Sistem Pelaporan Pajak Pertambahan Nilai pada Web dengan Menggunakan Teknik Blockchain

Bhadrika Evandito Atmomintarso, dan Wirawan
Departemen Teknik Elektro, Institut Teknologi Sepuluh Nopember (ITS)
e-mail: wirawan@ee.its.ac.id

***Abstrak*—Blockchain merupakan sebuah teknologi baru yang sedang berkembang. Sifat blockchain terdesentralisasi digunakan pada jaringan untuk proses validasi data dan penyimpanan pada node. Teknologi ini menggunakan teknik kriptografi dan penggunaannya dimanfaatkan dalam bidang keuangan. Pada pemerintahan dapat diterapkan pada Faktur Pajak sebagai bukti telah dilakukan pungutan Pajak Pertambahan Nilai. Dengan blockchain diharapkan dapat mempermudah proses pembuatan dan validasi Faktur Pajak. Namun, dikarenakan pembayaran harus menggunakan Rupiah, pembuatan Faktur Pajak berupa kontrak pintar tidak dapat ditumpangkan pada jaringan blockchain yang sudah ada seperti mata uang kripto. Maka dari itu diperlukan perancangan blockchain yang sesuai untuk sistem pelaporan PPN di Indonesia. Jaringan blockchain perpajakan yang digunakan topologi mesh agar memiliki data dan sifat yang sama pada setiap node. Pembuatan *digital signature* pada e-Faktur (Faktur Pajak elektronik) sebagai kontrak pintar digunakan sebagai proses validasi Faktur Pajak. Kemudian Faktur Pajak dikirim dan disimpan pada blok baru berdasarkan tingkat kerumitan penambangan. Hasil dari Tugas Akhir ini berupa pembuatan e-Faktur pada browser dapat digunakan sebagai kontrak pintar yang divalidasikan pada node menggunakan pasangan kunci. Dalam pengujian disimpulkan bahwa tingkat kerumitan penambangan yang besar diperlukan waktu penambangan yang lebih lama. Maka dalam perancangan sistem setiap node harus memiliki konfigurasi yang sama agar lama waktu penambangan dan penambahan blok baru memiliki waktu yang sama.**

***Kata Kunci*—Blockchain, Kontrak Pintar, Penambangan, Pajak Pertambahan Nilai.**

I. PENDAHULUAN

SAAT ini perkembangan teknologi akan memasuki era revolusi industri 4.0. Apabila kesempatan ini dapat digunakan dengan baik, terutama oleh negara berkembang, dapat meningkatkan produktivitas, perekonomian, dan kesejahteraan rakyat. Perekonomian dan kesejahteraan rakyat dapat dipantau dalam arus perdagangan antara bisnis dan rekanannya dimana dapat menghasilkan tanda terima pajak bagi pemerintah. Sebagai salah satu sumber pendapatan terbesar untuk negara, sektor perpajakan harus bisa beradaptasi dengan apapun.

Jenis dari pajak yang perlu diperhatikan dari era revolusi industri 4.0 ini adalah pajak barang dan jasa atau pajak pertambahan nilai (PPN). Pajak jenis ini dapat memberikan kontribusi yang signifikan terhadap pendapatan negara karena dikumpulkan untuk kegiatan masyarakat dan bisnis. Berdasarkan Badan Pusat Statistik Indonesia, rasio penerimaan pajak cenderung menurun pada periode tahun 2013-2016 [1]. Rasio terbesar bernilai 4,24% pada tahun 2013 dan terendah 3,32% pada tahun 2016. Salah satu penyebab turunnya rasio PPN adalah kurangnya teknologi yang memadai dalam pencatatan secara maksimal. Sebagai permulaan era industri 4.0, pemerintah dapat mengembangkan teknologi digital sebagai administrasi PPN untuk mengatasi hal tersebut.

Salah satu teknologi digital yang berkembang adalah blockchain. Teknologi blockchain akan mencatat data pada sebuah blok dan mendistribusikan blok dalam jaringan blockchain. Ketika pencatatan selesai dan telah ditambahkan dalam blok baru, tidak ada pihak yang dapat mengubah pencatatan tersebut. Teknologi blockchain dapat menjaga transparansi, akurasi, dan keamanan untuk keseluruhan pihak.

Dalam pelaporan PPN di Indonesia memerlukan 2 sistem, yaitu untuk membuat faktur dan melaporkan faktur. Proses pembuatan dan proses validasi faktur yang dilaporkan memerlukan waktu yang cukup lama karena masih menggunakan tenaga kerja manusia. Disisi lain sistem yang bersifat sentral apabila diakses secara serentak akan menimbulkan permasalahan dan memperlambat proses pelaporan faktur. Apabila menggunakan blockchain, faktur dapat diterapkan dengan kontrak pintar yang mempermudah proses validasi. Namun karena pembayaran PPN hanya menerima Rupiah, proses kontrak pintar tidak dapat ditumpangkan pada jaringan blockchain yang sudah ada seperti mata uang kripto. Sehingga dibutuhkan perancangan yang sesuai dengan sistem perpajakan di Indonesia.

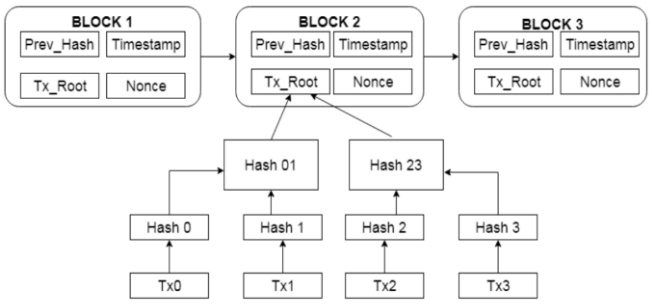
Model yang digunakan berupa contoh pelaporan Faktur Pajak Keluaran di Indonesia yang melibatkan penjual dan pembeli sebagai Wajib Pajak. Tujuan dari penelitian ini untuk mengetahui penerapan teknologi blockchain dari sistem pelaporan Faktur Pajak yang sesuai di Indonesia. Proses yang akan dilakukan antara lain menghubungkan antar node, pembuatan Faktur Pajak berupa kontrak pintar pada browser, dan mengirimkannya pada node untuk disimpan pada blok baru.

