BAB I

PENDAHULUAN

1.1 Latar Belakang Penelitian

Perkembangan teknologi dewasa ini memberikan dampak yang begitu besar terhadap kehidupan masyarakat. Akses yang mudah, murah, dan cepat terhadap informasi bukanlah hal yang mahal lagi. Hal ini disebabkan karena jaringan internet yang kini semakin mudah dijangkau setiap lapisan masyarakat. Internet menjadi salah satu media transfer data yang paling sering digunakan dalam bertransaksi. Contohnya transaksi keuangan, pelaporan pajak, transaksi jual beli, dan lain sebagainya. Setiap transaksi tersebut akan menyimpan beberapa atau keseluruhan data pribadi setiap pihak yang terlibat. Data pribadi yang dimaksud seperti nama, tempat lahir, tanggal lahir, alamat, pekerjaan, dan lain sebagainya. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia nomor 20 tahun 2016 Bab I Ayat 1 menjelaskan data pribadi merupakan data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Data perseorangan tertentu adalah setiap keterangan yang benar dan nyata yang melekat dan dapat diidentifikasi, baik langsung maupun tidak langsung, pada masing-masing individu yang pemanfaatannya sesuai ketentuan peraturan perundang-undangan. Undang-undang Republik Indonesia Nomor 19 Tahun 2016 Bab I Pasal 1 Ayat 2 menjelaskan bahwa transaksi elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya.

Di Indonesia, KTP / E-KTP memuat identitas yang berisikan data pribadi yang digunakan syarat administrasi seperti pembukaan rekening Bank, pengajuan kredit, pembayaran pajak, pelayanan Kesehatan, dan lain sebagainya. Teknologi yang terdapat dalam E-KTP yaitu sebuah chip berbasis mikroprosessor dengan besaran memory 8 *kilobytes* (Suryani, Rahayu and Ardiningsih, 2014). Fungsi dari chip E-KTP adalah untuk menyimpan data biodata pemilik (nama, tempat, tgl. lahir, alamat dan lain-lain), tanda tangan, pas foto dan dua data sidik jari (Indarto, 2013). Chip pada KTP elektronik hanya bisa dibaca oleh perangkat pembaca tertentu untuk menjamin keamanan data. Pada praktiknya, ada tiga cara untuk verifikasi data e-KTP, yakni menggunakan NIK, akses biometrik berupa foto dan sidik jari, serta alat baca *card reader*. Namun ternyata tak semua lembaga-lembaga menggunakan verifikasi dengan card reader, sehingga tak jarang tetap harus melakukan fotokopi KTP (Aida, 2021). Kurangnya *card reader* di berbagai lembaga membuat duplikasi KTP dengan fotocopy masih terjadi. Disamping itu kemajuan teknologi membuat pendaftaran berbagai platform digital dengan cara memfoto KTP sering dilakukan. Hal ini akan dijadikan celah untuk melakukan penipuan atau pemalsuan identitas. Menurut situs *scamwatch* (Australian Competition & Consumer Commission) beberapa hal yang dilakukan penipu terhadap data pribadi adalah mengakses dan menguras rekening bank, buka rekening bank baru dan ambil pinjaman atau kredit, beli barang mahal, dan lain sebagainya. Adapun teknik yang digunakan dalam mencuri data pribadi adalah *hacking*, peretasan, penipuan jarak jauh, *malware & ransomware*, profil online palsu, pencurian dokumen, dan kebocoran data. Data iii.org (*Facts + Statistics: Identity theft and cybercrime | III*) menyebutkan kasus penipuan pinjaman kredit

menggunakan data pribadi berada diposisi ke-4 dengan jumlah 99.667 laporan telah terjadi di Amerika tahun 2020. *FTC Consumer Sentinel Network* melaporkan penipuan pinjaman di bank dari tahun 2017 kian mengalami peningkatan hingga tahun 2020. Namun di Indonesia sendiri jika melihat statistik kriminal BPS tahun 2020 terdapat sejumlah 54.115 kejadian penipuan, penggelapan, korupsi yang terjadi pada tahun 2015 telah menurun menjadi 39.320 kejadian ditahun 2019. Jumlah ini harus diturunkan lagi untuk menghindari kerugian yang diterima masyarakat.

