisien sebagai media yang digunakan oleh masyarakat dalam melakukan kegiatan penggalangan dana. Popularitas *crowdfunding* dapat dilihat pada contoh perkembangan Kitabisa, dimana berdasarkan *Kitabisa Online Giving Report 2018*, tercatat peningkatan penyaluran donasi yang dilakukan masyarakat setiap tahunnya selalu meningkat lebih dari 100%.

Perkembangan *platform crowdfunding* yang dampaknya begitu besar di masyarakat mengharuskan bahwa *platform* tersebut memiliki sistem yang dapat

dipercaya dan aman untuk digunakan oleh masyarakat dalam melakukan kegiatan penggalangan dana. Dalam pengembangan sistem *crowdfunding*, properti utama yang perlu diperhatikan yaitu keamanan data dan transparansi transaksi keuangan yang terjadi pada kegiatan penggalangan dana.

Transparansi pada transaksi keuangan yang terjadi dalam sistem *crowdfunding* dapat memberikan kepercayaan kepada pengguna dalam melakukan aktivitas pemberian dana pada suatu penggalangan dana. Sementara itu, keamanan data memberikan proteksi terhadap proses penggalangan dana yang terjadi dalam sistem *crowdfunding* sehingga berjalan secara sesuai tanpa adanya gangguan dari pihak yang tidak diketahui. Kedua properti ini sangat rentan dan dibutuhkan oleh pengguna sistem *crowdfunding* karena dalam kegiatan penggalangan dana terdapat proses transaksi keuangan yang jumlahnya tidak sedikit. Jika terjadi gangguan dari pihak yang tidak diketahui, maka kerugian yang dapat ditimbulkan akan berdampak besar pada banyak orang.

Properti transparansi dan keamanan pada sistem *crowdfunding* tidak dapat tercapai secara maksimal apabila penerapan dari sistem *crowdfunding* masih dilakukan secara tersentralisasi (*centralized*). Artinya, otoritas dari sistem hanya dipegang oleh pihak tertentu saja. (Kaushik, et al. 2017)

Selain properti transparansi dan keamanan, pengoptimalan biaya pemrosesan juga dibutuhkan pada sistem *crowdfunding* yang ada saat ini. Seluruh proses kontrak penggalangan dana masih dilakukan dengan bantuan dari sistem milik pihak ketiga, yang dalam hal ini adalah *platform crowdfunding*. Sistem *crowdfunding* umumnya menerapkan biaya pemrosesan pada suatu penggalangan

dana sebagai bentuk bayaran atas mengerjakan pemrosesan yang dibutuhkan dalam kegiatan galang dana. Besar biaya pemrosesan ini berkisar antara 3% sampai dengan 5% dari total donasi yang diterima pada suatu penggalangan dana. Model perhitungan biaya pemrosesan yang memiliki tarif berbasis persentase tidak menguntungkan bagi penggalangan dana yang memiliki dana dengan jumlah besar. Semakin besar dana yang diterima oleh penggalangan dana maka akan semakin besar juga biaya pemrosesan yang perlu dibayar.

Pada penelitian yang dilakukan oleh Satoshi Nakamoto (2008) dengan judul *Bitcoin: A Peer-to-Peer Electronic Cash System*, terdapat konsep teknologi yang disebut dengan *blockchain*. *Blockchain* memungkinkan suatu sistem untuk dikembangkan secara terdesentralisasi (*decentralized*) sehingga otoritas dari sistem tidak dipegang oleh satu pihak saja, tetapi semua entitas di dalam sistem memiliki hak otoritas yang sama. Sifat terdesentralisasi yang dimiliki oleh *blockchain* memberikan dampak yang signifikan pada properti keamanan dan transparansi dari suatu sistem.

Pengembangan *blockchain* ini awalnya diberlakukan untuk sistem transaksi mata uang digital, atau biasa disebut dengan *cryptocurrency*. Sistem ini memungkinkan suatu transaksi dapat dilakukan tanpa adanya pihak ketiga yang bertugas untuk melakukan validasi dalam menentukan keabsahan dari suatu transaksi. Validasi dari transaksi dilakukan bersama oleh seluruh *node* berupa entitas-entitas yang terhubung pada jaringan sistem. Pencatatan transaksi ini akan tersimpan di seluruh *node* yang tergabung pada jaringan sistem. Dengan kata lain, penyimpanan data tidak terpusat di satu tempat penyimpanan.

Dalam penerapan *blockchain* saat ini, terdapat berbagai macam pengembangan yang telah diterapkan, salah satunya adalah pengintegrasiannya dengan *smart contract*. *Smart contract* adalah perangkat lunak terotomatisasi berisi protokol kesepakatan antara dua pihak atau lebih yang dikelola menggunakan sistem terdesentralisasi.

Berdasarkan permasalahan yang ada pada sistem *crowdfunding* dan pengembangan yang terjadi pada teknologi *blockchain*, maka dalam Tugas Akhir ini akan dibangun sistem *crowdfunding* dengan memanfaatkan penggunaan teknologi *blockchain* untuk meningkatkan properti transparansi kegiatan penggalangan dana dan keamanan data yang ada pada sistem, serta integrasi *smart contract* untuk mengoptimalkan biaya pemrosesan yang umumnya diterapkan pada berbagai sistem *crowdfunding*.

1.2. Rumusan Masalah

Rumusan masalah yang akan diuraikan dalam Tugas Akhir ini adalah sebagai berikut:

1. Rendahnya transparansi dan keamanan yang ada pada sistem *crowdfunding* saat ini.
2. Besarnya biaya pemrosesan penggalangan dana yang umumnya diterapkan pada sistem *crowdfunding* saat ini.

1.3. Tujuan Penelitian

Tujuan yang akan dicapai dalam Tugas Akhir ini adalah sebagai berikut:

1. Membangun sistem *crowdfunding* dengan penerapan teknologi *blockchain* sehingga dapat meningkatkan transparansi dan keamanan.

2. Mengintegrasikan *smart contract* pada sistem *crowdfunding* untuk mengoptimalkan biaya pemrosesan penggalangan dana.

1.4. Manfaat Penelitian

Tugas Akhir ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Dari segi akademis, Tugas Akhir ini dapat digunakan sebagai referensi ilmiah terkait informasi mengenai proses pengembangan dan keuntungan penerapan *blockchain* dengan integrasi *smart contract* pada sistem *crowdfunding*.
2. Dari segi praktis, arsitektur sistem *crowdfunding* yang dibangun dalam Tugas Akhir ini dapat digunakan sebagai acuan dalam membangun suatu *platform crowdfunding* yang optimal.

