

## IMPLEMENTASI *BLOCKCHAIN* PADA PEMADANAN NIK DAN NPWP SEBAGAI LANGKAH NYATA OPTIMALISASI KEAMANAN DATA WAJIB PAJAK DI ERA *SOCIETY 5.0*

Ahmad Fariz Sabili

Fakultas Ilmu Administrasi Universitas Indonesia

Aqila Bagus Misbahuddin

Fakultas Ilmu Administrasi Universitas Indonesia

I Putu Naratama Wira Chandra

Fakultas Ilmu Administrasi Universitas Indonesia

Alamat Korespondensi: [ahmad.fariz12@ui.ac.id](mailto:ahmad.fariz12@ui.ac.id)

---

### INFORMASI ARTIKEL

Diterima Pertama  
[22 11 2023]

Dinyatakan Diterima  
[28 11 2023]

KATA KUNCI:  
blockchain, keamanan data, wajib pajak, *Society 5.0*

KLASIFIKASI JEL:  
H21, H24, H26, M38, M40

### ABSTRACT

*Society 5.0 emphasizes the use of technology in everyday life with the simplicity principle. The implementation of this principle is done through the integration of the Population Identification Number (NIK) and Taxpayer Identification Number (NPWP). However, some problems need to be solved immediately from the integration, namely the security of taxpayer data, which is often a threat to tax digitalization. The method used in this research is the desk research method by qualitatively analyzing books, journals, articles, and taxation materials published on the internet. The results show that blockchain has good potential to provide taxpayer data protection in NIK-NPWP matching. Blockchain utilization has also been carried out in public administration services in Estonia and Italy. As with policies in general, blockchain implementation is inseparable from aspects that become opportunities and challenges to maintain taxpayer data security.*

### ABSTRAK

*Society 5.0 menekankan pada pemanfaatan teknologi dalam kehidupan sehari-hari yang berprinsip pada kesederhanaan. Implementasi prinsip tersebut dilakukan melalui pemadanan Nomor Induk Kependudukan (NIK) dan Nomor Pokok Wajib Pajak (NPWP). Namun, terdapat permasalahan yang perlu segera dicari solusinya dari pemadanan tersebut, yakni keamanan data wajib pajak yang sering kali menjadi ancaman digitalisasi perpajakan. Metode yang digunakan dalam penelitian ini adalah metode kepustakaan (*desk research*) dengan menganalisis secara kualitatif buku, jurnal, artikel, dan materi perpajakan yang dimuat di internet. Hasil penelitian menunjukkan bahwa *blockchain* memiliki potensi yang baik untuk memberikan perlindungan data wajib pajak dalam pemadanan NIK-NPWP. Pemanfaatan *blockchain* juga telah dilakukan pada pelayanan administrasi publik di Estonia dan Italia. Sebagaimana kebijakan pada umumnya, implementasi *blockchain* tidak terlepas dengan aspek yang menjadi peluang dan tantangan untuk menjaga keamanan data wajib pajak.*

## 1. PENDAHULUAN

Gagasan mengenai tahap baru berupa *Society 5.0* lahir dari pemaparan Kabinet Jepang pada *The 5th Science and Technology Basic Plan* di tahun 2016 lalu (Fukuyama, 2018). Kelahiran tahap baru dalam masyarakat merupakan kontribusi dari adanya transformasi digital, yaitu kemajuan pesat pada bidang teknologi digital dan pemanfaatan data yang mampu mengubah aspek-aspek masyarakat, seperti kehidupan pribadi, administrasi publik, struktur industri, dan pekerjaan (Keidanren, 2018). Dalam konsep *Society 5.0*, masyarakat akan berdampingan dengan teknologi dalam keseharian mereka sebagai alat untuk memecahkan masalah dan membawa prinsip kesederhanaan (Sugiono, 2021; Suryaputra, 2023).

Dalam hal prinsip kesederhanaan, Indonesia sendiri belum dapat menerapkan prinsip tersebut. Sebagai contoh konkret adalah banyaknya kartu identitas yang harus dimiliki oleh tiap-tiap individu, seperti Kartu Tanda Penduduk (KTP), Nomor Pokok Wajib Pajak (NPWP), Surat Izin Mengemudi (SIM), kartu Badan Penyelenggara Jaminan Sosial (BPJS) Ketenagakerjaan, kartu Anjungan Tunai Mandiri (ATM), dan masih banyak lagi kartu lainnya (Tobing & Kusmono, 2022). Hal tersebut menunjukkan bahwa Indonesia belum menerapkan *Single Identity Number* (SIN) (Suryaputra, 2023). Implikasinya, masyarakat akan direpotkan dengan banyaknya kartu dan apabila kehilangan satu kartu akan melakukan pembuatan ulang yang menguras banyak waktu, tenaga, dan biaya (Angga et al., 2019).