Dalam RUU Perlindungan Data Pribadi (PDP) (Kominfo, 2015) yang diusulkan memuat ketentuan penggunaan bagaimana data pribadi harus diproses, digunakan, dan dilindungi termasuk pidana atas pelanggaran yang dilakukan oleh perorangan maupun korporasi. Ada berbagai kasus penyalahgunaan data pribadi yang merugikan pemiliknya, diantaranya pada bulan Januari 2018 telah ditangkap pemalsu KTP, Kartu Keluarga, dan Surat Tanah untuk Pinjaman Bank di Jawa Timur (Pradhitya Fauzi, 2018). Setelah dilakukan pengecekan pihak bank, diketahui bahwa kelengkapan pengajuan kredit tersebut palsu dan pelaku berhasil diamankan pihak berwajib. Kasus selanjutnya merupakan kasus penipuan identitas diri di Jakarta. Menurut sumber kompas.com (Aprillia, 2018), pemalsu memalsukan data pribadi seseorang untuk mengajukan pinjaman ke bank guna membeli sejumlah mobil secara kredit. Korban baru tahu identitasnya telah dipalsukan dan disalahgunakan, ketika si pemalsu hendak membeli mobil ketiga yaitu Toyota Fortuner. Bagi instansi keuangan, dalam hal ini bank, akan sangat dirugikan serta berdampak buruk bagi kelancaran kegiatan perbankan karena akan menurunkan kepercayaan dari nasabah.

Singh dkk (2018) membahas mengenai kelayakan teknologi *Smart Card* sebagai solusi identitas dan kemampuannya untuk melakukan berbagai fungsi dengan kontrol akses yang kuat. *Smart card* memungkinkan menggabungkan berbagai jenis kartu seperti kartu tempat makan, kartu perpustakaan, surat izin mengemudi, dan lain sebagainya. Akses data pada smart card mirip dengan E-KTP yaitu dengan melakukan kontak pada *card reader*, namun smart card memiliki fitur keamanan seperti PIN untuk menjaga kerahasiaan data. Setiap data yang ditransaksikan dilakukan proses enkripsi dan data disimpan dalam suatu server. Penggunaan *smart card* yang mengenkripsi data dan menggunakan PIN untuk authentikasi menjadikannya alternatif baik dalam setiap transaksi menggunakan data pribadi. Mirip seperti penelitian Singh dkk, Datta dkk (2020) mengusulkan arsitektur baru yang mengintegrasikan *blockchain* sebagai elemen utama dalam smart card. Tujuannya yaitu memastikan keamanan, privasi, dan integritas data untuk sistem manajemen *smart national identity card* di Bangladesh. Dalam arsitekturnya, sistem dibagi menjadi tiga bagian, yaitu *central station, sub-station,* dan *rural station*. Ketiga stasiun ini saling terhubung menggunakan mekanisme server terdistribusi. C*entral station* ditempatkan di ibu kota negara. S*ub-station* akan ditempatkan di setiap distrik. Terakhir, *rural station* akan ditempatkan di daerah-daerah terpencil. Data warga akan dikumpulkan dan dikirimkan menggunakan *rural station* selanjutnya dibawa ke S*ub-station*. Pemilihan *blockchain* bertujuan untuk membuat model dapat diperluas dari waktu ke waktu. Fleksibilitas akan muncul pada *rural station* dan *sub-stations* untuk meningkatkan keamanan, dan efisiensi transaksi. Selain itu, sifat terdistribusi dari buku besar memberikan perlindungan dari kehilangan data jika terjadi kegagalan

node. Jika ada kegagalan operasi suatu *node*, sistem tidak akan berhenti beroperasi karena menggunakan database *blockchain* yang terdistribusi. Penelitian oleh Bae dan Kim (Bae and Kim, 2010) menggunakan PIP *(Personal Information Protect Model)* untuk melindungi data pribadi dalam pendaftaran suatu layanan. Pengguna yang memiliki informasi mengontrol informasi pribadinya dengan mengatur kebijakan privasinya sendiri. Ketika pengguna perlu menerima layanan yang membutuhkan informasi pribadi, dia akan menyetujui informasi pribadi apa yang dirilis untuk menerima layanan tersebut. Penyedia layanan hanya dapat menyediakan layanan jika kebijakan layanan pengguna dan penyedia sesuai.