Dalam proses penambangan diberi tingkat kerumitan yang berbeda. Dari pengujian tersebut didapatkan bahwa tingkat kerumitan penambanngan yang tinggi, yaitu yang memiliki banyak nilai awal 0 pada hash, akan menghasilkan blok baru yang lebih lama. Maka dari itu diperlukan sebuah konfigurasi dan regulasi yang sesuai agar sistem yang diharapkan dapat berjalan dengan baik.

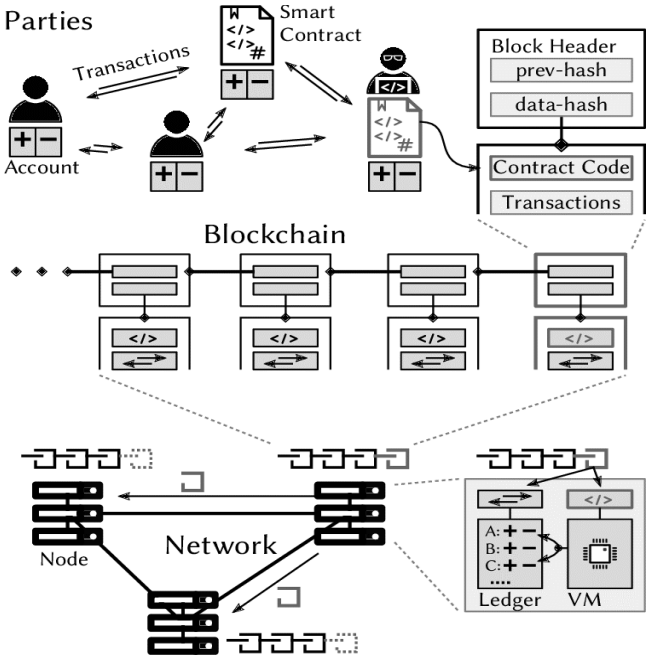
II. DASAR TEORI

A. Blockchain

Blockchain adalah suatu teknologi penyimpanan data yang menggunakan teknik kriptografi, dimana data-data tersebut saling berhubungan. Blockchain ditemukan oleh Satoshi Nakamoto pada tahun 2008 dan digunakan sebagai



Gambar 1. Struktur blockchain.

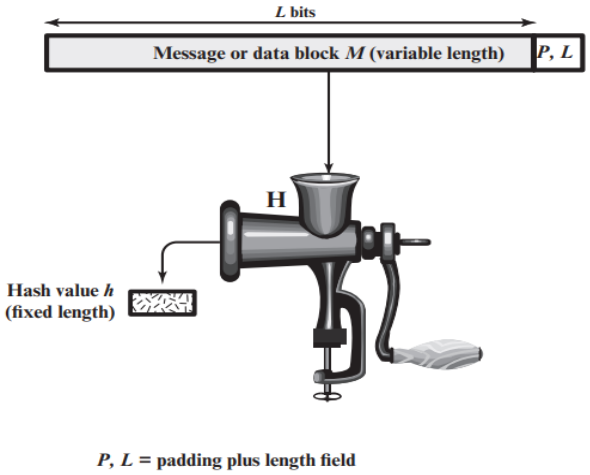


Gambar 2. Kontrak pintar tersimpan dalam blok baru dan terdistribusi dalam jaringan blockchain.

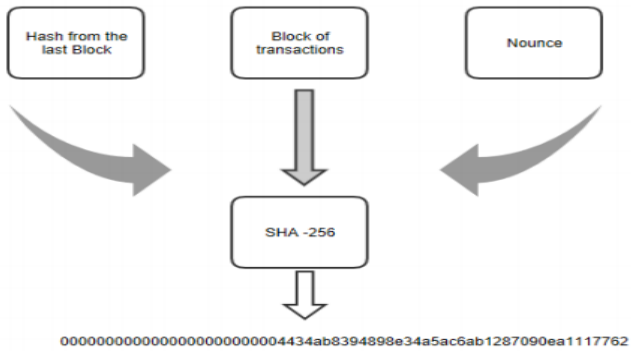
pencatatan transaksi Bitcoin. Seiring dengan perkembangannya, teknologi blockchain kini dapat diterapkan dalam beberapa aspek. Beberapa contoh penerapan blockchain antara lain mata uang kripto (*cryptocurrency)*, *smart contract*, *supply chain*, finansial dan pemerintahan.

Penerapan blockchain dalam sektor finansial merupakan sebuah solusi alternatif untuk menyederhanakan proses persetujuan pergerakan barang yang melintasi perbatasan dari beberapa badan hukum (Bea Cukai, pelabuhan, perusahaan angkutan truk atau kereta api, dan sebagainya) [2]. Blockchain digunakan oleh badan hukum untuk menandatangani semua persetujuan dan menginformasikan status persetujuan, saat barang diterima, dan saat pembayaran ditransfer ke semua pihak.

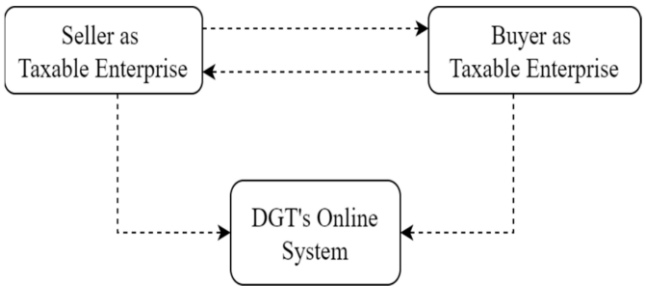
Pada sektor pemerintahan, blockchain digunakan sebagai media pencatatan transaksi dan pelacakan kepemilikan aset sehingga prosesnya menjadi lebih efisien dan transparan [2]. Salah satu permasalahan yang sering ditemui pada sektor ini adalah keaslian data. Hal tersebut disebabkan oleh banyaknya pemalsuan dokumen yang ditambah dengan proses verifikasi yang sulit. Blockchain dapat diterapkan untuk mengatasi masalah ini dengan cara menerbitkan dokumen yang dapat diautentikasi secara digital yang tidak dapat dipalsukan, diberi stempel waktu, dan dapat diakses oleh siapa saja. Pengaplikasian blockchain ini dapat mengurangi biaya dan waktu yang diperlukan untuk melakukan verifikasi dokumen



Gambar 3. Kriptografi fungsi hash.



