BAB II

TINJAUAN PUSTAKA

Dalam BAB ini berisi berbagai konsep dasar dan teori-teori yang berkaitan dengan pembangunan APLIKASI E-TRANSKRIP BERBASIS TEKNOLOGI BLOCKCHAIN dan IPFS.

2.1 Profil SMK BPI Bandung

SMK BPI Bandung adalah sebuah sekolah kejuruan yang dibawahi Yayasan Badan Perguruan Indonesia. Sekolah Menegah Kejuruan BPI Bandung adalah salah satu Sekolah berbasis Teknologi yang mempunyai 3 Program Studi Unggulan Ter-Akreditasi A. Sekolah yang mengedepankan Pendidikan dan Akhlak Mulia Berbasis Penilaian Holistik, menjadikan peserta didik SMK BPI Bandung Bermartabat, Berkualitas, dan Terpercaya.

Nama Sekolah	:	SMK BPI BANDUNG
Alamat Sekolah	:	Jl. Burangrang No.8 Bandung
Alamat Email	:	info@smkbpi.sch.id
Alamat Website	:	www.smkbpi.sch.id

Sekolah yang mempunyai letak strategis pada pusat Kota Bandung, yang menjadikan mobilitas Sekolah Menengah Kejuruan BPI Bandung menjadi mudah diakses. Dan Di lengkapi pula dengan pendidik yang berkompeten dan ahli pada setiap Program Studinya.

Program Studi pada SMK BPI Bandung antara lain :

1) Otomatisasi dan Tata Kelola Perkantoran (OTKP).
2) Rekayasa Perangkat Lunak (RPL).
3) Teknik Komputer Jaringan (TKJ)

2.1.1 Logo Sekolah

Logo merupakan ciri khas atau karakter yang mencerminkan suatu sekolah. SMK BPI BANDUNG memiliki logo yang sama dengan Yayasan Badan Perguruan Indonesia yang dapat dilihat pada gambar di bawah.

Gambar 2.1. Logo Yayasan Badan Perguruan Indonesia

2.1.2 Visi dan Misi SMK BPI

Sekolah SMK BPI Bandung memiliki visi dan misi tersendiri untuk mewujudkan Sekolah yang Bermartabat, Berkualitas dan Terpercaya.

1. **Visi**

   Menjadikan penyelenggara pendidikan berkualitas dan terpercaya.

2. **Misi**

SMK BPI juga memiliki beberapa misi yang ingin di wujudkan kedapannya antara lain sebagai berikut:

1) Mewujudkan tata kelola, sistem pengendalian manajemen, dan sistem. Pengawasan internal yang modern, efektif, dan efesien
2) Menyalurkan dan Mendukung kreativitas peserta didik dengan sarana dan prasarana yang lengkap.
3) Mewujudkan budaya religi, jujur, disiplin, beretika, berestetika, pekerja keras, kreatif, inovatif, komptetitif, dan berkualitas.
4) Mewujudkan dinamisasi peningkatan kualitas pendidikan berkarakter yang berkesinambungan dan berkelanjutan.

5) Mewujudkan produk kompetensi keahlian bernilai Jual Pasar Global.
6) Memperluas akses kemitraan dunia kerja yang menjamin lapangan kerja dan prakerin bagi peserta didik dan lulusan SMK BPI.
7) Mewujudkan lulusan yang handal di bidangnya dan fasih berbahasa Inggris sehingga dipercaya oleh segenap dunia kerja pemerintah maupun swasata.
8) Mewujudkan jiwa entrepreneurship kuat yang mampu meningkatkan kualitas hidup civitas akademika SMK BPI Bandung.

2.2 Rapor

Fungsi pokok evaluasi hasil belajar siswa secara umum adalah untuk mengukur tingkat kemajuan siswa dalam belajar, untuk menyusun rencana bealajar selanjutnya dan untuk memperbaiki proses pembelajaran. Laporan evaluasi hasil belajar siswa dituliskan pada sebuah dokumen yaitu rapor. Nilai rapor ditulis berdasarkan hasil belajar siswa dalam satu semester dan ditulis pada akhir semester.

Nilai rapor merupakan hasil kumpulan nilai mata pelajaran dimiliki setiap siswa yang berisi laporan nilai selama satu semester. Rapor diterimakan sebagai tolak ukur dan untuk mengetahui perkembangan terhadap prestasi siswa setelah mengikuti proses pembelajaran.