Dari hal tersebut, pemerintah sekarang telah melakukan pepadanan NIK dan NPWP sebagaimana diatur dalam ketentuan Pasal 2 ayat (1a) Undang-Undang Nomor 28 Tahun 2007 tentang Ketentuan Umum dan Tata Cara Perpajakan (KUP) sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 7 Tahun 2021 tentang Harmonisasi Peraturan Perpajakan, Peraturan Menteri Keuangan (PMK) Nomor PMK-112/PMK.03/2022 tentang NPWP bagi Orang Pribadi, Badan dan Instansi Pemerintah, dan Peraturan Presiden Nomor 83 Tahun 2021 tentang Pencantuman dan Pemanfaatan NIK dan/atau NPWP dalam Pelayanan Publik. Menurut Tobing & Kusmono (2022), pepadanan NIK-NPWP sebagai wujud SIN ini menjadi langkah nyata pemerintah untuk simplifikasi administrasi pajak. Dari sisi Direktorat Jenderal Pajak (DJP), SIN ini diharapkan dapat membantu dalam pengawasan kepatuhan wajib pajak, sedangkan dari sisi wajib pajak dapat mengurangi *cost of compliance*, seperti waktu, tenaga dan biaya kepengurusan NPWP karena biaya-biaya tersebut harus ditekan semaksimal mungkin agar meningkatkan efisiensi dalam pengelolaan pajak.

Kendati demikian, kebijakan tersebut tidak mulus begitu saja, tetapi justru dengan adanya digitalisasi menimbulkan potensi masalah baru, misalnya keamanan data. Menurut Ketua Badan Pemeriksa Keuangan (BPK) Republik Indonesia periode 2009-2014, implementasi SIN tersebut dapat berimplikasi

pada tersebarluasnya Surat Pemberitahuan (SPT) Tahunan milik wajib pajak yang semestinya bersifat rahasia (FIA UI, 2023). Melihat hal tersebut, pemerintah perlu mengambil tindakan preventif agar tujuan awal kebijakan dapat berjalan dengan baik. Oleh karena itu, penulis melalui kajian kali ini ingin menganalisis solusi dari permasalahan keamanan data dari pepadanan NIK-NPWP tersebut.

Berangkat dari latar belakang tersebut, diperlukan suatu kajian yang membahas solusi atas keamanan data wajib pajak sebagai implikasi diterapkannya pepadanan NIK dan NPWP. Oleh karena itu, *paper* ini akan menjawab beberapa pertanyaan berikut, yakni: (1) Bagaimana urgensi keamanan data wajib pajak? dan (2) Bagaimana peran teknologi *blockchain* dalam menjaga keamanan data wajib pajak? Dengan demikian, tujuan dari penelitian ini antara lain: (1) Memberikan gambaran urgensi keamanan data wajib pajak dan (2) Memberikan penjelasan peran teknologi *blockchain* dalam menjaga keamanan data wajib pajak.

## 2. KERANGKA TEORI

### 2.1. Pajak

Menurut James dalam Rosdiana & Irianto (2014), pajak adalah pungutan wajib yang dilakukan oleh otoritas publik yang tidak mendapatkan imbalan secara langsung. Definisi ini dipertegas oleh Soemitro sebagaimana dikutip Brotodihardjo yang menjelaskan pajak sebagai kontribusi rakyat berupa pembayaran ke kas pemerintah sesuai dengan hukum yang dapat ditegakkan tanpa perlu adanya manfaat langsung yang dapat dibuktikan, dana yang terkumpul tersebut selanjutnya dipergunakan untuk membiayai pengeluaran umum (Rosdiana & Irianto, 2014). Setelah diselenggarakannya kongres pajak sedunia di Argentina pada tahun 2005, terdapat pergeseran paradigma dalam pendefinisian pajak, yakni pajak tidak boleh memaksa sehingga pajak lebih netral dan tak berkonotasi negatif, pajak harus dikembalikan ke masyarakat, pembayar pajak harus memperoleh *benefit*, dan pajak juga mempunyai pengukuran *benefit* (Rosdiana & Irianto, 2014).

### 2.2. Kepatuhan Pajak

Kepatuhan pajak atau *tax compliance* merupakan kondisi di mana wajib pajak berperilaku memenuhi semua kewajiban perpajakannya serta melaksanakan semua hak perpajakannya (Waluyo, 2020). Menurut Nurmantu dalam Waluyo (2020), ada dua jenis kepatuhan, yaitu kepatuhan formal dan kepatuhan materiil. Kepatuhan formal adalah situasi di mana wajib pajak memiliki kesadaran untuk memenuhi kewajiban formalnya sesuai dengan peraturan perundang-undangan perpajakan, sedangkan kepatuhan materiil adalah kondisi di mana wajib pajak memenuhi secara substantif ketentuan materiil perpajakan sesuai dengan undang-undang yang berlaku (Waluyo, 2020).

### 2.3. Reformasi Perpajakan

Direktorat Jenderal Pajak (2022) mendefinisikan reformasi perpajakan sebagai perubahan sistem perpajakan secara menyeluruh, seperti perbaikan regulasi, pembetulan administrasi, dan peningkatan basis perpajakan. Reformasi Perpajakan dinilai perlu untuk dilakukan karena rendahnya tingkat kepatuhan wajib pajak, semakin berkembangnya transaksi dagang sehingga harus adanya pembaruan regulasi, perkembangan ekonomi digital, tingginya target penerimaan pajak setiap tahun, dan kurangnya sumber daya manusia di bidang perpajakan yang jumlahnya tidak sebanding dengan pertumbuhan populasi (Direktorat Jenderal Pajak, 2022). Adapun lima pilar reformasi perpajakan adalah peraturan perundang-undangan, proses bisnis, organisasi, sumber daya manusia, serta teknologi informasi dan basis data (Direktorat Jenderal Pajak, 2022).