Perkembangan teknologi kriptografi telah menuju babak baru semenjak *bitcoin* muncul sebagai mata uang digital yang memanfaatkan teknologi *blockchain*. Teknologi *blockchain* diperkenalkan pertama kali oleh Satoshi Nakamato dan menawarkan teknologi untuk berbagi informasi yang aman. *Blockchain* adalah basis data terdistribusi yang terdiri dari catatan transaksi yang dibagi di antara pihak yang berpartisipasi (Zhao, Fan and Yan, 2016). Setiap transaksi diverifikasi oleh mayoritas konsensus yang berpartisipasi dalam sistem, dengan tujuan membuat transaksi palsu tidak dapat diproses. Rivera dkk (Rivera *et al.*, 2017) melakukan penelitian *systematic mapping review* dengan tujuan mengumpulkan semua penelitian relevan yang ada tentang *Digital Identity* pada teknologi *Blockchain* untuk diimplementasikan di lingkungan *smart city*. Hasilnya menyimpulkan teknologi *blockchain* membuat banyak proses dan layanan transaksi lebih transparan, terdesentralisasi, demokratis, dan aman tanpa perlu organisasi pihak ketiga di tengah. Pengimplementasian identitas digital pada *blockchain* menjadi sangat penting dalam waktu dekat untuk mengotentikasi

warga dan membuktikan identitas mereka untuk sekelompok layanan digital yang saat ini ada di dunia yang saling terhubung ini. Kelebihan utama *blockchain* yaitu memastikan agar seluruh data yang tersimpan tidak bisa diubah, namun data dapat bertambah seiring dengan jumlah transaksi oleh berbagai pihak.

Ethereum merupakan salah satu *crypto currency* yang merepresentasikan *blockchain* dengan menyediakan lapisan abstrak yang memungkinkan siapa pun untuk membuat aturan (kontrak) mereka sendiri untuk kepemilikan, format transaksi, dan fungsi transisi. Kelebihan Ethereum dibandingkan *crypto currency* lainnya adalah fitur *smart contract* yang merupakan seperangkat aturan kriptografi yang dijalankan hanya jika kondisi tertentu terpenuhi (Buterin, 2013).

Beranjak dari permasalahan penyalahgunaan data pribadi yang merugikan masyarakat maupun pihak perbankan, penelitian ini mengusulkan pengembangkan sistem transaksi data pribadi menggunakan *smart contract* Ethereum yang memungkinkan pengguna untuk mengatur informasi pribadinya dan kebijakan perlindungan privasi untuk menerima layanan yang disediakan oleh penyedia layanan tanpa harus mengungkapkan informasi pribadi yang tidak diperlukan. Transaksi data pribadi yang dimaksud dalam penelitian ini adalah dimana seseorang atau pemilik data pribadi mengirimkan satu atau keseluruhan bagian data pribadinya kepada pihak lainnya. Bagian dari data pribadi yang dimaksud seperti nama, tempat lahir, alamat, pekerjaan, dan lain sebagainya.