Gambar 4. Contoh hasil penyelesaian tingkat kerumitan=24.

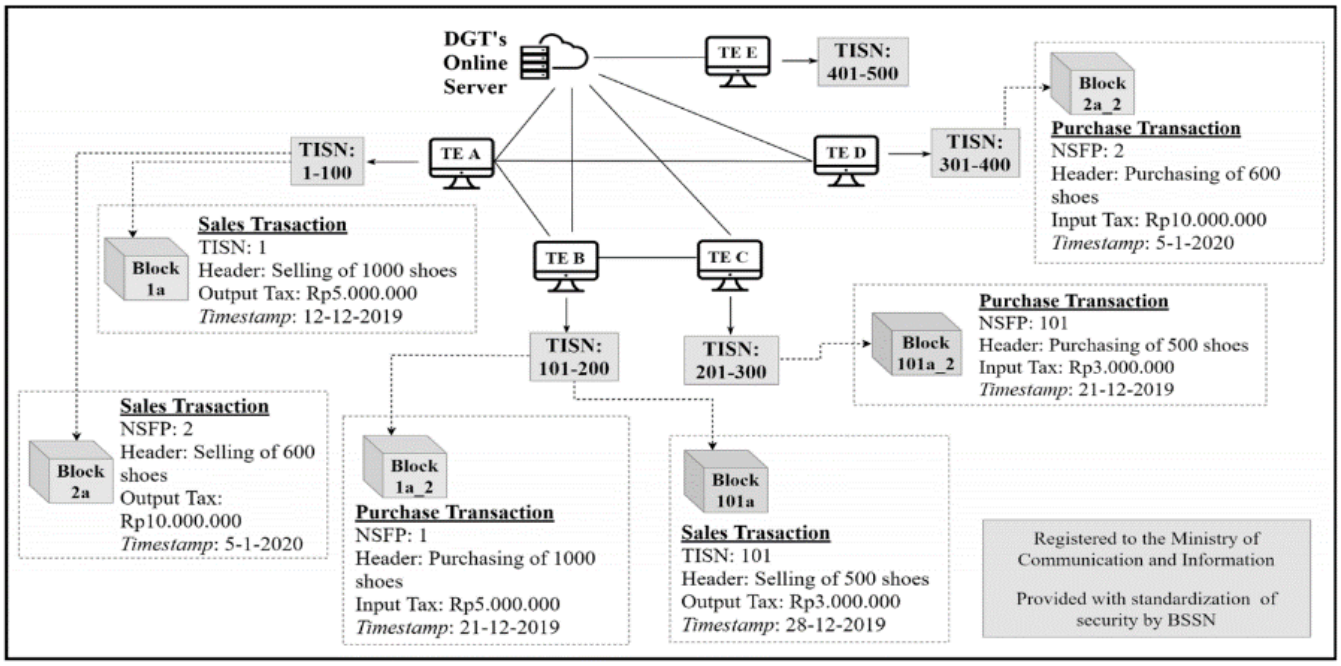


Gambar 5. Skema Wajib Pajak sebagai pembeli dan penjual dalam sistem Direktorat Jenderal Pajak.

serta menjamin adanya transparansi dalam proses dokumentasi.

Seperti namanya, blockchain terdiri dari kata *block* (blok/balok) dan *chain* (rantai). Setiap blok berisikan data (umumnya diwakilkan dalam *Merkle Tree*) [3], *timestamp*, *nonce* dan hash blok sebelumnya yang berfungsi sebagai rantai untuk menghubungkan antar blok. Struktur blockchain teridi dari blok yang terhubung dengan hash sebelumnya dan berisikan kumpulan data yang disederhanakan dalam pohon merkle yang tertera dalam Gambar 1.

Pohon Merkle menggunakan algoritma hash SHA256 untuk mengenkripsi data transaksi dan menyimpulkan keseluruhan transaksi kedalam blok dalam bentuk hash [4]. Nilai hash ini akan digunakan sebagai acuan pada blok berikutnya. *Timestamp* atau stempel waktu membuktikan bahwa data tercatat pada saat itu untuk dijadikan hash. Dengan setiap stempel waktu yang ditambahankan pada blok baru akan memperkuat stempel waktu sebelumnya. *Nonce* atau *number used once* merupakan merupakan sebuah *counter* untuk memastikan transaksi hanya dapat dilakukan sekali. Selain itu *nonce* merupakan sebuah hasil penyelesaian



Gambar 6. Rancangan faktur pajak yang disimpan dalam jaringan blockchain.

kriptografi yang akan dijelaskan lebih lanjut pada sub bab berikutnya.

Secara desain, blockhain tahan dari pengubahan data. Ketika transaksi sudah tervalidasi, data akan disimpan pada blok. Setiap blok menggunakan hash dari blok sebelumnya untuk saling menghubungkan. Selain itu, blok yang lebih lama tidak dapat diubah tanpa memutus rantai ke setiap blok yang direkam dan terdistribusi dalam jaringan komputer blockchain. Jika seorang penyerang akan mencoba untuk mengubah blok, dia harus mengubah semua blok yang terjadi setelahnya.