#### 2.4. *Single Identity Number*

*Single Identity Number* (SIN) adalah sebuah identitas unik dimiliki oleh setiap individu yang tidak hanya mencakup nomor identitas pribadi, tetapi juga mencakup informasi terkait seperti data keluarga, kepemilikan aset, informasi polisi, perbankan, pajak, dan banyak lagi, seperti yang dijelaskan oleh Edhy dalam Siregar (2017). Selanjutnya, dalam Siregar (2017), SIN digambarkan sebagai nomor identitas unik yang menggabungkan data dari berbagai lembaga pemerintah dan swasta dan berkarakteristik unik, tidak bisa digandakan, datanya lengkap bersifat nasional, dan dalam hal perpajakan ditujukan agar pengawasan perpajakan menjadi lebih mudah.

#### 2.5. *Blockchain*

*Blockchain* adalah jenis dari *database* terdistribusi yang terdesentralisasi atau *ledger*. Terkadang pengertian tentang *Decentralized Ledger Technology* (DLT) dan *blockchain* secara keliru dipersamakan (Panait *et al.*, 2020). Pada dasarnya, *blockchain* tersebar ke beberapa *node*, dan setiap *node* itu menyimpan salinan *blockchain*. Lebih lanjut lagi, dalam *blockchain* tidak ada satu keputusan, melainkan keputusan dihasilkan dari konsensus di setiap *node* (Panait *et al.*, 2020). *Blockchain* dapat dibedakan menjadi dua, yakni *blockchain* tidak berizin dan berizin (*permissionless* dan *permissioned*). Dalam *blockchain* tidak berizin, setiap entitas dapat menjadi sebuah *node* serta berpartisipasi dalam konsensus *blockchain*. Namun, dalam *blockchain* tidak berizin, terdapat protokol konsensus yang hanya mengizinkan *node* tertentu untuk berkonsensus (Panait *et al.*, 2020).

### 3. METODE PENELITIAN

Penelitian menggunakan metode kepustakaan (*desk research*) dengan menganalisis secara kualitatif data yang diperoleh dari buku, jurnal, dan artikel yang termuat di internet. Sistematika kepenulisan dilakukan bersifat naratif melalui analisis implementasi *blockchain* pada keamanan data wajib pajak dalam pepadanan NIK-NPWP yang disertai dengan penelitian terdahulu, pendapat ahli, dan kajian

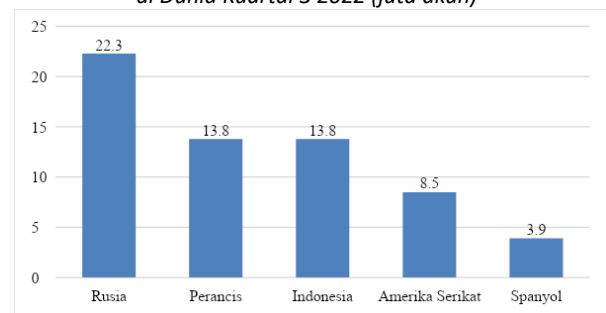
penerapan *blockchain* pada administrasi pajak. Adapun dampak implementasinya dapat dilihat melalui *benchmarking* negara lain dan analisis peluang serta tantangan penerapan *blockchain* untuk menjamin keamanan data.

### 4. HASIL PENELITIAN

#### 4.1. Urgensi Perlindungan Data Wajib Pajak

Sebagaimana telah disebutkan sebelumnya, pepadanan NIK-NPWP berpotensi pada kebocoran data. Senada dengan hal tersebut, penelitian yang dilakukan Tobing & Kusmono (2022) membuktikan bahwa sebanyak 40% responden sangat khawatir data-data mereka akan bocor apabila pepadanan NIK-NPWP diimplementasikan. Kemudian, untuk responden yang khawatir sebanyak 40% dari total responden, 12% responden bersikap netral, dan 8% responden menjawab tidak setuju bahwa mereka khawatir apabila data mereka bocor. Dari data tersebut, dapat dilihat bahwa sebanyak 80% responden masuk dalam kriteria “khawatir” apabila datanya bocor.

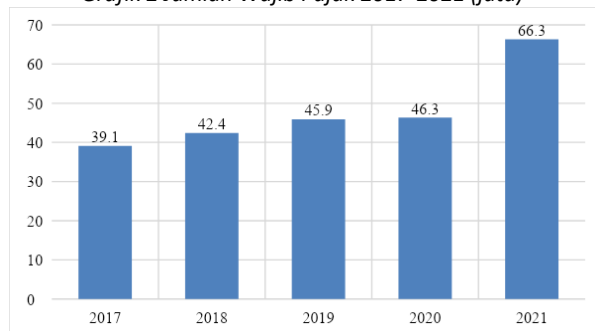
Grafik 1 Negara dengan Kasus Pembobolan Data Terbanyak di Dunia Kuartal 3 2022 (juta akun)



Sumber: Surfshark (2022). Telah diolah kembali.

