

BAB 2 LANDASAN TEORI

2.1 Polygon Blockchain

Blockchain merupakan *database* dari rekaman transaksi yang pernah terjadi lalu didistribusikan, validasi, dan dijaga oleh jaringan komputer yang ada di seluruh dunia [9]. Hal ini membuat teknologi *blockchain* tidak dapat diatur oleh suatu individu. Teknologi ini juga tidak rentan diretas dikarenakan data yang tersebar pada banyak komputer dan data yang terenkripsi dengan baik sehingga peretas tidak dapat mengganti maupun melihat isi dari data yang tersimpan pada *blockchain*. Proses validasi pada *blockchain* dapat dilakukan dengan beberapa cara, namun terdapat dua algoritma konsensus yang paling populer pada *blockchain* yaitu adalah *proof of work* dan *proof of stake* [10].

Ethereum merupakan platform *blockchain* terbesar yang memiliki sistem *smart contract* [11]. *Ethereum* merupakan salah satu platform yang pertama kali menerapkan *smart contract* pada sistem *blockchain*, hal ini membuat *Ethereum* memiliki kegunaan yang lain selain daripada menjadi mata uang untuk transaksi saja. Hingga saat ini *Ethereum* menjadi *blockchain* yang memiliki *smart contract* terbanyak pada platformnya. Untuk membuat *smart contract* pada *Ethereum* diperlukan sebuah bahasa pemrograman, oleh karena itu *Ethereum* membuat bahasa yang dikhususkan untuk membuat *smart contract* yaitu adalah *Solidity*. *Solidity* merupakan bahasa pemrograman yang paling populer untuk digunakan dalam pembuatan *smart contract* [12].

Polygon network merupakan jaringan *blockchain* yang berfokus dalam melakukan optimisasi terhadap jaringan *Ethereum* [13]. Polygon merupakan jaringan *blockchain* yang dapat menjalankan *Ethereum Virtual Machine* (EVM) sehingga seluruh jaringan *blockchain* yang menggunakan EVM dapat dijalankan diatas jaringan Polygon. Jaringan Polygon sendiri memiliki seluruh fitur yang dimiliki oleh *Ethereum* dan jaringan ini menyelesaikan permasalahan yang sedang terjadi pada *Ethereum* pada saat ini yaitu *gas fee* yang sangat tinggi sehingga menyebabkan sulit untuk melakukan *scalability* pada jaringan *Ethereum*. Polygon menggunakan konsensus *Proof of Stake* yang lebih hemat biaya dan lebih cepat dibandingkan dengan *Proof of Work* yang digunakan oleh *Ethereum*. Perbedaan konsensus yang ada pada Polygon dan *Ethereum* membuat perbedaan *transaction per sec-*

ond(tps) pada setiap jaringan Polygon memiliki dapat mengolah sekitar 7200 tps dan Ethereum hanya dapat mengolah sekitar 10 tps saja. Perbedaan konsensus ini juga tentunya memberikan perbedaan *gas fee* yang diperlukan, pada jaringan Polygon *gas fee* yang perlu dibayarkan setiap menambahkan data ke *blockchain* sangat rendah (dibawah 0.01 USD) sementara pada jaringan Ethereum *gas fee* dapat mencapai ratusan dollar.

2.2 Decentralized Application

Decentralized application merupakan sebuah *web application* yang berjalan di atas teknologi *blockchain* sehingga tidak memiliki sebuah server sentral [14]. Hal ini akan membuat tidak adanya *single point of failure* yang dapat terjadi pada media sosial yang akan dibangun di atas teknologi *blockchain*. *Decentralized application* sendiri biasanya dibuat menggunakan *smart contract* yang merupakan sebuah *set of rules* dari aplikasi yang dibuat dalam hal ini media sosial. Penggunaan sebuah *decentralized application* juga akan memerlukan *gas fee* yang telah ditetapkan oleh jaringan *blockchain* apabila ingin menambahkan sebuah data. Penggunaan *decentralized application* sendiri memerlukan para pengguna untuk memiliki *crypto wallet* milik mereka sendiri sebagai akun untuk mengakses sebuah *decentralized application*. *Decentralized application* sendiri dapat mencegah terjadinya pencurian konten yang sering terjadi pada platform *content sharing* [15]. Hal ini dapat mendukung media sosial yang tidak hanya dapat melindungi privasi para pengguna namun juga dapat menjaga hak cipta dari pos yang diberikan oleh pengguna.