1.5. Batasan Masalah

Batasan-batasan masalah yang ditetapkan dalam Tugas Akhir ini adalah sebagai berikut:

1. Sistem yang diterapkan menggunakan aplikasi sisi klien berbasis *website*.
2. Sistem dibangun dengan menggunakan *platform blockchain* Ethereum.
3. *Smart contract* sistem dibangun dengan menggunakan bahasa pemrograman Solidity.

1.6. Sistematika Penulisan

Sistematika penulisan yang digunakan dalam Tugas Akhir ini terbagi menjadi beberapa pokok bahasan, yaitu :

BAB I PENDAHULUAN

Bab ini memberikan gambaran terkait latar belakang masalah penelitian, rumusan masalah yang diuraikan, tujuan penelitian yang akan dicapai, manfaat penelitian yang diharapkan, batasan penelitian yang ditetapkan, dan sistematika penulisan penelitian.

BAB II TINJAUAN PUSTAKA

Bab ini memberikan kajian-kajian pustaka yang berkaitan dengan topik penelitian dan teori-teori dari berbagai referensi ilmiah yang digunakan dalam pelaksanaan penelitian.

BAB III METODE PENELITIAN

Bab ini memberikan gambaran terkait perancangan sistem yang akan direalisasikan beserta metode pengujiannya.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menguraikan hasil penelitian yang telah dilaksanakan.

BAB V PENUTUP

Bab ini berisi kesimpulan dari hasil penelitian dan saran untuk pengembangan penelitian lebih lanjut.

BAB II

TINJAUAN PUSTAKA

2.1. *Crowdfunding*

Salah satu manfaat utama yang diberikan oleh bank adalah ketersediaannya sebagai salah satu sumber pinjaman dana untuk masyarakat yang sedang membutuhkan. Kebutuhan pendanaan ini dapat berupa berbagai macam hal, salah satunya yaitu untuk mengembangkan usaha yang sedang dijalani oleh peminjam. Manfaat ini tentunya dapat diberikan apabila memenuhi beberapa persyaratan yang ditetapkan oleh bank, dimana syarat tersebut belum tentu dapat dipenuhi oleh individu ataupun kelompok masyarakat yang membutuhkan pendanaan.

Seiring dengan berkembangnya zaman, terbentuk metode baru dalam melakukan pengumpulan dana yang diperoleh dari kontribusi masyarakat dalam memenuhi suatu tujuan tertentu. Metode ini disebut sebagai *crowdfunding* atau bisa diartikan sebagai penggalangan dana. *Crowdfunding* umumnya dilakukan oleh suatu individu atau kelompok dengan menggunakan bantuan media publikasi untuk menyebarluaskan informasi terkait penggalangan dana yang dilakukan ke masyarakat. Media informasi ini dapat berupa media sosial atau media yang khsusus digunakan sebagai media *crowdfunding*, seperti Kickstarter, GoFundMe, Kitabisa, dan sebagainya.

Crowdfunding terbagi menjadi dua jenis yang dibedakan berdasarkan bentuk kesepakatan antara penggalang dana dan pemberi dana, yaitu *crowdfunding* yang memiliki upah yang akan diberikan kepada pemberi dana

apabila target total pendanaan yang ditetapkan tercapai dan *crowdfunding* yang tidak memiliki upah sama sekali, dengan kata lain dana yang diberikan tergolong sebagai donasi. (Belleflamme, Lambert and Schwienbacher 2013)

Crowdfunding yang dibentuk umumnya memiliki tujuan pendanaan yang jelas. Tujuan pendanaan ini dapat berdasarkan kebutuhan masyarakat di suatu daerah ataupun kebutuhan personal dari suatu individu dan kelompok. Tujuan pendanaan yang jelas dan sesuai dalam suatu penggalangan dana dapat meningkatkan insentif masyarakat dalam berkontribusi sebagai pemberi dana.

Insentif masyarakat untuk berkontribusi sebagai pemberi dana pada suatu *crowdfunding* merupakan hal utama yang harus ditingkatkan oleh penggalang dana untuk dapat mencapai target pendanaan yang ditetapkan. Selain daripada tujuan pendanaan yang jelas dan sesuai, intensif masyarakat dapat ditingkatkan cara lain seperti menyampaikan seluruh informasi yang berhubungan dengan *crowdfunding* yang diadakan secara jelas, meningkatkan publikasi dari *crowdfunding* yang diadakan sehingga dapat mencakup masyarakat yang lebih luas, dan menjaga kepercayaan masyarakat terkait kesesuaian seluruh kegiatan yang terjadi pada *crowdfunding* yang diadakan.

Media sosial merupakan media yang umum digunakan oleh masyarakat dalam melakukan publikasi *crowdfunding*. Media ini banyak digunakan oleh pihak penggalang dana karena kemudahannya dalam menyebarluaskan informasi dari *crowdfunding* yang diadakan kepada masyarakat. Walaupun demikian, penggunaan media sosial sebagai media publikasi *crowdfunding* masih memiliki kekurangan. Kekurangan ini yaitu media sosial tidak memiliki fitur yang dapat

memberikan jaminan bahwa *crowdfunding* yang diadakan oleh suatu individu atau kelompok bukan merupakan suatu rekayasa penipuan untuk mendapatkan keuntungan personal. Sebagai akibatnya, kepercayaan terhadap kebenaran dari *crowdfunding* yang diadakan tidak dapat terbentuk secara utuh.

Platform khusus *crowdfunding* saat ini telah banyak dikembangkan untuk memenuhi kebutuhan masyarakat dalam melakukan kegiatan penggalangan dana. Selain sebagai media publikasi, *platform* khusus ini menyediakan berbagai macam fitur untuk memudahkan masyarakat dalam membentuk *crowdfunding* secara efisien dan sesuai. Fitur yang disediakan dapat berupa verifikasi kebenaran dan keabsahan dari suatu *crowdfunding*, integrasi *payment gateway* untuk memudahkan kegiatan pemberian dana pada suatu *crowdfunding*, dan sebagainya.

2.2. *Blockchain*

Teknologi *blockchain* awalnya dikembangkan pada Bitcoin (Nakamoto 2008), yaitu sistem pembayaran elektronik pada jaringan *peer-to-peer* yang bersifat terdesentralisasi tanpa adanya institusi finansial yang bertindak sebagai pengatur jalannya transaksi. *Blockchain* ini diterapkan untuk menghilangkan kebutuhan institusi finansial sebagai pihak ketiga dalam pengelolaan suatu proses transaksi.