Pada faktanya, kekhawatiran tersebut memang bukan tanpa sebab. Berdasarkan data yang diterbitkan oleh Surfshark sebagaimana Grafik 1, Indonesia menempati peringkat tiga sebagai negara dengan kasus pembobolan data terbanyak di dunia pada kuartal 3 tahun 2022 sebanyak 13,8 juta akun. Peringkat tersebut berada di bawah Rusia dan Perancis serta di atas Amerika Serikat dan Spanyol di urutan paling bawah. Tak hanya sampai di situ, terdapat 502 ribu data kredensial yang bocor dan didistribusikan melalui situs gelap di mana data-data tersebut merupakan data pengguna yang mengakses sejumlah situs pemerintahan, termasuk DJP (Ashari, 2022). Hal tersebut juga sejalan dengan apa yang diungkapkan oleh peneliti siber Singapura, DarkTracer, bahwa terdapat kebocoran data kredensial lebih dari 49 ribu situs pemerintah di seluruh dunia. Berdasarkan data tersebut pula, dari 10 situs pemerintah dengan kebocoran terbanyak, terdapat tiga situs pemerintah Indonesia salah satunya DJP dengan jumlah kebocoran sebanyak 17.585 data kredensial yang berasal dari situs [djponline.pajak.go.id](https://djponline.pajak.go.id) dan data wajib pajak dari [ereg.pajak.go.id](https://ereg.pajak.go.id) (Ashari, 2022).

Grafik 2 Jumlah Wajib Pajak 2017-2021 (juta)



Sumber: Direktorat Jenderal Pajak (2017, 2018, 2019, 2020, 2021). Telah diolah kembali.

Melihat banyaknya data yang bocor tersebut, kekhawatiran muncul kembali setelah melihat jumlah wajib pajak yang setiap tahun selalu meningkat sehingga meningkat pula jumlah data yang harus dilindungi sebagaimana Gambar 2 di atas. Berdasarkan gambar tersebut, jumlah wajib pajak dalam kurun waktu 2017 hingga 2021 meningkat dari 39,1 juta di tahun 2017 menjadi 66,3 juta di tahun 2023. Pengamat teknologi informasi dan media sosial Kun Arief Cahyantoro berpendapat bahwa apabila terjadi pembobolan SIN dengan sistem penyimpanan data yang terpusat, maka akan mengakibatkan hilangnya atau tercurinya seluruh data warga negara (Saptohotomo, 2022).

Untuk itu diperlukan solusi, salah satunya dengan penerapan teknologi *blockchain* dalam integrasi NIK dan NPWP. *Blockchain* memiliki karakteristik yang terdesentralisasi, di mana setiap data tersimpan dalam beberapa komputer (*nodes*) yang terpisah (Okazaki, 2018). Dengan penyimpanan data yang terdesentralisasi dapat mengurangi potensi penyalahgunaan data oleh pihak internal dan peran pihak ketiga dalam manajemen data untuk mencegah potensi intervensi dari luar sehingga data wajib pajak lebih terjaga (Maulana & Juliarto, 2021; Fathiyana *et al*, 2022).

#### 4.2. Benchmark Implementasi *Blockchain* di Negara Lain

Sebelum memilih kebijakan yang tepat terkait permasalahan yang diuraikan di atas, terdapat beberapa negara yang dapat dijadikan acuan untuk pengimplementasian *blockchain* dalam administrasi publik. Negara pertama adalah Estonia yang sejak tahun 2008 sudah menggunakan teknologi *blockchain* dalam urusan governansi publiknya (PWC, 2019). Estonia memulai membangun masyarakat digitalnya dari tahun 1997 melalui *e-governance system* dalam penyediaan layanan publik berupa e-Tax, x-Road, Digital ID, e-School, e-Voting, Mobile ID, e-Health, *blockchain*, e-residency, dan *data embassy*. Dengan demikian, 99% dari layanan publik di Estonia dilaksanakan sepenuhnya secara *online* (PWC, 2019). Estonia menggunakan teknologi *blockchain* pertama

kali untuk memastikan e-voting bagi warga negara. Melalui penyertaan teknologi *blockchain* dalam arsitektur digitalnya, Menurut Iglesia (2022), sistem *blockchain* yang telah digunakan di tingkat pemerintahan di Estonia didasarkan pada *private blockchain*, yang mencerminkan pendekatan terpusat (*centralized approach*) pada teknologi pencatatan terdistribusi. Pemerintah Estonia mengklaim telah memenuhi tujuan yang diharapkan dengan mengandalkan sifat kekekalan dan desentralisasi *blockchain*, warga negara dapat yakin bahwa informasi mereka tetap aman dan karenanya dapat mempercayai pemerintah (Iglesia, 2022).

Sistem *blockchain* yang digunakan oleh pemerintah Estonia adalah *Keyless Signature Infrastructure (KSI) Blockchain*. Melalui *KSI Blockchain*, data-data vital pemerintah seperti sektor kesehatan, properti, bisnis, dan pengadilan digital terproteksi secara maksimal dan meningkatkan kepercayaan publik (*public trust*) Estonia (PWC, 2019). Lebih daripada itu, *Single Identity Card* Estonia mencakupi *legal travel ID*, asuransi kesehatan nasional, identifikasi masuk ke rekening bank, tanda tangan digital, e-Voting, dan rekam medis (PWC, 2019). Dengan sistem terintegrasi dan diperkokoh dengan *blockchain* ini, Estonia menjadi negara yang memiliki sistem kartu identitas nasional yang paling maju di dunia (PWC, 2019).