Blockchain terdiri dari beberapa jenis, antara lain publik, konsursium, dan privat. Berikut penjelasan yang diberikan berdasarkan sifat aksesibilitas data [5]. Blockchain dapat dikategorikan sebagai berikut:

1) Blockchain Publik

Blockchain publik merupakan blockchain yang dapat diakses secara umum dengan mudah. Setiap orang dapat memeriksa dan memverifikasi transaksi secara langsung pada jaringan blockchain publik. Keterbukaan menyebabkan data menjadi sangat mudah diakses dan transparan. Beberapa keunggulan dari blockchain publik dapat ditingkatkan, diuji, dan diakses oleh siapapun.

2) Blockchain Konsursium/Gabungan

Blockchain konsorsium/gabungan adalah blockchain dimana proses konsensusnya dikendalikan oleh satu set node yang dipilih sebelumnya. Disisi lain, tidak semua node pada jaringan blockchain dapat memiliki hak konsensus di jaringan itu. Pihak yang berhak membaca dan memasukkan transaksi ke dalam jaringan dalam blockchain konsorsium adalah beberapa organisasi yang telah ditentukan sebelumnya dan membentuk asosiasi bersama bersama.

3) Blockchain Privat

Blockchain privat dikelola oleh sebuah organisasi. Akses untuk melihat data dapat bersifat publik atau terbatas pada kelompok pihak. Setiap node maupun pengguna dalam jaringan blockchain akan dibatasi, sehingga terdapat otoritas manajemen yang ketat pada jaringan tersebut. Dengan manajemen yang ketat ini, tidak semua node dapat berpartisipasi dalam jaringan blockchain. Dapat dinyatakan bahwa keanggotaan node dalam jaringan blockchain privat dikendalikan dan tidak bebas untuk mengakses blok. Pada tipe ini, hanya pihak-pihak tertentu yang dapat membaca atau mengirimkan transaksi yaitu organisasi atau anak perusahaan dalam grup yang sama.

B. Kontrak Pintar (Smart Contract)

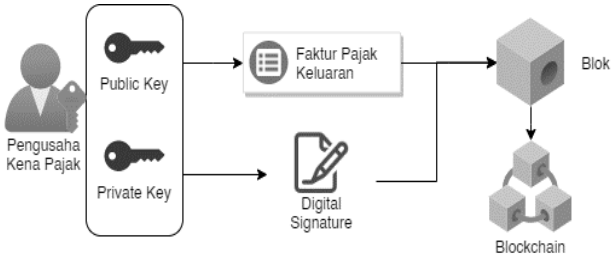
Kontrak pintar atau *smart contract* dikenalkan oleh Nick Szabo pada tahun 1994 sebagai sebuah kontrak, *smart contract* memiliki sifat deterministik (disebabkan oleh faktor sebelumnya), transparan, otonom, terdistribusi dan abadi. Sifat-sifat ini menjadikannya ideal untuk dipakai sebagai nilai tukar pengganti kepercayaan antar dua pihak dalam jaringan *decentralization finance* atau DeFi.

Penggunaan *kontrak pintar* terus berkembang menjadi program yang berjalan pada *platform blockchain*. Program ini membuat protokol persetujuan digital yang aturannya ditentukan oleh kode komputer dan disepakati oleh node jaringan. Kini *smart contract* adalah bagian dari alat transaksi dengan memenuhi kode tersebut.

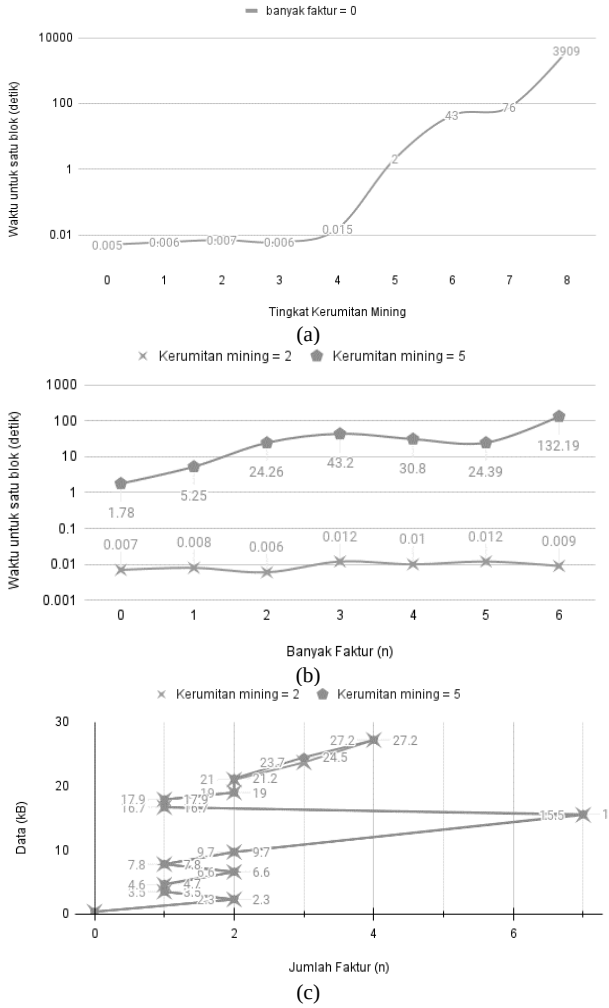
C. Kriptografi Kunci Publik

Kriptografi kunci publik, atau kriptografi asimetris, adalah sistem kriptografi yang menggunakan pasangan kunci dalam proses enkripsi dan dekripsi dan selalu berpasangan. Kunci privat adalah kode yang bersifat rahasia dan hanya diketahui oleh pemiliknya. Kunci publik tidak dirahasiakan oleh pemiliknya dan dapat diketahui oleh siapapun. Jika data asli (*plaintext*) dienkripsi dengan kunci privat dan menjadi data yang disandikan (*ciphertext*), maka untuk dekripsi menggunakan kunci publik untuk menampilkan kembali data asli [5]. Kontrak pintar tersimpan dalam blok baru dan terdistribusi dalam jaringan blockchain tertera pada Gambar 2.