Blockchain pada dasarnya merupakan basis data transaksi yang terdistribusi pada berbagai *node* yang tergabung dalam suatu jaringan *peer-to-peer*. *Blockchhain* merupakan salah satu bentuk dari *Distributed Ledger Technology* (DLT), dimana teknologi ini bersifat terdesentralisasi dan memiliki protokol konsensus yang digunakan untuk mencapai kesepakatan bersama dalam

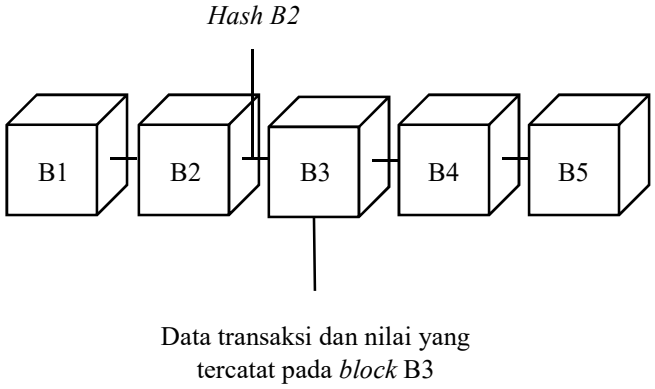
proses pengelolaan basis data yang ada. Akan tetapi, terdapat suatu perbedaan pada *blockchain* jika dibandingkan dengan DLT pada umumnya. Perbedaan ini terletak di struktur basis data yang ada pada *blockchain*, dimana setiap data transaksi yang tercatat akan tergabung ke dalam suatu *block* yang saling terhubung antara satu sama lain dan tidak dapat mengalami perubahan. (Hileman and Rauchs 2017)

Pencatatan data pada teknologi *blockchain* dilakukan melalui beberapa tahap, yaitu :

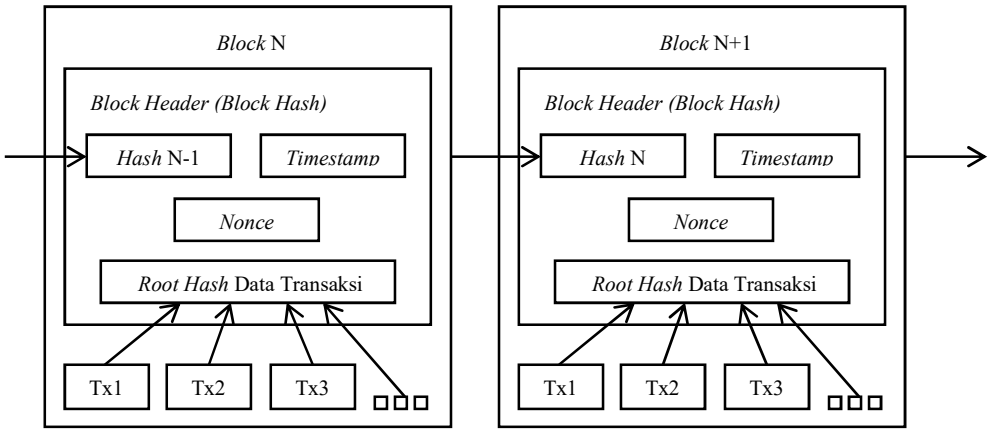
1. *Node* akan melakukan transaksi data menggunakan *digital signature* dan kemudian akan mengumumkannya ke jaringan. *Digital signature* merupakan tanda pengenal yang digunakan oleh suatu *node* dalam jaringan *blockchain*.
2. *Node* lain yang tergabung dalam jaringan akan menerima pengumuman transaksi dan kemudian menggabungkannya ke dalam suatu *block* baru.
3. *Node* penerima akan melakukan eksekusi pembentukan *block* berdasarkan protokol konsensus yang ditetapkan, seperti *Proof of Work*. Pembentukan *block* ini dikenal dengan istilah *mining*.
4. Setelah *node* penerima berhasil membentuk *block* baru berdasarkan protokol yang ditetapkan, selanjutnya *block* baru ini akan diumumkan ke jaringan sehingga dapat ditambahkan ke rantai *block* yang ada.

Pada *blockchain* sistem Bitcoin (Nakamoto 2008), setelah transaksi mata uang digital (*cryptocurrency*) dilakukan oleh suatu *node* menggunakan *digital signature*-nya, *node* tersebut selanjutnya akan mengumumkan transaksi yang

terjadi ke jaringan. *Node* lain kemudian akan menerima pengumuman transaksi-transaksi yang terjadi dan menggabungkannya dengan membentuk *block* menggunakan mekanisme protokol *Proof of Work*. Mekanisme *Proof of Work* akan membentuk suatu *block* baru yang terhubung ke *block* terakhir pada rantai *block* yang ada menggunakan fungsi *hash* kriptografi, seperti SHA-256. *Block* dibentuk dengan cara menghitung nilai *hash*-nya. Nilai *hash* ini biasa disebut sebagai *block hash* atau *block header*. *Block hash* akan didapatkan melalui komputasi fungsi *hash* dari nilai data transaksi yang tergabung dalam *block* dan beberapa nilai khusus, seperti *timestamp*, *nonce*, ataupun *block hash* dari *block* terakhir yang sebelumnya terbentuk pada rantai *block*. Hubungan antara suatu *block* dan *block* lainnya akan terbentuk dengan adanya penggunaan nilai *block hash* terakhir sebagai nilai masukan (*input*) dalam pembentukan nilai *block hash* baru. Ilustrasi *blockchain* dapat dilihat pada Gambar 2.1 dan Gambar 2.2.