Melalui rapor wali kelas dapat mengetahui kekuatan dan kelemahan siswa dalam kelas yang diampunya wali kelas dapat menentukan strategi dalam pengelolaan kelas yang menjadi tanggung jawabnya misalnya dengan menata strategis belajar untuk membantu siswa meningkatkan kompetensi siswa atau membantu mengatasi kesulitan belajar siswa yang lemah.

2.3 Transkrip Nilai

Transkrip berdasarkan KBBI [16], memiliki arti salin. Yang artinya transkrip merukapan suatu salinan dokumen tertentu. Transkrip nilai adalah kumpulan nilai dari semua mata pelajaran mulai semester 1 hingga semester terakhir dari SMA/SMK/Sederajat atau Perguruan Tinggi[17]. Transkrip nilai berbeda dengan rapor. Rapor biasanya terdiri dari beberapa lembar kertas, sedangkan Transkrip nilai biasanya hanya berbentuk satu lembar saja. Transkrip nilai juga berbeda dengan ijazah pada jenjang sekolah menengah, karena transkrip berisi nilai keseluruhan dari semester awal hingga akhir, sedangkan ijazah hanya berupa nilai akhir rekapitulasi nilai rapor dan nilai ujian nasional. transkrip nilai biasanya sering digunakan sebagai salah satu syarat pendaftaran beasiswa hingga syarat untuk pelamaran pekerjaan[18].

2.4 Aplikasi Web

Aplikasi Web (Web app) adalah program aplikasi yang disimpan di server jarak jauh dan dikirimkan melalui Internet melalui antarmuka browser. Aplikasi web dapat dirancang untuk berbagai kegunaan dan dapat digunakan oleh siapa saja dari organisasi ke individu karena berbagai alasan [19]. Aplikasi Web yang umum digunakan dapat mencakup webmail, kalkulator online, atau toko *e-commerce*. Beberapa aplikasi Web hanya dapat diakses oleh browser tertentu. namun, sebagian besar dapat diakses dengan browser apapun.

Menurut Educhannel.id [20], ada beberapa keuntungan dan kemudahan jika menggunakan aplikasi berbasis web yaitu:

1. Bisa diakses dari mana saja tanpa perlu menginstal karena aplikasi telah terpasang di server.
2. Multi platform atau bisa digunakan pada sistem operasi apapun baik menggunakan sistem operasi Linux, Windows atau Mac OS, yang terpenting pada komputer tersebut telah terpasang web browser dan terhubung ke internet.

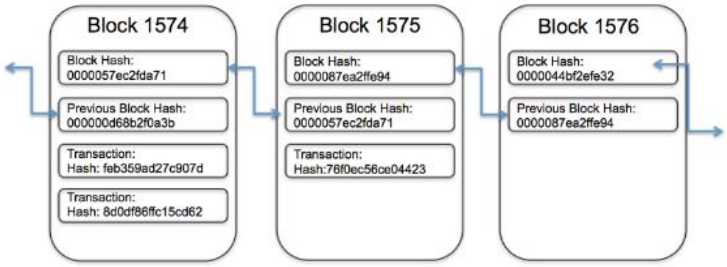
3. Terkait dengan isu lisensi (hak cipta), telah menjadi tanggung jawab dari penyedia aplikasi web sehingga pengguna tidak memerlukan lagi.
4. Dapat diakses melalui banyak media seperti : computer, tab dan handphone yang sudah sesuai dengan standar WAP.

2.5 UML (Unified Modelling Language)

Unified Modeling Language (UML) merupakan kumpulan struktur ataupun teknik yang digunakan untuk memodelkan desain program berorientasi objek (OOP) [21]. Unified Modeling Language (UML) juga digunakan untuk mengembangkan sistem dalam rekayasa perangkat lunak, yang merupakan bahasa visual untuk mendefinisikan dan mendokumentasikan suatu sistem. Persyaratan dalam skenario yang mengungkapkan bagaimana pengguna menggunakan sistem ditunjukkan dengan UML. Kendala dari suatu sistem juga ditunjukkan dengan UML [22]. Oleh karena itu, banyak peneliti yang bekerja sebagai insinyur perangkat lunak menerbitkan makalah tentang bagaimana diagram UML digunakan untuk mengembangkan sistem dan berkontribusi pada praktik untuk memajukan disiplin rekayasa perangkat lunak.