2.3 Media sosial

Media sosial merupakan sebuah media untuk menyebarkan sebuah informasi antar masyarakat dan negara [16]. Media sosial menghubungkan para penggunanya dengan menggunakan internet, para pengguna akan berinteraksi dengan sebuah website yang telah disediakan oleh platform media sosial yang ingin digunakan. Para pengguna dapat menggunakan media sosial melalui sebuah laman web maupun aplikasi seluler yang dapat diunduh pada perangkat pengguna tersebut. Pada saat ini media sosial seperti *Facebook*, *Twitter*, dan *Instagram* berjalan diatas website yang disebut web 2.0 dimana web 2.0 sendiri memiliki kekurangan menurut [17] yaitu:

- *Loss of Democracy*

Hal ini terjadi dengan banyak pemilik atau perusahaan yang memiliki *Web 2.0* menggunakan otoritasnya untuk mengumpulkan data para pengguna dengan tujuan untuk mendapatkan keuntungan dengan cara melakukan *targeted ads*. Hal ini membuat para pengguna tidak memiliki kuasa terhadap data tentang mereka sendiri.

- *Censorship*

Banyak negara atau instansi yang ingin menggiring opini publik dengan melakukan sensor terhadap sebuah *post* yang memiliki arah yang berbeda dengan yang diinginkan pihak yang memiliki kuasa. Hal ini menyebabkan banyaknya informasi salah yang diberikan kepada publik dikarenakan unsur sensor yang dilakukan tersebut.

- *Bandwidth*

Penggunaan server yang diperlukan untuk menjalankan sebuah web membutuhkan biaya yang besar sehingga sangat sulit untuk melakukan *maintain* terhadap web yang sudah berjalan.

- *Security*

Keamanan pada *Web 2.0* yang menyebabkan kekhawatiran para pengguna, hal ini disebabkan oleh data yang disimpan pada server sehingga dapat menyebabkan *single point of failure* yang dimana ketika hacker berhasil masuk ke dalam server tersebut maka hacker tersebut dapat mengambil seluruh data yang ada pada server tersebut.

2.4 Performa Smart Contract

Smart contract merupakan sebuah program yang dijalankan diatas sebuah *blockchain*. Seluruh fungsi yang membutuhkan untuk menambah atau memperbarui data pada *blockchain* akan membutuhkan *transaction*. Performa *smart contract* sendiri dapat ditentukan berdasarkan *transaction* yang dilakukan oleh *smart contract*. Berdasarkan [18] sebuah objek *transaction* mengandung beberapa properti yaitu:

- *from*

Menunjukkan *address* yang memanggil transaksi.

- *to*
Menunjukkan *address* transaksi itu ditujukan.
- *gas limit*
Menunjukkan batas maksimal *gas* yang diperlukan.
- *max fee per gas*
Menunjukkan jumlah biaya yang dibayarkan per unit *gas*.
- *max priority fee*
Menunjukkan jumlah biaya lebih yang ingin dibayarkan akan mendapatkan prioritas.
- *nonce*
Menunjukkan jumlah transaksi yang pernah dilakukan oleh pembuat *transaction*.
- *value*
Menunjukkan jumlah *native currency* yang digunakan atau dikirimkan dalam *transaction* ini.

Semakin rumit sebuah fungsi yang akan dipanggil dari *smart contract* maka akan semakin besar juga *gas* yang diperlukan untuk menyelesaikan transaksi tersebut [18]. Jumlah *gas* yang diperlukan adalah tetap namun dapat berubah juga memiliki ukuran *input* data yang berbeda. Sementara *gas fee* dapat berubah tergantung *traffic* dari jaringan *blockchain* yang digunakan. Kecepatan sebuah *transaction* dilakukan juga tergantung dari *miner* yang mengerjakan *transaction* tersebut. Performa sebuah *smart contract* dapat diukur dengan cara mengetahui waktu yang dibutuhkan untuk sebuah transaksi serta *cost* yang harus dibayarkan [19]. *Cost* yang dibutuhkan sebuah transaksi terdiri dari *gas fee* serta *gas* yang diperlukan. Performa suatu jaringan *blockchain* untuk menjalankan fungsi dari *smart contract* bergantung terhadap kecepatan sebuah *block* di olah oleh *miner* dan *gas price* yang diberikan, namun evaluasi akan menggunakan harga standar atau sesuai dengan *market price* pada saat itu.