Gambar 2. 1 Ilustrasi *Blockchain*

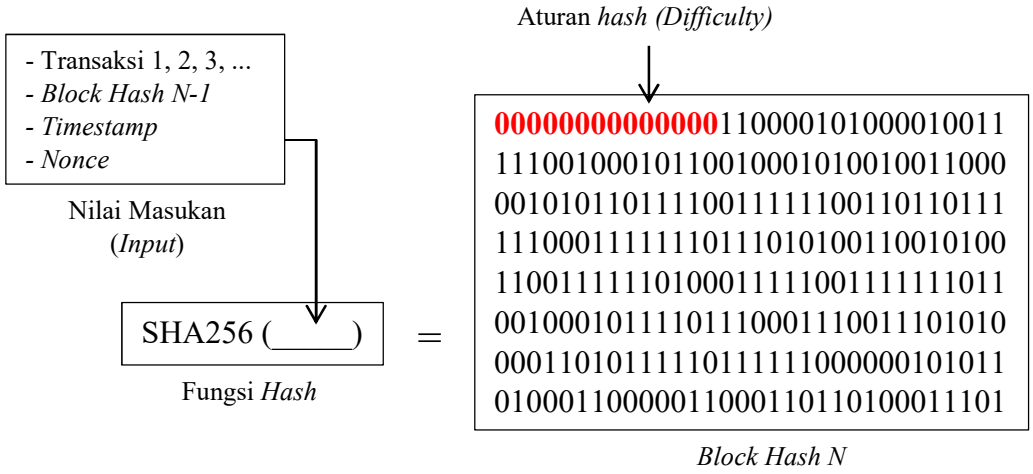


Gambar 2. 2 Detail *Block* pada *Blockchain*

Protokol konsensus *Proof of Work* merupakan mekanisme yang digunakan jaringan *blockchain* untuk mencapai kesepakatan bersama dalam pembentukan *block* data yang valid. Kesepakatan didapatkan berdasarkan besar komputasi yang digunakan dalam suatu proses pembentukan *block*. *Proof of Work* ini dapat diartikan sebagai bukti penggunaan komputasi yang besar dalam proses pembentukan suatu *block*.

Dalam mekanisme protokol *Proof of Work*, terdapat aturan yang perlu dipenuhi dalam perhitungan *block hash* dari suatu *block* baru. Aturan ini biasa disebut sebagai *difficulty*. *Difficulty* mengharuskan nilai dari suatu *block hash* memiliki beberapa angka nol pada bit awalnya. Dalam perhitungan nilai *block hash* yang sesuai berdasarkan *difficulty*, nilai masukan *nonce* merupakan kunci utama dalam penyelesaiannya. *Nonce* adalah nilai masukan yang ditentukan oleh *node* dalam melakukan komputasi *block hash*. Penggunaan nilai masukan yang dinamis seperti *nonce* akan dibutuhkan untuk mendapatkan *block hash* yang sesuai berdasarkan *difficulty* yang ditetapkan. Nilai *nonce* dibutuhkan oleh *node* dalam komputasi *block hash* karena nilai masukan lain seperti data utama,

timestamp, ataupun *block hash* dari *block* sebelumnya memiliki nilai yang tetap. Gambaran komputasi *block hash* dapat dilihat pada Gambar 2.3.



Gambar 2. 3 Komputasi *Block Hash*

Fungsi *hash* kriptografi seperti SHA-256 akan menghasilkan nilai *hash* yang sangat tidak terduga dan bersifat satu arah. Dengan kata lain, *hash* yang terbentuk tidak dapat terdekripsi untuk mendapatkan nilai masukan awal yang digunakan pada fungsinya. *Block hash* yang memenuhi kriteria *difficulty* yang ditetapkan hanya dapat dihasilkan dengan cara menjalankan fungsi *hash* secara berulang kali menggunakan *nonce* yang berbeda. *Node* akan saling berkompetisi dalam membentuk suatu *block* dengan cara mencari *nonce* yang sesuai sehingga *block hash* yang didapatkan dapat memenuhi kriteria *difficulty*. Proses ini akan membutuhkan komputasi yang besar. Dengan demikian, didapatkannya nilai *nonce* yang sesuai dapat menjadi bukti bahwa pembentukan *block* telah melalui proses komputasi yang besar. *Block* yang terbentuk dengan nilai *nonce* yang sesuai akan dianggap oleh jaringan sebagai *block* yang valid.

Umumnya, berdasarkan protokol *blockchain* yang ditetapkan, ketika suatu *block* berhasil dibentuk oleh suatu *node*, *node* tersebut akan mendapatkan hadiah berupa *cryptocurrency*. Akan tetapi, karena proses pembentukan *block* ini membutuhkan komputasi yang besar, *node* memiliki pilihan untuk melakukannya atau tidak. *Node* yang melakukan pembentukan *block* dikenal dengan istilah *miner*.

Ketika *miner* telah menemukan *nonce* yang sesuai, selanjutnya *block* yang dibentuk akan diumumkan ke seluruh *node* yang tergabung dalam jaringan. Seluruh *node* akan melakukan verifikasi terkait pembentukan *block* hanya dengan sekali menjalankan fungsi *hash* menggunakan nilai masukan yang telah didapatkan oleh *miner*. Apabila *block* yang terbentuk sesuai berdasarkan protokol yang ditetapkan, maka *block* tersebut akan dimasukkan ke dalam rantai *block* yang sudah ada.

Teknologi *blockchain* terus berkembang dan telah dikenal secara umum sebagai *framework* dalam pengembangan sistem yang bersifat terdesentralisasi (Gao, Hatcher and Yu 2018). Setiap pengembangan sistem terdesentralisasi akan menerapkan *blockchain* dengan berbagai jenis perubahan berdasarkan kebutuhan yang ada. Perubahan ini mencakup jenis protokol konsensus yang digunakan, implementasi konsep teknologi lain, mekanisme pencatatan data, dan sebagainya.

Blockchain memiliki berbagai macam jenis yang dibedakan berdasarkan tiga aspek, yaitu aksesibilitas data, partisipasi *node* dan fungsionalitasnya (Shrivas and Yeboah 2018). Jenis-jenis *blockchain* dapat dilihat pada Tabel 2.1.

Tabel 2. 1 Jenis *Blockchain*

Jenis	Aspek	Penjelasan
Public Blockchain	Aksesibilitas data	Jenis *blockchain* ini memperbolehkan setiap individu/kelompok untuk bergabung sebagai *node* dalam melakukan pembacaan dan pencatatan data. (Lin and Liao 2017)
Consortium Blockchain	Aksesibilitas data	Jenis *blockchain* ini pada dasarnya bersifat tertutup, tetapi dapat memperbolehkan individu/kelompok tertentu yang tergabung dalam konsorsium untuk berpartisipasi sebagai *node* dalam melakukan pembacaan dan pencatatan data. (Lin and Liao 2017)
Private Blockchain	Aksesibilitas data	Jenis *blockchain* ini bersifat tertutup dan hanya ada satu pihak *node* saja yang dapat melakukan pembacaan dan pencatatan data. (Lin and Liao 2017)