Algoritma yang paling umum digunakan untuk menghasilkan kunci publik salah satunya adalah Rivest-Shamir-Aldeman (RSA), dikembangkan pada tahun 1977 oleh Ron Rivest, Adi Shamir, and Len Adleman. Sejak saat itu, algoritma RSA sebagai pendekatan yang paling banyak diterima dan diterapkan untuk enkripsi kunci publik [6].



Gambar. 7. Desain keseluruhan system.



Gambar 8. Plot hasil pengujian (a) pertama: waktu berdasarkan tingkat kerumitan mining, (b) kedua: waktu berdasarkan penambahan jumlah faktur, (c) ketiga: hasil ukuran data pada setiap penambahan blok baru.

Skema RSA adalah *cipher* (algoritma untuk melakukan enkripsi dan dekripsi) di mana *plaintext* dan *ciphertext* adalah bilangan bulat antara 0 dan n - 1 untuk beberapa n. Sebuah ukuran khas untuk n adalah 1024 bit, atau 309 angka desimal. Artinya, n kurang dari 2^{1024}. Berikut merupakan algoritma dalam RSA dalam proses pembuatan kunci publik dan kunci privat.

Pada umumnya, algoritma pasangan kunci ini digunakan sebagai alamat pengirim dan penerima dalam blockchain. Dengan menggunakan pasangan kunci ini, dapat mengurangi penyebaran informasi data pribadi pengguna dan melakukan verifikasi data dengan pembuatan *digital signature*.

D. Penambangan (Mining)

Dalam blockchain data akan disimpan pada sebuah blok. Pada Bitcoin umumnya penambahan blok dilakukan setiap 10 menit [4]. Setiap blok baru akan ditambahkan kedalam blockchain, tidak dapat diubah, tidak dapat dihapus atau dimodifikasi. Sekumpulan kelompok khusus dalam jaringan blockchain atau penambang/*miner* (node komputer terhubung dalam blockchain) akan bertanggung jawab untuk menambahkan data pada penambahan blok baru. Penambang harus mengotentikasi setiap data menggunakan kunci publik pengirim dan menambahkan transaksi ke blok.

Agar sebuah blok dapat ditambahkan dalam blockchain, perlu dilakukan proses *mining/*menambang. Untuk menambang blok, penambang perlu menemukan solusi untuk teka-teki kriptografi. Jika blok yang ditambang diterima oleh blockchain, pada umumnya penambang akan menerima *reward/*hadiah dalam mata uang kripto (misal: Bitcoin) yang merupakan biaya tambahan dalam transaksi [4]. Proses penambangan juga disebut sebagai *Proof-of-Work* (PoW), dan ini adalah mekanisme utama yang memungkinkan blockchain menjadi *trustless* dan aman (keamanan blockchain akan dibahas lebih lanjut).

Tabel 1.
Perbedaan sistem konvensional dan sistem blockchain

No	Pembanding	Sistem Konvensional	Sistem Blockchain
1	Aplikasi pelaporan faktur	2 (e-Nova dan e- Faktur)	1 (Kontrak pintar)
2	Validator	Tenaga manusia	Node dalam jaringan
3	Lama proses validasi	Beberapa jam hingga hari	Beberapa menit
4	Penyimpanan	Satu server terpusat	Beberapa server/node terdistribusi
5	Regulasi	• Penggunaan e-Faktur, • Perhitungan PPN, • Pembayaran Rupiah	Belum ada

Tabel 2.
Kelebihan dan kelemahan sistem blockchain

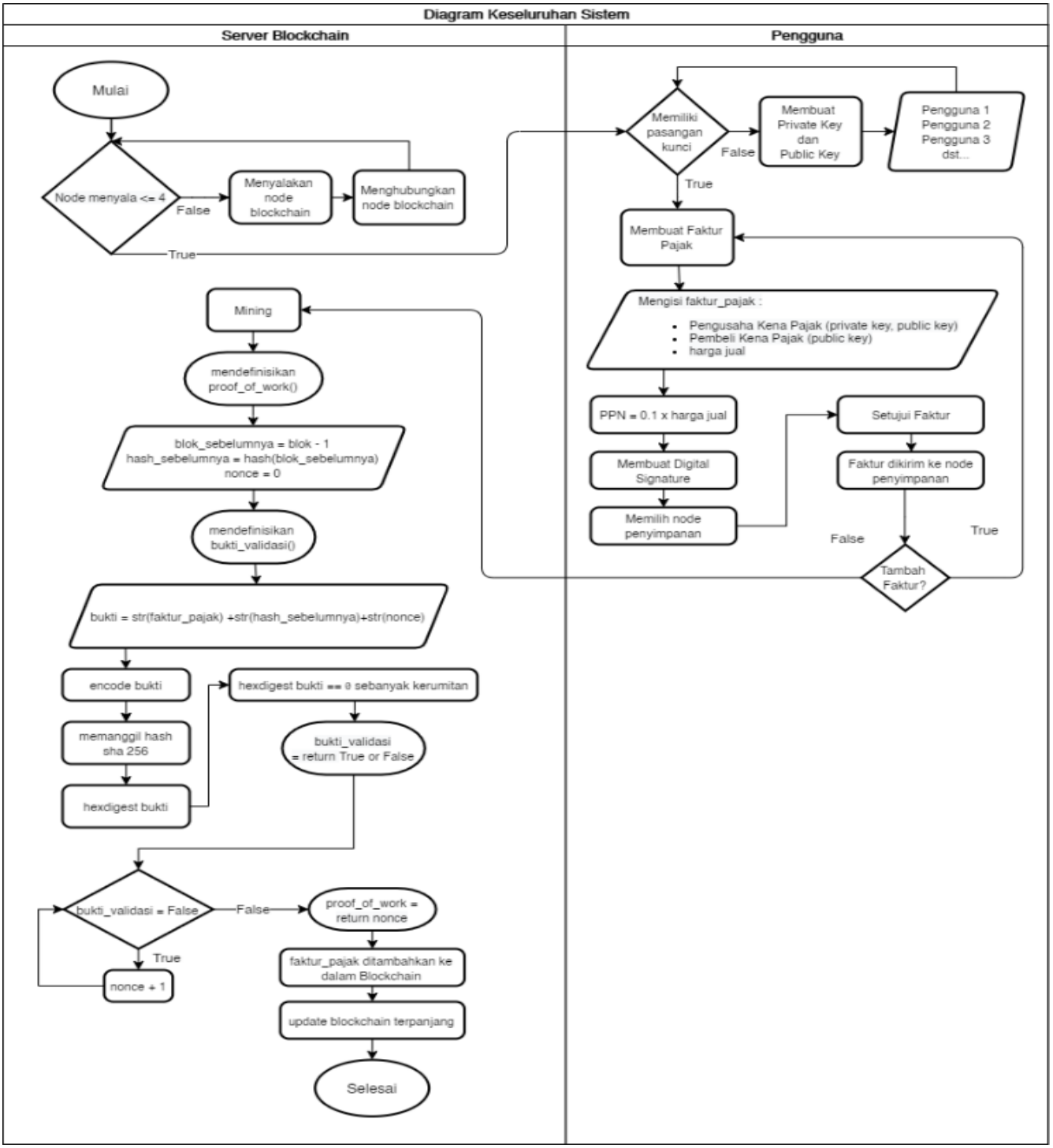
No	Kelebihan	Kekurangan
1	Identitas yang tersimpan dalam faktur aman dengan kunci publik	Pengguna mungkin kesulitan menggunakan dan menyimpan pasangan kunci publik
2	Dapat memanfaatkan server setiap wilayah kantor pajak	Perawatan server dilakukan pada wilayah kantor masing-masing
3	Faktur tersimpan secara permanen	Bila terjadi kesalahan harus membuat faktur baru sebagai revisi faktur sebelumnnya
4	Sistem validasi yang sulit dilanggar untuk proses otomasi	Harus terhindar dari gangguan/*bug free*
5	Dapat dikembangkan sesuai kebutuhan organisasi	Seluruh node dalam jaringan harus memiliki konfigurasi yang sama