Selanjutnya, melalui *Strategic Tenders Program*, *The Agency for Digital Italy* (AGID), *three-year 2019-2021 plan*, Italia mulai mengadopsi layanan *blockchain* dalam sistem administrasi publiknya (AGID, 2019). Kota Milan sebagai salah satu kota besar di Italia yang sudah menerapkan teknologi *blockchain* hanya memerlukan waktu sepuluh menit dalam pengurusan administrasi publik. Lebih lanjut lagi, 70 persen tahapan administrasi publik dapat dipangkas dan disederhanakan setelah penerapan teknologi ini (Coin Idol, 2019). Selain itu, ada 118 *startup* dari berbagai bidang bisnis di Italia yang mengadopsi *blockchain* untuk proteksi terbaik dalam aktivitas bisnisnya (PWC Italy, 2023). Pada tahun 2015, pemerintah Italia bersama dengan enam negara lainnya mencoba proyek EU Horizon untuk mengaplikasikan *information sharing* yang aman antara Kementerian Keuangan dan Kementerian Dalam Negeri melalui teknologi *blockchain*. Infrastruktur *blockchain* digunakan di sini untuk memastikan integritas dan kerahasiaan dalam pertukaran informasi antara Kementerian Keuangan dan Kepolisian Negara, khususnya dalam kaitannya dengan tempat tinggal dan status agen keamanan publik Italia. Hasilnya, pertukaran data antara *public cloud* dengan privat terjadi dengan aman dan bahkan sudah digunakan untuk sistem penggajian karyawan melalui pembaruan NoiPA (OECD, 2020).

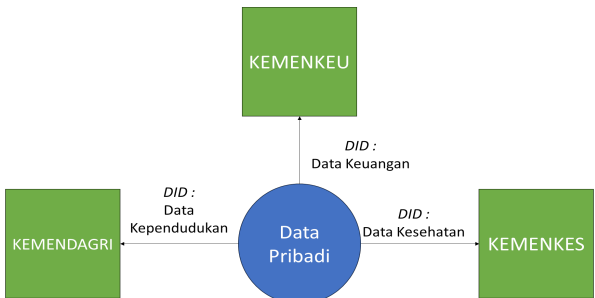
Berdasarkan pengalaman implementasi kedua negara tersebut, dapat diketahui bahwa penerapan *blockchain* dalam sistem administrasi publik dapat meningkatkan keamanan data secara masif. Selain itu, simplifikasi dan percepatan layanan publik pun menjadi dampak positif lain yang dihasilkan dari

pemanfaatan ini. Terlebih lagi, cara masyarakat berhubungan dengan pemerintah sedang berubah, didorong oleh kemungkinan yang timbul akibat teknologi-teknologi baru (PWC, 2019).

4.3. Merancang Perlindungan Data Wajib Pajak dengan Teknologi *Blockchain*

Mewujudkan pemadanan NIK-NPWP yang aman merupakan suatu keharusan mengingat data wajib pajak yang bersifat *credential*. Menurut Lembaga Studi dan Advokasi Masyarakat (ELSAM) pemadanan data NIK-NPWP menimbulkan potensi penyalahgunaan data sehingga diperlukan standar pengamanan yang ketat, salah satunya adalah dengan penerapan teknologi *blockchain* (Iskandar, 2021). Penerapan *blockchain* dengan *decentralized identity* (DID) dapat meningkatkan privasi dan keamanan data pribadi (Heister & Yuthas, 2021). DID merupakan sebuah bukti kepemilikan data pribadi dalam sistem *blockchain*, sehingga wajib pajak sebagai pemilik data dapat membatasi apa, kapan dan seberapa banyak yang dapat dibagikan kepada pihak lain (Heister & Yuthas, 2021). Dengan adanya hal tersebut dapat mencegah korelasi atau pemanfaatan data yang tidak dikehendaki (Heister & Yuthas, 2021).

Gambar 1 Alur *Decentralized Identity* (DID) dalam Pemadanan NIK-NPWP



Sumber: diolah oleh penulis.

Sebagai gambaran implementasi DID, dalam Gambar 1 wajib pajak dapat mengatur akses atas data pribadi mereka untuk layanan tertentu. Sebagai contoh dalam memanfaatkan pelayanan publik yang disediakan Kementerian Keuangan (Kemenkeu), wajib pajak dapat memanfaatkan DID untuk membatasi akses yang diberikan kepada Kemenkeu hanya atas data-data yang berhubungan dengan keuangan, seperti data perpajakan dan data terkait kepabeanan dan cukai. Dengan adanya DID dalam penerapan *blockchain* memungkinkan pengguna untuk menyimpan data mereka di luar dari *database* pihak lawan transaksi untuk mengurangi risiko pembobolan data secara masif (Heister & Yuthas, 2021).

Kemudian, data pada sistem *blockchain* disimpan dalam bentuk *block* beserta perubahannya yang dihubungkan dengan *hash* dan enkripsi pada setiap *block* data yang saling terhubung pada sistem *blockchain* sehingga membentuk ketergantungan (Maulana & Juliarto, 2021). Dengan data yang saling berhubungan, dapat mencegah orang lain untuk merusak data dan mempermudah DJP dalam melakukan pelacakan apabila terjadi pembobolan

data serta mempermudah proses pengawasan (Fathiyana *et al*, 2022; Okazaki, 2018). Penerapan *blockchain* dapat dilakukan melalui beberapa skema dengan karakteristik sebagaimana dijelaskan dalam Tabel 1.