Permissionless Blockchain	Partisipasi *node*	Jenis *blockchain* ini tidak memiliki protokol perizinan yang harus dipenuhi oleh suatu pihak untuk berpartisipasi sebagai *node*. (Rennock, Cohn and Butcher 2018)
Permissioned Blockchain	Partisipasi *node*	Jenis *blockchain* ini memiliki protokol perizinan yang harus dipenuhi oleh suatu pihak untuk dapat berpartisipasi sebagai *node*. (Rennock, Cohn and Butcher 2018)
Stateless Blockchain	Fungsionalitas	Jenis *blockchain* ini hanya dapat menjalankan logika komputasi sederhana saja seperti pencatatan data transaksi. (Hileman and Rauchs 2017)
Stateful Blockchain	Fungsionalitas	Jenis *blockchain* ini dapat menjalankan logika komputasi yang lebih kompleks daripada hanya sekedar komputasi pencatatan data. Contoh komputasi kompleks ini seperti

		pemrosesan *state* berdasarkan logika bisnis yang ada dalam suatu sistem. (Hileman and Rauchs 2017)

Dengan penerapan *framework blockchain* pada suatu sistem, berbagai keuntungan dapat tercapai (Sarmah 2018). Keuntungan-keuntungan yang didapatkan antara lain sebagai berikut :

a. Sistem akan bersifat terdesentralisasi, dimana pengelolaan sistem dilakukan tanpa adanya otoritas yang terpusat.
b. Pengguna akan memiliki wewenang untuk berpartisipasi dalam melakukan pengelolaan data yang ada.
c. Data dapat tersedia secara konsisten, lengkap, dan terkini karena tersebar pada setiap *node* yang tergabung dalam jaringan sistem.
d. Dikarenakan tidak adanya wewenang yang terpusat, pengguna dapat yakin bahwa data akan dieksekusi berdasarkan mekanisme dari protokol yang ada.
e. *Blockchain* memberikan kekekalan pada setiap datanya sehingga data yang telah tercatat tidak dapat termanipulasi.
f. Data yang tercatat dapat terlindungi karena terenkripsi menggunakan mekanisme dari protokol *blockchain*.
g. Sistem memiliki kekebalan pada berbagai jenis serangan (*cyber attack*) karena dibangun menggunakan jaringan *peer-to-peer*. Jaringan sistem

dapat beroperasi secara normal walaupun terdapat *node* yang tidak aktif akibat dari suatu serangan.

Dengan adanya arsitektur yang sangat kompleks dan integrasi berbagai macam teknologi yang diterapkan sehingga dapat menimbulkan bermacam-macam keuntungan, teknologi *blockchain* memiliki bidang penerapan yang luas (Gao, Hatcher and Yu 2018). Penerapan-penerapan ini dapat dilihat pada Tabel 2.2.

Tabel 2. 2 Bidang Aplikasi Blockchain

Bidang Aplikasi	**Penjelasan**
Internet of Things (IoT)	Sistem *IoT* dengan skala yang besar dapat dikembangkan secara terdesentralisasi dengan jaringan *peer-to-peer* menggunakan *blockchain*. Sifat terdesentralisasi dan dengan adanya protokol *blockchain* yang diterapkan dapat memberikan proteksi pada sistem *IoT* dari serangan yang umumnya terjadi pada sistem yang terpusat.
Big Data	*Blockchain* dianggap mampu memberikan solusi pada permasalahan manajemen data dalam sistem *big data* seperti proteksi data personal ataupun properti digital. Keandalan dan keamanan yang lebih dalam proses pencatatan data merupakan manfaat yang dapat diberikan

	oleh *blockchain* pada sistem *big data*.
Cloud & *Edge Computing*	Proteksi data merupakan alasan utama penerapan *blockchain* dalam sistem *cloud* ataupun *edge computing*. Data yang tercatat menggunakan mekanisme *blockchain* tidak dapat termanipulasi sehingga kredibilitas data dalam sistem *cloud/edge computing* dapat terjaga.
Manajemen Identitas	Dalam bidang ini, *blockchain* memberikan kemampuan dalam membentuk suatu identitas menggunakan *digital signature*. *Digital signature* akan digunakan sebagai tanda untuk memverifikasi kebenaran suatu identitas.
Finansial & *Cryptocurrency*	Teknologi *blockchain* awalnya dikembangkan pada bidang finansial. *Blockchain* memberikan kemungkinan dalam membentuk suatu sistem transaksi yang terdesentralisasi, dimana kebutuhan akan pihak ketiga sebagai pengelola transaksi dapat dihilangkan.
Smart Contract & Otomatisasi	*Smart contract* pada dasarnya merupakan kode-kode yang dibentuk untuk menjalankan suatu logika bisnis. *Smart contract* dapat dikembangkan menggunakan *blockchain* sehingga logika bisnis yang ada dapat dijalankan

	secara otomatis dengan menggunakan jaringan yang terdesentralisasi.
Rantai Suplai	Pada rantai suplai, terdapat berbagai entitas tergabung dalam prosesnya sehingga permasalahan kepercayaan menjadi hal utama di dalamnya. *Blockchain* memberikan solusi dalam memastikan integritas data pada sistem rantai suplai.
Informasi Medis	Dikarenakan informasi medis bersifat pribadi dan sensitif, *blockchain* dapat diimplementasikan dalam mengelola aksesibilitas data sehingga pihak yang memiliki wewenang saja yang dapat melihat dan melakukan penyimpanan.
Komunikasi & Jaringan	*Blockchain* memberikan proteksi dalam proses komunikasi yang terjadi pada suatu jaringan menggunakan *digital signature* sebagai metode dalam melakukan verifikasi kebenaran identitas.

2.3. *Smart Contract*

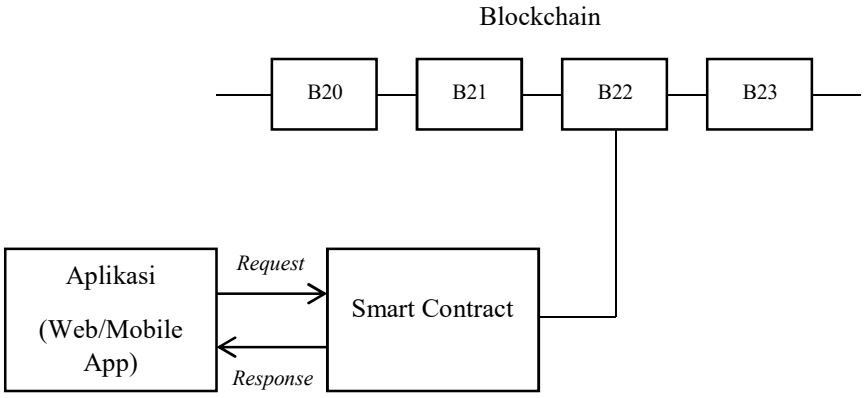
Kontrak pada dasarnya merupakan cara untuk membentuk kesepakatan persetujuan terhadap suatu hal (Szabo 1996). Kontrak secara umum digunakan untuk keperluan dalam membangun protokol persetujuan terhadap suatu hubungan yang dibentuk oleh dua pihak individu/kelompok atau lebih. Kontrak akan dibentuk oleh dua pihak atau lebih dengan menggunakan bantuan supervisi

dari pihak ketiga yang dianggap terpercaya. Supervisi ini sangat penting dimiliki untuk menghindari adanya manipulasi oleh salah satu pihak terhadap kontrak yang dibentuk.