E. Hash

Untuk memahami teka-teki kriptografi blockchain akan dibantu dengan fungsi hash. Fungsi hash yang akan digunakan merupakan salah satu bentuk teknik kriptografi tanpa menggunakan kunci (*unkeyed cryptosystem*). Fungsi hash adalah fungsi yang dapat digunakan untuk memetakan data dengan ukuran arbitrer (tidak adanya hubungan langsung yang antara data asli dengan data yang terenkripsi) ke data dengan ukuran tetap. Nilai yang dikembalikan oleh fungsi hash disebut hash. Berikut merupakan persamaan fungsi hash [6]:

$$h = H(M)$$

Keterangan:
M = pesan dengan ukuran sembarang
H = fungsi hash



Gambar 9. Diagram keseluruhan sistem.

h = *message-digest* atau nilai hash

Fungsi hash satu arah (*one-way function*) adalah fungsi hash yang bekerja dalam satu arah. Pesan yang sudah diubah menjadi *message digest* tidak dapat dikembalikan lagi menjadi pesan semula (*irreversible)*. Salah satu algoritma fungsi hash ini adalah *Secure Hash Algortihm* (SHA). Gambar 3 merupakan gambaran kriptografi fungsi hash.

SHA merupakan algortima kriptografi hash yang dibuat oleh *National Institute of Standards and Technology* (NIST) dan dipublikasikan sebagai standar. Saat kelemahan SHA diketahui, maka dilakukan revisi dan sekarang ditetapkan SHA-2 yang memiliki variasi 256, 384, dan 512 bit yang dikenal juga sebagai SHA-256, SHA-384, dan SHA-512. Dalam melakukan proses pembuatan *digital signature*, telah diregulasi dalam S/MIME (*Secure/Multipurpose Internet Mail Extensions).* Dimana proses penandatanganan tersebut bila menggunakan kunci RSA harus menggunakan SHA-256 sebagai *message digest* dalam pembuatan *digital signature* tersebut [6].

F. Tingkat Kerumitan

Pada umumnya blockchain menggunakan fungsi hash kriptografi yang disebut SHA-256. Panjang dari SHA-256 adalah 256 bit, dan umumnya direpresentasikan dalam heksadesimal sepanjang 64 karakter. SHA-256 diterapkan pada kombinasi data dari blok (umumnya transaksi) dan nomor yang disebut *nonce*. Dengan mengubah data blok atau *nonce*, akan mendapatkan hash yang berbeda. Agar sebuah blok dianggap valid atau ditambang, nilai hash blok dan *nonce* harus memenuhi kondisi tertentu.

Misalnya, dari empat digit utama (*most significant bit*) hash harus sama dengan "0000". Untuk meningkatkan kerumitan penambangan dengan membuat kondisinya lebih kompleks, dapat menambahkan jumlah 0 yang diperlukan untuk memulai nilai hash. Teka-teki kriptografi yang harus dipecahkan oleh penambang adalah menemukan nilai *nonce* yang membuat nilai hash memenuhi kondisi penambangan. Memiliki jawaban yang benar adalah apa yang dikenal sebagai *Proof-of-Work*. *Proof-of-Work* merupakan sebuah proses yang memakan waktu untuk diproduksi, tetapi mudah untuk diverifikasi oleh pihak lain. Untuk menemukan jawaban yang benar, penambang harus melakukan hash ke nilai yang lebih kecil dari target saat ini [3]. Contoh hasil penyelesaian dengan tingkat kerumitan 24 tertera pada Gambar 4.

G. Model Konsensus

Penambang pertama yang berhasil menyelesaikan teka-teki kriptografi akan menambahkan data pada blok baru yang tervalidasi, kemudian blok baru ditambahkan ke dalam jaringan blockchain. Jika terdapat 2 penambang memecahkan satu blok pada waktu yang hampir bersamaan, maka akan memiliki 2 blockchain yang berbeda dalam jaringan, dan diperlukan blok berikutnya untuk menyelesaikan konflik tersebut. Beberapa penambang akan memutuskan untuk menambang di atas blockchain 1 dan yang lainnya di atas blockchain 2. Penambang pertama yang menemukan blok baru akan menyelesaikan konflik. Jika blok baru ditambang di atas blockchain 1, maka blockchain 2 menjadi tidak valid, dan transaksi yang merupakan bagian dari blockchain 2 dan tidak ditambahkan ke blockchain akan kembali ke kumpulan transaksi dan ditambahkan ke blok berikutnya. Singkatnya, jika ada konflik di blockchain, maka rantai terpanjang menang.