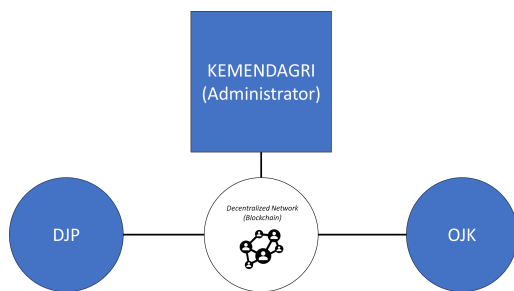
Tabel 1 Perbandingan Karakteristik *Blockchain*

| Karakteristik | Public Blockchain                                                     | Private Blockchain                                                               | Hybrid Blockchain                                                                   |
|---------------|-----------------------------------------------------------------------|----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Administrator | Semua pihak dapat menjadi administrator.                              | Hanya satu pihak yang dapat menjadi administrator                                | Hanya beberapa pihak tertentu yang dapat menjadi administrator.                     |
| Permissions   | Semua pihak dapat memiliki izin untuk mengakses dan mengedit data.    | Hanya beberapa pihak yang dapat memiliki izin untuk mengakses dan mengedit data. | Hanya beberapa pihak tertentu yang memiliki izin untuk mengakses dan mengedit data. |
| Accessibility | Semua pihak dapat memiliki akses tak terbatas terhadap data yang ada. | Hanya beberapa pihak yang memiliki akses tak terbatas terhadap data yang ada.    | Hanya beberapa pihak tertentu memiliki akses tak terbatas terhadap data yang ada.   |

Sumber: Laurence (2019). Telah diolah kembali

Berkaca pada keberhasilan Estonia dalam sistem administrasi publiknya, skema yang dapat diadopsi adalah *private blockchain* dengan memperhatikan aspek keamanan, kecepatan, dan skalabilitas. Dari sisi keamanan, *private blockchain* bekerja dalam sebuah sistem tertutup di mana hanya beberapa pihak yang memiliki akses informasi dalam *blockchain* (Paul *et al*, 2021). *Private blockchain* memiliki sistem keamanan yang mumpuni dan sering kali digunakan dalam mengelola identitas digital (Paul *et al*, 2021). Kemudian, dari sisi kecepatan, *private blockchain* menawarkan proses administrasi yang lebih cepat dan efisien karena jumlah *nodes* yang lebih sedikit memberikan proses administrasi lebih sederhana. Dari sisi skalabilitas, *private blockchain* fleksibel dalam kustomisasi dan penambahan *nodes* ke dalam jaringan *blockchain* (Paul *et al*, 2021). Dengan demikian, mengingat 3 aspek penting, yakni data wajib pajak yang bersifat *credential*, kebutuhan proses administrasi perpajakan yang cepat, dan kolaborasi antar lembaga, *private blockchain* menjadi pilihan tepat karena memenuhi aspek keamanan, kecepatan, dan skalabilitas dibandingkan dengan skema *blockchain* lainnya.

Gambar 2 Alur Penerapan Blockchain dalam Pemadanan NIK-NPWP



Sumber : diolah oleh penulis.

Dalam hal kolaborasi antar lembaga, Kementerian Dalam Negeri (Kemendagri) berperan sebagai administrator dalam sistem *blockchain* sebagaimana Gambar 2 di atas. Lebih lanjut, Kemendagri bertindak sebagai pemberi akses kepada lembaga-lembaga terkait dalam jaringan *blockchain*. Pemberian dan pencabutan akses dalam jaringan *blockchain* dapat dilakukan melalui *Smart Contract* (Stockburger *et al*, 2021). *Smart Contract* merupakan sebuah protokol komputer yang memungkinkan pelaksanaan kontrak yang aman tanpa adanya keterlibatan pihak ketiga (Okazaki, 2018). Dalam konteks pemadanan NIK-NPWP, Kemendagri dapat membatasi akses data yang dapat diakses DJP hanya pada data yang berhubungan dengan kewajiban perpajakan seseorang. Namun, dalam kondisi tertentu, DJP dapat meminta akses data keuangan terhadap wajib pajak tertentu melalui Otoritas Jasa Keuangan (OJK). Hal tersebut telah diatur pula dalam Peraturan Pengganti Undang-Undang Nomor 1 Tahun 2017 tentang Akses Informasi Keuangan untuk Kepentingan Perpajakan.

#### 4.4. Peluang dan Tantangan

Implementasi *blockchain* dalam pemadanan NIK-NPWP memiliki beberapa potensi dalam meningkatkan keamanan data. *Blockchain* memberikan lapisan proteksi dalam proses transaksi data dapat mengurangi potensi pemalsuan data, pencurian data dan manipulasi data (Dewi & Mangkono, 2022). Selain itu, dengan data yang saling terkoneksi satu *block* dengan yang lain, mempermudah DJP dalam melakukan pelacakan apabila terjadi pembobolan data dan mempermudah proses pengawasan (Fathiyana *et al*, 2022; Okazaki, 2018). Terakhir, *blockchain* memberikan kewenangan kepada wajib pajak sebagai pemilik data untuk mengelola data yang mereka miliki dengan adanya DID (Heister & Yuthas, 2021).