Seiring dengan perkembangan teknologi, terbentuk suatu konsep kontrak baru yang dinamakan dengan *smart contract*. *Smart contract* pada dasarnya merupakan perangkat lunak berisi protokol kesepakatan dan hubungan antara dua pihak atau lebih yang dikelola menggunakan sistem terdesentralisasi. Pengawasan terhadap kesepakatan dan hubungan yang terbentuk akan dilakukan oleh semua pihak yang tergabung dalam jaringan berdasarkan protokol konsensus sistem sehingga kebutuhan supervisi dari suatu pihak ketiga tidak diperlukan.

Smart contract memungkinkan adanya pengembangan yang lebih pada teknologi *blockchain* karena kedua teknologi pada dasarnya diterapkan pada ekosistem yang sama, yaitu dibangun dengan menggunakan jaringan terdesentralisasi. *Blockchain* yang pada awalnya hanya digunakan untuk melakukan proses komputasi sederhana, seperti pencatatan data transaksi, telah dapat dikembangkan untuk melakukan proses komputasi yang lebih kompleks dengan integrasi *smart contract* (Jani 2020).

Kombinasi dari teknologi *blockchain* dan *smart contract* ini dinamakan *decentralized application*. Arsitektur *decentralized application* dapat dilihat pada Gambar 2.4.



Gambar 2. 4 Arsitektur *Decentralized Application*

Decentralized application, bekerja dengan tiga komponen utama, yaitu aplikasi klien, *smart contract*, dan *blockchain*. Aplikasi klien dapat berupa aplikasi *web* ataupun *mobile* yang memiliki kemampuan untuk berkomunikasi dengan *smart contract* melalui *application programming interface* (API). *Smart contract* sendiri akan bekerja layaknya seperti aplikasi *server-side* (*back-end*). *Smart contract* tersimpan pada *blockchain* yang tersebar di setiap *node* yang tergabung dalam jaringan terdesentralisasi. *Smart contract* akan dieksekusi berdasarkan permintaan yang dikirim oleh aplikasi klien dan hasilnya akan dikembalikan dalam bentuk respon data. (Sayeed, Marco-Gisbert and Caira 2020)

2.4. Ethereum

Ethereum merupakan salah satu bentuk pengembangan dari teknologi *blockchain* yang awalnya diterapkan pada Bitcoin. Ethereum dikembangkan untuk memungkinkan pengerjaan komputasi yang lebih kompleks pada *framework blockchain* daripada hanya sekedar komputasi pencatatan data transaksi.

Sama halnya dengan Bitcoin, Ethereum pada dasarnya merupakan sistem pembayaran mata uang digital (*cryptocurrency*) yang terdesentralisasi. Perbedaan

utama yang ada pada Ethereum yaitu sistemnya dibangun dengan menggunakan bahasa pemrograman *turing-complete* (Ethereum Community 2020) sehingga memungkinkan pengerjaan komputasi yang lebih kompleks, seperti *smart contract*, dilakukan dengan mekanisme *blockchain*. Ethereum telah dikenal luas sebagai *framework* dalam mengembangkan *decentralized application*.

Blockchain Ethereum pada dasarnya merupakan *state machine* berbasis transaksi. *State machine* sendiri mengacu pada proses pengelolaan suatu susunan *input* untuk mengubah *state* yang tersimpan. *State machine* pada Ethereum disebut sebagai Ethereum Virtual Machine (EVM). Pengubahan suatu *state* dilakukan oleh suatu *node* dengan mengirim transaksi yang berisi *input* untuk melakukan proses pengubahan *state*. (Kasireddy 2017)

State pada Ethereum merepresentasikan seluruh transaksi yang terjadi. Sama halnya dengan Bitcoin, transaksi-transaksi ini tergabung pada suatu *block*, dimana setiap *block* ini saling terhubung dengan *block* yang telah terbentuk sebelumnya. *Block* akan dibentuk dengan menggunakan protokol konsensus yang dinamakan GHOST (*Greedy Heavies Observed Subtree*). (Kasireddy 2017)

Protokol GHOST pada dasarnya merupakan protokol *Proof of Work*, tetapi dengan beberapa penyempurnaan. Protokol GHOST menyelesaikan permasalahan terkait *stale block*, yaitu *block* lain yang terbentuk secara bersamaan dengan *block* yang tervalidasi. Dalam protokol GHOST, *miner* tetap akan menerima hadiah apabila membentuk *stale block*. Hal tersebut diterapkan karena pembentukan *block* pada Ethereum tergolong lebih cepat jika dibandingkan dengan Bitcoin.

Sebagai akibatnya, kemungkinan terbentuknya suatu *stale block* pada Ethereum lebih besar dibandingkan pada Bitcoin.

2.4.1. *Account*

Account merupakan tanda pengenal (identitas) dari suatu entitas, seperti pengguna, *node*, ataupun *smart contract*, yang tergabung dalam Ethereum. *Account* pada Ethereum terbagi menjadi dua jenis, yaitu *externally owned account* dan *contract account* (Kasireddy 2017). *Externally owned account* pada dasarnya merupakan akun yang dimiliki oleh pengguna ataupun *node*. Sementara *contract account* merupakan tanda pengenal dari suatu *smart contract* yang tercatat dalam Ethereum. Pada dasarnya, hanya *externally owned account* yang dapat memulai mengirim pesan ke *account* lainnya dengan cara membuat dan menandatangani transaksi menggunakan *digital signature* berupa *private key*, sementara *contract account* hanya bisa melakukan transaksi sebagai bentuk respon apabila telah menerima suatu transaksi dari *account* lain.

Account merupakan obyek yang membentuk *state* pada Ethereum. Setiap *account* memiliki alamat (*address*) dan terdiri dari empat komponen *state* (Wood 2019), berupa :

- *nonce*, merupakan nilai yang merepresentasikan jumlah transaksi yang telah dilakukan oleh suatu *account*.
- *balance*, merupakan jumlah *cryptocurrency* Ethereum (Ether) yang dimiliki oleh suatu *account*.
- *storageRoot*, merupakan *root hash* dari konten-konten milik suatu *account* yang tersimpan. Secara *default*, *storageRoot* memiliki nilai kosong.