2.6 Blockchain

Blockchain merupakan struktur informasi permanen, yang dibentuk oleh blok-blok data yang saling terhubung dengan blok data transaksi sebelum maupun setelahnya [23]. Setiap data transaksi yang tersimpan pada setiap blok akan dienkripsi menggunakan algoritma kriptografi asimetris agar data yang tersimpan pada setiap blok terjamin keamanannya saat melakukan transmisi dan akses data.



Gambar 2.2. Ilustrasi Blockchain

Menurut Oracle ada 3 tipe blockchain yaitu *Public blockchain*, *Permissioned or private blockchain* dan *Federated or consortium blockchain* [24]. *Public blockchain* merupakan sebuah jaringan blockchain yang di mana siapa pun dapat berpartisipasi tanpa batasan. *Permissioned or private blockchain* adalah jaringan blockchain yang hanya pengguna dengan izin saja yang dapat mengakses kumpulan data tertentu pada blockchain tersebut. *Federated or consortium blockchain* merupakan Jaringan blockchain di mana proses konsensus (proses penambangan) dikontrol secara ketat oleh kumpulan node yang telah dipilih sebelumnya atau oleh sejumlah pemangku kepentingan yang telah dipilih sebelumnya.

2.7 Smart Contract

Blockchain 2.0. merupakan perkembangan dari teknologi Blockchain dimana penerapan teknologi blockchain lebih luas dengan menggunakan mekanisme baru yang di sebut sebagai smart contract. *Smart contract* adalah suatu kontrak yang dibuat secara khusus dengan tujuan untuk menjalankan atau mengeksekusi serangkaian perintah-perintah pada blockchain .Istilah "*smart contract*" awalnya diciptakan oleh Nick Szabo pada tahun 1990-an [25]. Dia menyarankan untuk menerjemahkan ketentuan ketentuan kontrak ke dalam kode dan memasukkannya ke dalam perangkat lunak atau perangkat keras untuk membuatnya dapat berjalan sendiri, untuk meminimalkan biaya kontrak antara pihak-pihak yang bertransaksi dan untuk menghindari tindakan jahat selama pelaksanaan kontrak.

2.8 Solidity

Solidity adalah sebuah bahasa pemrograman. Solidity adalah bahasa pemrograman yang khusus untuk Smart Contract. Cardano menggunakan Solidity untuk smart contract nya. Solidity dapat berjalan pada IELE compiler yang dimiliki

oleh Cardano jika Anda ingin mencoba membuat Smart Contract. Bahasa pemrograman Solidity mirip dengan javascript. Mirip karena pada javascript terdapat class, class yang terdapat pada soldity disebut contract. Syntax dan function nya pun banyak kemiripan dengan javascript [26].

Solidity ditulis dengan format file .sol. Solidity bukanlah bahasa yang dieksekusi pada Blockchain Virtual Machine. Tetapi solidity adalah bahasa yang bertujuan untuk mempermudah kita membuat smart contract. Saat akan dicompile ataupun dideploy smart contract, kita membutuhkan yang namanya Solidity Compiler. Dengan menggunakan solidity compiler tersebut maka smart contract yang telah kita buat akan di compile ke dalam bytecode yang nantinya bytecode tersebut lah yang akan dieksekusi oleh virtual machine.

2.9 Konsensus

Dalam aplikasi blockchain, kita perlu menyelesaikan dua masalah yaitu pengeluaran ganda dan *Byzantine Generals Problem*. Masalah pengeluaran ganda berarti menggunakan kembali mata uang dalam dua transaksi sekaligus. Mata uang tradisional adalah entitas, jadi kami tidak akan menghadapi masalah pengeluaran ganda saat menggunakan mata uang tradisional. masalah pengeluaran ganda dalam transaksi Internet dapat di selesaikan dengan lembaga terpercaya yang terpusat [27]. Blockchain memecahkan masalah ini dengan metode verifikasi transaksi oleh banyak node terdistribusi secara bersamaan.