H. Pajak Pertambahan Nilai

Pajak Pertambahan Nilai atau PPN adalah pungutan yang dibebankan atas transaksi jual-beli barang dan jasa yang dilakukan oleh Wajib Pajak pribadi atau Wajib Pajak badan yang telah menjadi Pengusaha Kena Pajak (PKP). Pihak yang wajib memungut, menyetor, dan melaporkan PPN adalah pedagang/penjual. Namun, pihak yang berkewajiban membayar PPN adalah konsumer akhir.

Gambar 5 merupakan gambaran sederhana bagaimana sistem PPN saat ini diterapkan. Ketika penjual (pihak yang tergolong sebagai Wajib Pajak) melakukan pungutan atas Barang Kena Pajak maupun Jasa Kena Pajak kepada pembeli (tergolong sebagai Wajib Pajak), terdapat kewajiban yang harus dilakukan yaitu memungut PPN, seperti Gambar 5. Pungutan pajak atas Barang Kena Pajak (BKP) atau Jasa Kena Pajak (JKP) yang dikenakan PPN dibuktikan dengan Faktur Pajak. Faktur Pajak dibuat oleh Wajib Pajak (WP) atau Pengusaha Kena Pajak (PKP) yang menjual BKP maupun JKP sebagai bukti bahwa perusahaan telah memungut PPN dari pihak yang membeli BKP/JKP tersebut.

Dari pembuatan Faktur Pajak ini harus berupa elektronik atau dapat disebut dengan e-Faktur sesuai Peraturan Direktur Jenderal Pajak Nomor PER-16/PJ/2014 tentang Tata Cara Pembuatan dan Pelaporan Faktur Pajak Berbentuk Elektronik. Besar tarif PPN yang dikenakan sesuai dengan ketentuan dalam Undang-Undang Nomor 42 Tahun 2009 tentang Pajak Pertambahan Nilai, yaitu 10% dari objek yang dikenakan pajak. Untuk pembayaran harus menggunakan Rupiah, seperti yang diatur dalam UU No 7 Tahun 2011 tentang mata uang yang berbunyi, “Undang-Undang ini mewajibkan penggunaan Rupiah dalam setiap transaksi yang mempunyai tujuan pembayaran, penyelesaian kewajiban lainnya yang harus dipenuhi dengan uang, dan/atau transaksi keuangan lainnya, yang dilakukan di Wilayan Negara Kesatuan Republik Indonesia.

I. Sistem Pelaporan e-Faktur Menggunakan Blockchain

Gambar 6 menunjukkan adanya transparansi dan keamanan data ketika menggunakan teknologi blockchain. Data yang tercatat di setiap blok dari setiap Pengusaha Kena Pajak (PKP) akan dikunci menggunakan fungsi hash pada blockchain. Data tersebut meliputi data yang terlibat dalam transaksi jual beli barang atau layanan yang dikenai pajak dengan rekanan transaksinya. Adanya fungsi hash membuat PKP tidak dapat memanipulasi data di dalam blok yang telah dicatat dalam teknologi jaringan blockchain. Sistem dalam teknologi blockchain juga memungkinkan Direktorat Jenderal Pajak sebagai regulator untuk memantau dan menelusuri transaksi secara komprehensif. Dengan demikian, semua pencatatan data transaksi yang menghasilkan Pajak Pertambahan Nilai (PPN) akan terlacak dan dicatat dengan baik dan aman. Desain keseluruhan sistem tertera pada Gambar 7.

III. PERANCANGAN SISTEM

A. Diagram Blok Sistem

Dalam penelitian ini, diagram blok keseluruhan sistem dapat dilihat pada Gambar 9. Terdapat 3 bagian utama pada sistem yang dibuat:

1. Pengusaha Kena Pajak memiliki kunci publik dan kunci privat.
2. Pembuatan faktur dan menandatangani dengan kunci privat Pengusaha Kena Pajak.
3. Mengirim faktur kedalam jaringan blockchain, proses verifikasi dalam blockchain.

Untuk mengirim atau menerima Faktur Pajak, pengguna harus memiliki sepasang kunci publik dan privat. Jika Alice membeli barang dari Bob, dia membuat Faktur Pajak Keluaran di mana Alice memasukkan kunci publik Alice dan Bob, dan jumlah harga akhir yang dilaporkan. Kemudian menandatangani transaksi menggunakan kunci pribadinya. Komputer di blockchain menggunakan kunci publik Alice untuk memverifikasi bahwa transaksi itu asli dan menambahkan transaksi ke blok yang nantinya akan ditambahkan ke blockchain.

B. Pembangunan Jaringan Blockchain

Arsitektur jaringan blockchain yang digunakan menggunakan topologi mesh. Dengan topologi mesh dapat memanfaatkan setiap komputer/server/node dari beberapa Kantor Pajak sebagai infrastruktur penyimpanan data, sehingga memiliki database yang sama dalam jaringan blockchain. Jika terjadi kerusakan pada sebuah node maupun penambahan node, maka data yang tersimpan akan aman karena ada node lain sebagai *backup.*

Pembuatan kontrak pintar atau e-Faktur dilakukan oleh setiap Pengusaha Kena Pajak pada komputer mereka masing-masing. Kemudian e-Faktur disimpan pada node atau

komputer Kantor Pajak yang telah ditentukan. Setiap node harus memiliki konfigurasi yang sama yaitu, tingkat kerumitan mining dan node lain yang terhubung. Faktur yang diterima pada setiap node akan ditampung sementara dan kemudian akan dilakukan proses mining. Pada proses mining akan mendapatkan *nonce* dan mencatat blok baru yang tersimpan pada alamat komputer tersebut.