- *codeHash*, merupakan *hash* dari kode yang dimiliki oleh suatu *account* yang akan dieksekusi oleh Ethereum Virtual Machine (EVM). Pada *contract account*, *codeHash* merupakan *hash* dari kode *smart contract* yang dibentuk. Sementara pada *externally owned account*, *codeHash* merupakan *hash* dari *string* yang bernilai kosong.

2.4.2. Transaksi

Pada dasarnya, transaksi merupakan suatu instruksi yang dihasilkan oleh *externally owned account*. Transaksi akan dihasilkan dengan menggunakan *digital signature* yang berbasis *public/private key* milik *externally owned account*. Setiap transaksi yang dihasilkan akan tercatat ke dalam *blockchain* Ethereum.

Transaksi dalam Ethereum terbagi menjadi dua jenis, yaitu *message call* dan *contract creation* (Kasireddy 2017). *Message call* merupakan transaksi yang dilakukan dalam melakukan suatu perubahan *state*. *Contract creation* merupakan transaksi yang dilakukan untuk membentuk *contract* baru.

Setiap proses komputasi yang dibutuhkan untuk memproses suatu transaksi dalam Ethereum akan dieksekusi oleh *node miner*. *Miner* akan membutuhkan sebuah bayaran sebagai bentuk hadiah dalam mengeksekusi proses komputasi dari suatu transaksi. Biaya pemrosesan ini dibayar oleh *account* selaku pengirim transaksi berdasarkan unit khusus dalam Ethereum yang dinamakan *gas* (Kasireddy 2017). *Gas* pada dasarnya merupakan satuan unit yang digunakan untuk mengukur besar komputasi yang dibutuhkan dari suatu transaksi.

Penentuan biaya transaksi akan diukur dengan menggunakan dua variabel yaitu *gasPrice* dan *gasLimit*. *gasPrice* merupakan jumlah Ether yang pengirim

transaksi bersedia bayar untuk penggunaan satu *gas* dalam proses komputasi transaksi. Sementara *gasLimit* merupakan jumlah maksimum *gas* yang akan dipakai dalam proses komputasi transaksi. Kedua variabel ini akan ditentukan oleh pengirim transaksi. Sebagai contoh, pengirim transaksi menentukan *gasLimit* sebesar 50000 dan *gasPrice* sebesar 20 Gwei (1 Ether = 1000000000 Gwei) sehingga menghasilkan biaya transaksi sebesar 50000 x 20 Gwei = 100000 Gwei = 0.0001 Ether.

Adapun komponen-komponen yang terdapat dalam transaksi dapat dilihat pada Tabel 2.3.

Tabel 2. 3 Komponen Transaksi (Kasireddy 2017)

Komponen	**Penjelasan**
nonce	Nomor transaksi yang ditentukan berdasarkan jumlah transaksi yang telah dilakukan oleh *account* pengirim transaksi.
gasPrice	Jumlah Ether yang ditentukan oleh pengirim transaksi untuk membayar setiap unit *gas* yang digunakan dalam proses eksekusi transaksi.
gasLimit	Jumlah maksimum unit *gas* yang dapat digunakan dalam proses eksekusi transaksi. *gasLimit* akan ditentukan oleh pengirim transaksi.
to	*Address* dari *account* penerima transaksi.

value	Jumlah Ether yang akan ditransfer dari pengirim transaksi ke penerima transaksi.
v, r, s	Digunakan untuk menghasilkan *digital signature* sebagai pengidentifikasi pengirim transaksi.
init	Sebuah bagian kode Ethereum Virtual Machine (EVM) yang digunakan untuk menginisialisasi *contract account* baru. Nilai ini hanya ada pada transaksi jenis *contract creation*.
data	*Input* yang akan digunakan untuk mengubah suatu *state* pada Ethereum. Nilai ini hanya ada pada transaksi jenis *message call*.

2.4.3. *Block*

Block pada Ethereum terdiri dari tiga bagian, yaitu *block header*, informasi transaksi-transaksi yang tergabung dalam *block*, dan kumpulan *block header* dari *ommer*, yaitu *stale block* yang terbentuk secara bersamaan dengan *block* yang tervalidasi. (Kasireddy 2017)

Pada Ethereum, *ommer* dipertimbangkan sebagai salah satu penunjang mekanisme *blockchain* agar dapat berjalan dengan baik. Hal tersebut dikarenakan Ethereum memiliki waktu pembentukan *block* yang lebih cepat (15 detik) dibanding *blockchain* lain seperti Bitcoin (10 menit). Semakin cepat waktu

pembentukan *block* pada suatu *blockchain* maka semakin besar juga persaingan yang ada dalam proses pembentukan *block*.

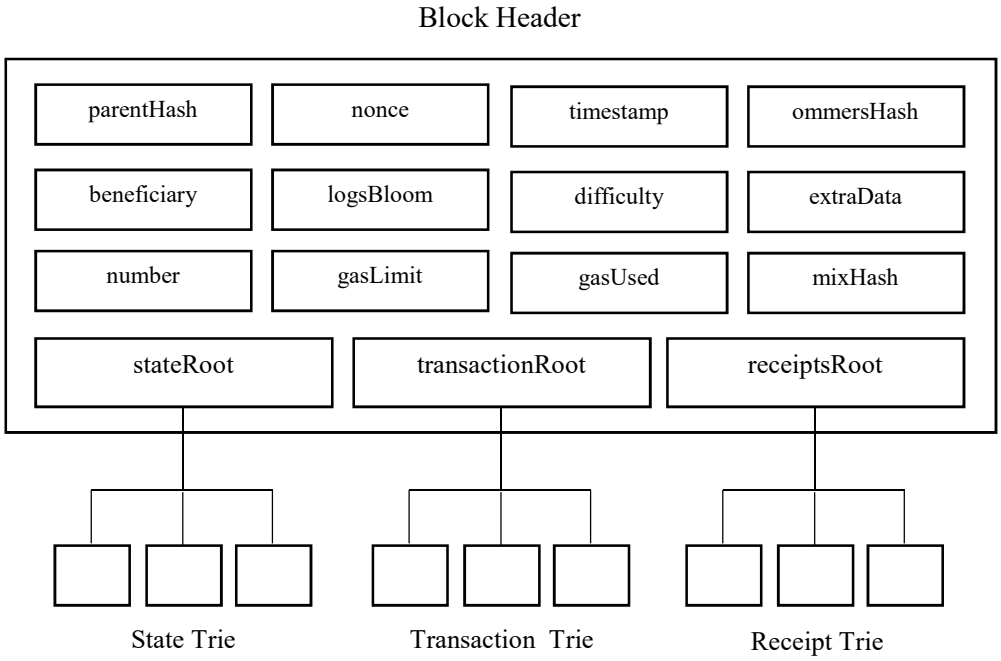
Protokol *blockchain* pada umumnya hanya memberikan hadiah kepada *miner* yang melakukan pembentukan *block* yang tervalidasi. Pada protokol yang diterapkan Ethereum, *miner* yang membentuk *ommer* juga akan mendapatkan hadiah, walaupun jumlahnya tidak sebanyak hadiah *block* tervalidasi. Dengan demikian, insentif *miner* dapat bertambah dalam melakukan pembentukan *block*.