Di sisi lain, terdapat beberapa tantangan dalam implementasi *blockchain*, seperti kurangnya pengetahuan dan kesadaran akan teknologi *blockchain* yang masih cukup kompleks dan sulit untuk dimengerti (Mulaji & Roodt, 2021; Dewi & Mangkono, 2022). Lebih lanjut, implementasi *blockchain* perlu mempertimbangkan kesesuaian dengan kebijakan dan panduan yang berlaku terkait standar keamanan data (Mulaji & Roodt, 2021; Dewi & Mangkono, 2022).

Terakhir, penerapan teknologi *blockchain* memerlukan biaya yang cukup tinggi yang mencakup biaya inisiasi, seperti biaya pembangunan infrastruktur, biaya pengembangan kompetensi sumber daya manusia, dan biaya pemeliharaan serta pelatihan berkelanjutan yang dapat berdampak pada penerimaan (Mulaji & Roodt, 2021; Indraprakoso & Haripin, 2023).

## 5. KESIMPULAN DAN SARAN

Keamanan data wajib pajak menjadi hal vital dalam digitalisasi perpajakan. Apalagi, apabila melihat data yang ada, Indonesia menjadi salah satu negara yang sering kali mengalami pembobolan data. Hal tersebut pun juga dikhawatirkan dalam pemadanan NIK-NPWP. Dengan struktur data yang saling terkoneksi dan tersebar dalam beberapa *nodes*, sistem *blockchain* dapat memberikan proteksi keamanan data dan mempermudah pengawasan DJP dalam pemadanan NIK-NPWP. Ditambah lagi, dengan penerapan DID dalam sistem *blockchain* yang memberikan kewenangan pengelolaan data kepada wajib pajak sebagai pemilik data, dapat mencegah potensi pemanfaatan data yang tidak dikehendaki. Di samping keunggulan tersebut, pemerintah perlu memperhatikan kompleksitas *blockchain* yang dinilai cukup rumit, kesesuaian dengan standarisasi kebijakan, dan biaya yang cukup tinggi. Oleh karena itu, penerapan teknologi *blockchain* diharapkan dapat memberikan proteksi maksimal untuk melindungi data pribadi wajib pajak dalam rangka pemadanan NIK-NPWP di era *Society 5.0* yang bergantung pada teknologi ini.

## 6. IMPLIKASI DAN KETERBATASAN

Hasil kajian ini dapat berimplikasi untuk dijadikan acuan kepada pemerintah dalam rangka penentuan arah kebijakan. Terutama, kebijakan yang berkaitan dengan regulasi terkait perlindungan data wajib pajak di era *Society 5.0* di mana antara manusia dengan dunia digital sudah menjadi bagian yang tidak terpisahkan. Penulis menyadari terdapat keterbatasan dalam kajian ini karena menganalisis data dari jurnal-jurnal yang tersedia pada waktu penulisan. Oleh karena itu, penulis menyarankan untuk dilakukan riset dan kajian lanjutan di masa mendatang sehingga kajian ini dapat disesuaikan dengan perkembangan yang ada. Selain itu, penulis pun menyarankan agar ada penelitian empiris terkait keamanan data setelah diberlakukannya *blockchain* pada pemadanan NIK-NPWP ketika sudah diberlakukan nanti.

## DAFTAR PUSTAKA (REFERENCES)

- AGID. (2019). *2019 - 2021 Three-Year Plan for IT in the Public Administration*. Agenzia per l'Italia digitale.  
[https://www.agid.gov.it/sites/default/files/repository\\_files/three\\_year\\_plan\\_for\\_it\\_in\\_public\\_administration\\_2019-2021.pdf](https://www.agid.gov.it/sites/default/files/repository_files/three_year_plan_for_it_in_public_administration_2019-2021.pdf)
- Angga, D., Priyo, S., & F, H. (2019). *Hidup Kian Repot dengan Banyak Kartu : Okezone Economy*.