C. Perancangan Pengguna

Pada perancangan pengguna akan dibangun *class* Faktur_Pajak mengimplementasikan metode dengan menggunakan Python sebagai berikut:

1. daftar_faktur(): membuat daftar Faktur Pajak yang berurutan.
2. digital_signature(): menandatangani faktur dengan kunci privat.
3. ppn_10(): menghitung Pajak Pertambahan Nilai sebesar 10% dari harga yang dilaporkan.

D. Perancangan Node Blockchain

Pada perancangan node akan dibangun *class* Blockchain juga mengimplementasikan metode dengan menggunakan Python sebagai berikut:

1. tambah_node(node_url): menambahkan node blockchain baru ke daftar node.
2. buat_blok(*nonce*, hash_sebelumnya): menambahkan blok Faktur Pajak ke blockchain.
3. verifikasi_digital_signature(pengusaha_public_key, digital_signature, faktur): memeriksa bahwa tanda tangan yang diberikan sesuai dengan transaksi yang ditandatangani oleh kunci publik (pengusaha_public_key).
4. bukti_validasi(faktur_pajak, hash_sebelumnya, *nonce*, kerumitan=tingkat_kerumitan_mining): memeriksa apakah nilai hash memenuhi kondisi penambangan. Fungsi ini digunakan dalam fungsi proof_of_work.
5. proof_of_work(): mencari *nonce* yang memenuhi kondisi *mining*.
6. hash(data_blok): membuat hash SHA-256 dari sebuah blok.
7. update_blok_terpanjang(): menyelesaikan konflik antara node blockchain dengan mengganti rantai dengan yang terpanjang pada jaringan.
8. valid_chain(chain): memeriksa apakah bockchain valid.
9. kirim_faktur(pengusaha_public_key, pembeli_public_key, digital_signature, ppn): menambahkan transaksi ke daftar transaksi jika tanda tangan diverifikasi.

E. Kerumitan Mining

Pada simulasi dilakukan dengan tingkat kerumitan yang kecil, diberikan nilai integer 2 untuk mendapatkan hash dengan awalan ‘00’ dan integer 5 untuk mendapatkan hash dengan awalan ‘00000’ yang sesuai dalam proses bukti validasi, untuk diberikan nilai *nonce* pada proof_of_work.

IV. ANALISA HASIL SIMULASI DAN PEMBAHASAN

Pada Gambar 8(a) merupakan pengujian tingkat kerumitan penambangan tanpa melibatkan faktur. Dari hasil yang didapat, tingkat kerumitan 0-7 dapat menyelesaikan dalam hitungan detik dan menit. Sedangkan tingkat kerumitan 8 dan lebih diperlukan waktu lebih dari 1 jam dalam penambahan blok baru tanpa melibatkan faktur. Pada Gambar 8(b) merupakan pengujian jumlah faktur dari 2 tingkat kerumitan yang telah ditentukan, kerumitan 2 sebagai parameter mudah dan 5 sebagai parameter sedang. Dari hasil yang didapat, jumlah faktur sedikit mempengaruhi waktu penambangan karena melibatkan stempel waktu. Dapat dimungkinkan penambahan sebuah blok baru yang melibatkan lebih dari 6 faktur menyelesaikan dalam waktu yang jauh lebih lama. Pada Gambar 8(c) merupakan perbandingan data pada dua tingkat kerumitan yang telah diuji. Ukuran data yang didapat dapat dikatakan sama. Rata-rata *header* blok memiliki ukuran data 387 byte untuk memuat informasi blok dan untuk data setiap faktur memiliki ukuran sekitar 773 byte.

Tabel 1 digunakan untuk membandingkan sistem konvensional dan sistem yang menggunakan blockchain. Selain itu, sistem yang dirancang akan memiliki kelebihan dan kekurangan yang tertera pada Tabel 2.

V. KESIMPULAN

Setelah melakukan beberapa percobaan, pengolahan data, dan pengujian terhadap simulasi blockchain, dapat disimpulkan sebagai berikut pembuatan Faktur Pajak dalam bentuk kontrak pintar yang tervalidasi pada node akan disimpan dalam jaringannya. Agar panjang blok dalam blockchain sama dalam jaringan, digunakan topologi mesh untuk menghubungkan antar node dan model konsensus untuk mendapatkan blok terpanjang. Semakin besar tingkat kerumitan *mining* dan penambahan jumlah faktur pada sebuah blok, maka nilai *nonce* akan cenderung lebih tinggi dan dibutuhkan waktu iterasi pada *nonce* yang lebih lama. Maka diperlukan pengaturan yang sesuai pada tingkat kerumitan dan jumlah faktur untuk menjaga konsistensi waktu *mining.* Regulasi yang disarankan untuk blockchain antara lain regulasi penerapan kontrak pintar, regulasi infrastruktur dan proses penambangan, regulasi perbaikan faktur yang salah, regulasi dari kegagalan fungsi sistem.

DAFTAR PUSTAKA

[1] BPS, “Rasio Penerimaan Pajak Terhadap PDB (Persen), 2016-2018,” *Rasio Penerimaan Pajak Terhadap PDB*, Jakarta: Badan Pusat Statistika, 2019. https://www.bps.go.id/indicator/13/1529/1/rasio-penerimaan-pajak-terhadap-pdb.html.

[2] M. Gupta, *Blockchain for Dummies*. New Jersey: John Willey & Sons, Inc., 2017.

[3] M. Scherer, “Performance and Scalability of Blockchain,” Computer Science, Umea Universitet, 2017.

[4] P. S. Maharjan, “Performance Analysis of Blockchain Platforms,” Computer Science, University of Nevada, 2018.

[5] S. S. Sarmah, “Understanding blockchain technology,” *Comput. Sci. Eng.*, vol. 8, no. 2, pp. 23--29, 2018.

[6] W. Stallings, *Cryptography and Network Security*. London: Pearson education, 2017.