Block dalam Ethereum pada dasarnya mirip seperti *block* dalam Bitcoin, hanya saja berisi tambahan informasi khusus berdasarkan protokol yang ditetapkan. Setiap informasi yang ada akan tergabung dan membentuk *block header*. Informasi-informasi yang terdapat pada *block header* dari suatu *block* yaitu (Wood 2019) :

- *parentHash* : *hash* dari *block header* milik *parent block*, yaitu *block* terakhir sebelum *block* terkait.
- *ommersHash* : *hash* dari daftar *ommer block* terkait.
- *beneficiary* : *address* dari *account* yang menerima biaya pembayaran dalam proses *mining block* terkait.
- *stateRoot* : *hash* dari *state* yang tersimpan pada *block* terkait. *Hash* ini terbentuk menggunakan struktur Merkle Patricia Trie.
- *transactionRoot* : *hash* dari transaksi yang tercatat pada *block* terkait. *Hash* ini terbentuk menggunakan struktur Merkle Patricia Trie.
- *receiptsRoot* : *hash* dari resi transaksi yang tercatat pada *block* terkait. *Hash* ini terbentuk menggunakan struktur Merkle Patricia Trie.

- *logsBloom* : struktur data *bloom filter* yang terdiri atas *log*/catatan informasi.
- *difficulty* : tingkat *difficulty* dari penyelesaian *block* terkait.
- *number* : nilai penjumlahan (*count*) dari *block* terkait.
- *gasLimit* : batas maksimum *gas* yang dapat digunakan dalam pemrosesan komputasi transaksi pada *block* terkait.
- *gasUsed* : jumlah total *gas* yang digunakan pada pemrosesan komputasi transaksi dari *block* terkait.
- *timestamp* : *timestamp* yang berbasis unix dari pembentukan *block* terkait.
- *extraData* : data ekstra yang berhubungan dengan *block* terkait.
- *mixHash* : sebuah *hash*, yang jika dikombinasikan dengan *nonce*, akan membuktikan bahwa *block* terkait telah dibentuk melalui proses komputasi yang cukup.
- *nonce* : sebuah *hash*, yang jika dikombinasikan dengan *mixHash*, akan membuktikan bahwa *block* terkait telah dibentuk melalui proses komputasi yang cukup.

Ilustrasi *block header* dari suatu *block* pada Ethereum dapat dilihat pada Gambar 2.5.



Gambar 2. 5 *Block Header*

2.4.4. Eksekusi Transaksi

Eksekusi transaksi dalam Ethereum pada dasarnya mengacu pada proses transisi *state* yang ada (Wood 2019). Sebelum transaksi dieksekusi, terdapat beberapa syarat yang harus dipenuhi terlebih dahulu, yaitu :

- Transaksi harus memiliki format yang sesuai. Format *Recursive Length Prefix* (RLP) merupakan format data yang diterima oleh Ethereum.
- *Signature* transaksi yang valid.
- *Nonce* transaksi yang valid.
- *gasLimit* transaksi harus memiliki jumlah yang lebih besar atau sama dengan jumlah *gas* yang terpakai dalam eksekusi komputasi transaksi.

- Jumlah Ether yang dimiliki oleh pengirim transaksi dapat menutupi biaya pemakaian *gas* yang terbentuk berdasarkan perhitungan *gasLimit* dan *gasPrice* yang ditentukan.

Apabila syarat-syarat yang diperlukan telah terpenuhi, selanjutnya eksekusi transaksi dapat dilakukan. Eksekusi transaksi secara umum akan dilakukan melalui tahap-tahap sebagai berikut :

1. Biaya transaksi akan diukur berdasarkan *gasLimit* dan *gasPrice* yang ditentukan. Ether pengirim transaksi akan terpotong berdasarkan hasil perhitungan biaya transaksi tersebut.
2. Menginisialisasi jumlah *gas* yang akan digunakan selama proses komputasi transaksi.
3. Komputasi-komputasi yang diperlukan akan dieksekusi pada Ethereum Virtual Machine (EVM) oleh *miner*.
4. Ketika komputasi yang diperlukan oleh transaksi telah terproses, maka biaya yang terbayar untuk sisa *gas* yang tidak terpakai akan dikembalikan ke pengirim transaksi. Disaat yang bersamaan, biaya *gas* yang terpakai akan dikirim ke *miner*.
5. *State* baru dan *logs* yang berisi catatan transaksi yang terjadi akan terbentuk.

2.4.5. Arsitektur *Blockchain*

Ethereum memiliki arsitektur *blockchain* yang hampir sama dengan *blockchain* Bitcoin. Perbedaannya terletak pada informasi yang tersimpan pada *block* dan algoritma yang dipakai pada pembentukan *Proof of Work.* Pada *block*

Ethereum, selain daripada transaksi, *state* terbaru juga akan disimpan. Sementara itu, algoritma *Proof of Work* yang digunakan pada Ethereum dinamakan *Ethash*.

Algoritma *Ethash* secara formal didefinisikan pada Persamaan 2.1.

$$(m, n) = \mathrm{PoW}(HN, Hn, \mathrm{d}) \qquad (2.1)$$

Pada Persamaan 2.1, ***m*** merupakan *mixHash*, ***n*** adalah *nonce*, ***HN*** diartikan sebagai *block header* dari *block* baru yang terbentuk (tanpa komponen *nonce* dan *mixHash*), ***Hn*** sebagai *nonce* dari *block header*, serta **d** yaitu DAG (*data set* besar). (Wood 2019)

Algoritma *Ethash* pada dasarnya akan mencari nilai *mixHash* dan *nonce* yang sesuai berdasarkan *difficulty* yang ditetapkan pada proses pembentukan *block*. Kedua nilai ini merupakan bukti bahwa suatu pembentukan *block* telah melalui proses komputasi yang besar (*Proof of Work*).