Bank sebagai pengelola dana yang sudah terhimpun dari masyarakat atau disebut juga dana pihak ketiga (Wijaya, 2018), dimana dana yang dihimpun juga disalurkan kembali dalam bentuk kredit. Maka bank harus melakukan analisa dan mererapkan prinsip kehati-hatian sesuai dengan Peraturan Otoritas Jasa Keuangan

Nomor 42/POJK.03/2017 (OJK, 2017). Aktivitas perbankan sangat diatur oleh pemerintah dikarenakan apabila perbankan salah mengelola dana tersebut, maka banyak sekali masyarakat yang akan dirugikan. Pemilihan pengajuan kredit dalam penelitian ini didasari oleh masalah penipuan dan pemalsuan identitas yang kerap terjadi di beberapa tempat. Resiko yang dihadapi bank besar karena menghimpun dana masyarakat, jika banyak kredit yang bermasalah. Berdasarkan latar belakang tersebut dipilihlan studi kasus pengajuan permohonan kredit di Bank untuk mencegah terjadinya penipuan atau penyalahgunaan data pribadi dalam pengajuan kredit. Hasil akhir penelitian ini berupa analisis sistem dari kebutuhan fungsional, keamanan data, dan biaya.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah dijabarkan sebelumnya, maka dapat diidentifikasi permasalahan-permasalahan yang terjadi sehubungan dengan penggunaan data pribadi dalam pengajuan kredit, diantaranya:

1. Data pribadi masih rentan disalahgunakan oleh pihak yang tidak berwenang karena proses duplikasi yang mudah.
2. Pemilik data pribadi tidak tahu jika data pribadi mereka digunakan dalam administrasi perbankan seperti pembukaan rekening maupun pengajuan kredit.
3. Penggunaan card reader untuk membaca chip E-KTP di Indonesia masih jarang ditemui, yang mengakibatkan munculnya penyalahgunaan E-KTP.

1.3 Batasan Masalah

Batasan dalam penelitian ini adalah sebagai berikut:

1. Data pribadi yang dimaksud adalah data pribadi individu.
2. Data pribadi yang dikembangkan pada penelitian ini, menyesuaikan dengan kebutuhan data yang digunakan dalam pengajuan kredit di bank secara umum.
3. Pengujian transaksi data pribadi dilakukan dalam lingkungan lab / pengujian lokal.
4. Studi kasus yang digunakan adalah permohonan pengajuan kredit usaha mikro perorangan di bank umum dengan jumlah suami/istri 1 (satu).

1.4 Rumusan Masalah

Berdasarkan uraian latar belakang yang telah dijabarkan sebelumnya dapat dirumuskan beberapa permasalahan untuk dicari solusinya sebagai berikut:

1. Bagaimana rancangan sistem pada transaksi data pribadi menggunakan *Ethereum blockchain* dalam studi kasus pengajuan permohonan kredit di bank?
2. Bagaimana hasil pengujian sistem dan analisis dalam transaksi data pribadi dengan studi kasus pengajuan permohonan kredit di bank?
3. Bagaimana rekomendasi terhadap pemanfaatan *blockchain* dalam pengajuan permohonan kredit di bank?

1.5 Tujuan Penelitian

Adapun tujuan yang diharapkan dapat dicapai dari penelitian ini adalah sebagai berikut.

1. Untuk mengetahui rancangan sistem pada transaksi data pribadi dengan Ethereum *blockchain* untuk studi kasus pengajuan permohonan kredit di bank.
2. Untuk mengetahui hasil pengujian sistem dan analisis dalam transaksi data pribadi dengan studi kasus pengajuan permohonan kredit di bank.
3. Untuk mengetahui rekomendasi terhadap pemanfaatan *blockchain* dalam pengajuan permohonan kredit di bank.

1.6 Manfaat Penelitian

Manfaat teoritis dan praktis yang diperoleh dari penelitian ini adalah sebagai berikut:

1. Manfaat Teoritis

   Hasil penelitian ini secara teoritis diharapkan mampu menambah wawasan peneliti serta memberikan sumbangan pemikiran bagi pengembang sistem dengan *Ethereum blockchain*.

2. Manfaat Praktis

Dengan dilakukannya penelitian ini dapat memberikan rekomendasi pada pihak yang terkait, agar mampu memanfaatkan teknologi *blockchain* untuk menciptakan tunggalisasi data pribadi untuk mengurangi redundasi data, penipuan atau pemalsuan identitas serta memperkuat kepercayaan terhadap suatu data pribadi pada penyimpanan digital.