Byzantine Generals Problem adalah masalah pada sistem terdistribusi [28]. Data dapat dikirimkan antara node yang berbeda melalui komunikasi peer-to-peer. Namun, beberapa node mungkin diserang, yang akan menyebabkan perubahan konten komunikasi. Node normal perlu membedakan informasi yang telah diubah dan memperoleh hasil yang konsisten dengan node normal lainnya. Ini juga membutuhkan desain dari algoritma konsensus yang sesuai. Algoritma konsensus telah dipelajari selama bertahun-tahun dalam sistem terdistribusi. Ada beberapa algoritma konsensus yang sering diterapkan di blockchain.

2.9.1. Proof of Work (POW)

PoW (*Proof of Work*) adalah algoritma konsensus yang digunakan dalam Jaringan Bitcoin [29]. Pada jaringan terdesentralisasi, seseorang harus dipilih untuk mencatat transaksi. Cara termudah adalah pemilihan acak. Namun, pemilihan acak rentan terhadap serangan. Jadi jika sebuah node ingin mempublikasikan blok transaksi, banyak pekerjaan yang harus dilakukan untuk membuktikan bahwa node tersebut tidak mungkin menyerang jaringan.

Pada algoritma konsensus *Proof of Work* (PoW), setiap node jaringan menghitung nilai hash dari header blok. Header blok berisi nonce dan penambang akan sering mengubah nonce untuk mendapatkan nilai hash yang berbeda[30]. Konsensus mensyaratkan bahwa nilai yang dihitung harus sama dengan atau lebih kecil dari nilai tertentu yang diberikan. Ketika satu node mencapai nilai target, itu akan menyiarkan blok ke node lain dan semua node lainnya harus saling mengkonfirmasi kebenaran nilai hash. Jika blok divalidasi, penambang lain akan menambahkan blok baru ini ke blockchain mereka sendiri. Node yang menghitung nilai hash disebut penambang dan prosedur PoW disebut menambang di Bitcoin.

2.9.2. Proof of Stake (POS)

PoS (Proof of stake) adalah algoritma konsensus alternatif hemat energi untuk PoW. Penambang di PoS harus membuktikan kepemilikan sejumlah mata uang. Diyakini bahwa orang dengan lebih banyak mata uang akan lebih kecil kemungkinannya untuk menyerang jaringan. Pemilihan berdasarkan saldo akun cukup tidak adil karena satu-satunya orang terkaya pasti akan mendominasi jaringan. Akibatnya, banyak solusi yang diusulkan dengan kombinasi ukuran stake untuk memutuskan blok mana yang akan ditempa berikutnya. Secara khusus, Blackcoin [31] menggunakan pengacakan untuk memprediksi generator berikutnya. Ini menggunakan formula yang mencari nilai hash terendah dalam kombinasi dengan ukuran pasak. Peercoin [32] menyukai pemilihan berdasarkan usia koin. Di Peercoin, set koin yang lebih tua dan lebih besar memiliki kemungkinan lebih besar untuk menambang blok berikutnya. Dibandingkan dengan PoW, PoS lebih hemat energi dan lebih efektif. Sayangnya, karena biaya

penambangan hampir nol, serangan mungkin datang sebagai konsekuensinya. Banyak blockchain mengadopsi PoW di awal dan berubah menjadi PoS secara bertahap. Misalnya, ethereum berencana untuk berpindah dari Ethash (sejenis PoW) [33] ke Casper (semacam PoS) .

2.9.3. Practical Byzantine Fault Tolerance (PBFT)

Dalam sistem terdistribusi, Toleransi Kesalahan Bizantium dapat menjadi metode yang baik untuk memecahkan kesalahan transmisi. Tetapi sistem Bizantium awal membutuhkan operasi eksponensial. Sampai tahun 1999, sistem PBFT (Practical Byzantine Fault Tolerance) [34] diusulkan dan kompleksitas algoritma dikurangi ke tingkat polinomial, yang sangat meningkatkan efisiensi. Proses PBFT terdiri dari lima tahapan yaitu:

1) *Request*: Klien mengirimkan permintaan ke server master node, node master memberikan permintaan cap waktu.
2) *Pre-prepare*: Node server master merekam meminta pesan dan memberikan nomor pesanan. Kemudian node master menyiarkan pesan pra-persiapan ke node server berikutnya. Node server lain awalnya menentukan apakah akan menerima permintaan atau tidak.
3) *Prepare*: Jika node server memilih untuk menerima permintaan, itu menyiarkan pesan persiapan ke semua node server lain dan menerima pesan persiapan dari node lain. Setelah mengumpulkan pesan 2f+1, jika mayoritas node memilih untuk menerima permintaan, maka itu akan memasuki kondisi komit.
4) *Commit*: Setiap node dalam keadaan komit mengirimkan pesan komit ke semua node lain di server. Pada saat yang sama, jika node server menerima pesan komit 2f+1, diyakini bahwa sebagian besar node mencapai konsensus untuk menerima permintaan tersebut. Kemudian node mengeksekusi instruksi dalam pesan permintaan.
5) *Reply*: node server membalas klien. Jika klien tidak menerima balasan karena penundaan jaringan, permintaan dikirim ulang ke node server. Jika permintaan telah dieksekusi, node server hanya perlu mengirim pesan balasan berulang kali.

2.9.4. Delegated Proof of Stake (DPOS)

Perbedaan utama antara PoS dan DPOS adalah PoS melakukan demokrasi langsung sedangkan DPOS adalah demokrasi perwakilan[35].Pada tahap desain awal bitcoin, Satoshi Nakamoto berharap semua peserta dapat menggunakan CPU untuk menambang. Jadi kekuatan hashing dapat mencocokkan node dan setiap node memiliki kesempatan untuk berpartisipasi dalam pengambilan keputusan blockchain. Dengan perkembangan teknologi dan apresiasi bitcoin, mesin yang dirancang khusus untuk penambangan ditemukan. Kekuatan hashing dikelompokkan dalam peserta yang memiliki mesin penambangan dalam jumlah besar[36]. Penambang biasa jarang memiliki kesempatan untuk membuat blok.

BitShares adalah contoh blockchain yang menggunakan algoritma konsensus DPoS [37]. Di blockchain dengan DPoS, setiap node dapat memilih saksi berdasarkan stakenya. Di seluruh jaringan, N saksi teratas yang telah berpartisipasi dalam kampanye dan mendapat suara terbanyak memiliki hak akuntansi. Jumlah N saksi ditentukan sedemikian rupa sehingga setidaknya 50% pemangku kepentingan pemungutan suara percaya ada desentralisasi yang memadai .Saksi terpilih membuat blok baru satu per satu sesuai tugas dan mendapatkan beberapa hadiah. Saksi perlu memastikan waktu online yang memadai. Jika saksi tidak dapat membuat blok yang ditugaskan, aktivitas blok tersebut akan dipindahkan ke blok berikutnya dan pemangku kepentingan akan memilih saksi baru untuk menggantikannya. Blockchain menggunakan DPoS lebih efisien dan hemat daya daripada PoW dan PoS [27].

2.10 Metamask

Metamask merupakan dompet cryptocurrency yang dapat digunakan di browser Chrome, Firefox dan Brave. Metamask juga merupakan ekstensi browser. Yang berarti bahwa Metamask bekerja seperti jembatan antara browser normal dan blockchain Ethereum [38].

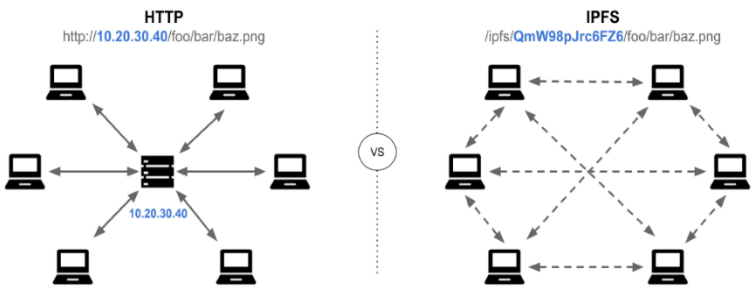
Blockchain Ethereum merupakan jaringan tempat para pengguna dapat membangun aplikasi mereka sendiri yang disebut dApps dan cryptocurrency.

Ethereum juga memungkinkan penggunanya untuk menulis pedoman transaksi yang disebut smart contract atau kontrak pintar.

Cryptocurrency atau mata uang kripto jaringan *blockchain* Ethereum disebut Ether. Mata uang kripto lain yang dibangun diatas jaringan blockchain Ethereum biasa disebut token. Sebagian besar token-token yang dibangun di jaringan blockchain Ethereum disebut dengan token ERC20 karena token-token yang dibangun mengikuti aturan yang telah ditetapkan oleh pengembang Ethereum untuk membuat cryptocurrency baru pada jaringan Ethereum.

2.11 Interplanetary File System (IPFS)

IPFS Merupakan sistem peer-to-peer seperti perangkat lunak berbagi P2P [39] menggunakan hash konten untuk mengatasinya (Lihat Gambar 2.3). Teknologi lain seperti Git menggunakan struktur kompleks Merkle-linked . IPFS mengintegrasikan penggunaan struktur terkait Merkle yang kompleks dengan kemampuan pengalamatan data dari sistem berbagi file P2P. Konten didistribusikan melalui jaringan peer-to-peer.



Gambar 2.3. HTTP vs IPFS

Protokol HTTP klasik yang digunakan di web seperti yang terlihat pada Gambar 2.3 menggunakan alamat lokasi , mengandalkan arsitektur terpusat di mana pengguna terhubung ke server pusat (lokasi) yang menyediakan file. Sebaliknya, IPFS menggunakan alamat konten, di mana pengguna dapat mengambil file yang diidentifikasi secara unik dari setiap node dalam jaringan terdistribusi yang menyimpan file tersebut[40].

Menggunakan IPFS tidak hanya memungkinkan untuk mengakses file pada halaman web namun juga berbagai file yang disimpan pada komputer dalam bentuk dokumen, email, atau bahkan rekaman database. Sehingga dalam konsepnya terdapat tiga prinsip fundamental yang digunakan oleh IPFS :

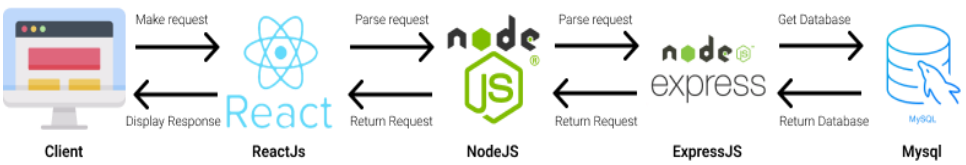
1. Identifikasi yang unik melalui content adressing
2. Menghubungkan konten melalui directed acyclic graphs (DAGs)
3. Menemukan konten melalui distributed hash tabels (DHTs)

2.12 Truffle Suite

Truffle suite merupakan framework paling simple dan mudah di mengerti untuk pemula mempelajari dan membangun *Decentralized application* (DApp) [41]. *Decentralized application* atau DApp adalah sebuah platform atau perangkat atau tools yang dapat menghubungkan antar pengguna dalam bertransaksi secara P2P, tanpa melibatkan perantara, open source, dan bersifat publik, serta otoritas berada pada masing-masing pengguna. Framework Truffle suite terdiri dari tiga sistem atau aplikasi yaitu Truffle, Gananche dan Drizzle. Yang penulis gunakan pada penelitian ini hanya dua yaitu Truffle dan Gananche. Truffle berfungsi sebagai *compailer* dari smart contract yang di buat menggunakan bahasa solidity. Gananche merupakan personal ethereum blockchain yang di sediakan oleh framework Truffle Suite untuk mempermudah integrasi sistem.

2.13 MERN Stack

Mern Stack merupakan sekumpulan teknologi atau gaya koding untuk membangun aplikasi website. Mern stack memiliki 2 versi, yaitu versi yang menggunakan Mysql atau versi yang menggunakan Monggo DB sebagai database utama yang di gunakan dalam membangun aplikasi website. Yang penulis gunakan untuk penelitian ini yaitu Mern stack versi Mysql oleh karena itu singatan MERN disini merujuk pada MYSQL,Express,React dan Node js.



Gambar 2.4. MERN Stack

MERN Stack sangat populer karena bahasa yang digunakan untuk membangun aplikasi menggunakan satu bahasa yaitu javascript selain itu MERN stack juga menerapkan konsep SPA (Single Page Aplication). Menurut Mesbah Ali, antarmuka web yang menerapkan konsep SPA terdiri dari komponen individual yang dapat diperbarui/diganti secara independen, sehingga seluruh halaman tidak perlu dimuat ulang pada setiap tindakan pengguna [42].