- <https://economy.okezone.com/read/2019/01/21/320/2007119/hidup-kian-repot-dengan-banyak-kartu?page=3>
- Ashari, M. (2022). *Belajar Dari Kebocoran Data Kredensial: Data Yang Paling Berharga adalah Data Pribadi*. <https://www.djkn.kemenkeu.go.id/artikel/baca/14838/Belajar-Dari-Kebocoran-Data-Kredensial-Data-Yang-Paling-Berharga-adalah-Data-Pribadi.html>
- BPS. (2023). *Realisasi Pendapatan Negara (Milyar Rupiah), 2021-2023*. <https://www.bps.go.id/indicator/13/1070/1/realisasi-pendapatan-negara.html>
- Coin Idol. (2019). *Lombardy region adopts blockchain in public administration*. Latest Bitcoin News. <https://coindol.com/lombardy-region-adopts/>
- Dewi, R., & Mangkono, S. (2022). Opportunities and Challenges of Utilizing Blockchain Technology in Marketing Management: A Case Study on the Financial Industry: A UTAUT Theory Approach. *International Journal of Artificial Intelligence Research*, ISSN(1), 2022. <http://ijair.id>
- Direktorat Jenderal Pajak. (n.d.). *Reformasi Perpajakan*. Retrieved May 26, 2023, from <https://pajak.go.id/id/reformasi-perpajakan>
- Direktorat Jenderal Pajak. (2017). *Transparansi Membangun Negeri : Annual Report DJP 2017*. 226. [www.pajak.go.id](http://www.pajak.go.id)
- Direktorat Jenderal Pajak. (2018). *Sinergi Menuju Kemandirian Ekonomi Nasional : Annual Report 2018*. 1–250. <https://www.pajak.go.id/sites/default/files/2019-11/LaporanTahunanDJP2018-bahasa-Indonesia.pdf>
- Direktorat Jenderal Pajak. (2019). *Peningkatan Kapasitas Secara Berkesinambungan : Annual Report DJP 2019. December*, i–140. <https://www.speakindonesia.org/peningkatan-kapasitas/>
- Direktorat Jenderal Pajak. (2020). *Konsisten Mengoptimalkan Peluang di Masa Menantang: Annual Report 2020*. 13.
- Direktorat Jenderal Pajak. (2021). *Laporan Tahun 2021: Berkontribusi Bersama Dalam Pemulihan Ekonomi Nasional*.
- FIA UI. (2023). *Penggunaan NIK sebagai NPWP Munculkan Potensi Masalah Optimalisasi Penerimaan Negara – Fakultas Ilmu Administrasi UI*. <https://fia.ui.ac.id/penggunaan-nik-sebagai-npwp-munculkan-potensi-masalah-optimalisasi-penerimaan-negara/>
- Firman Maulana, G., & Juliarto, A. (2021). THE IMPLEMENTATION OF BLOCKCHAIN IN INTERNATIONAL TRADE. *DIPONEGORO JOURNAL OF ACCOUNTING*, 10(4), 1–8. <http://ejournal-s1.undip.ac.id/index.php/accounting>
- Fukuyama, M. (2018). *Society 5.0: Aiming for a New Human-Centered Society*. *Japan SPOTLIGHT*.
- Heister, S., & Yuthas, K. (n.d.). *How Blockchain and AI Enable Personal Data Privacy and Support Cybersecurity*. [www.intechopen.com](http://www.intechopen.com)
- Iglesia, A. D. (2022). *The blockchain clash in the Estonian government*. P2P Models. <https://p2pmodels.eu/decentralizing-what-when-blockchains-perspectives-clash/>
- Indraprakoso, D. (2023). *Eksplorasi Potensi Penggunaan Blockchain Dalam Optimalisasi Manajemen Pelabuhan di Indonesia: Tinjauan Literatur*. *Sanskara Manajemen Dan Bisnis*, 01(03), 140–160. <https://doi.org/10.58812/smb.v1.i03>
- Keidanren. (2018). *Society 5.0 Co-Creating The Future*.
- Kementerian Keuangan. (2022). *Kementerian Keuangan Gelar Pajak Bertutur 2022*. <https://www.kemenkeu.go.id/informasi-publik/publikasi/berita-utama/Kementerian-Kuangan-Gelar-Pajak-Bertutur-2022-%281%29>
- Mulaji, S. S. M., & Roodt, S. S. (2021). The Practicality of Adopting Blockchain-Based Distributed Identity Management in Organisations: A Meta-Synthesis. *Security and Communication Networks*, 2021. <https://doi.org/10.1155/2021/9910078>
- OECD. (2020). *Blockchain for SMEs and entrepreneurs in Italy*. [oecd.org](http://oecd.org).
- Okazaki, Y. (2018). *Unveiling the Potential of Blockchain for Customs*. [www.wcoomd.org](http://www.wcoomd.org).
- Panait, A. E., Olimid, R. F., & Stefanescu, A. (2020). Identity management on blockchain – Privacy and security aspects. *Proceedings of the Romanian Academy Series A - Mathematics Physics Technical Sciences Information Science*, 21(1), 45–52.
- Paul, P. K., Aithal, P. S., Saavedra, R., & Ghosh, S. (2021). *Blockchain Technology and Its Types-A Short Review*. <https://ssrn.com/abstract=4050933>
- PWC. (2019). *Estonia – the Digital Republic Secured by Blockchain*. PwC: Audit and assurance, consulting and tax services. <https://www.pwc.com/gx/en/services/legal/tch/assets/estonia-the-digital-republic-secured-by-blockchain.pdf>
- PWC Italy. (2023). *The Blockchain Ecosystem in Italy*. PwC: Audit and assurance, consulting and tax services. <https://www.pwc.com/it/it/publications/doc/s/pwc-blockchain-ecosystem-italy.pdf>
- Rosdiana, H., & Irianto, E. S. (2014). *Pengantar Ilmu Pajak : Kebijakan dan Implementasi di Indonesia*. Jakarta : PT Raja Grafindo Persada.
- Saptohutomo, A. (2022). *Pakar Ungkap Kelemahan “Single Identity Number” Usulan Bamsoet*. <https://nasional.kompas.com/read/2022/04/25/06010021/pakar-ungkap-kelemahan-single-identity-number-usulan-bamsoet>

- Shenkoya, T., & Kim, E. (2023). Sustainability in Higher Education: Digital Transformation of the Fourth Industrial Revolution and Its Impact on Open Knowledge. *Sustainability (Switzerland)*, 15(3). <https://doi.org/10.3390/su15032473>
- Stockburger, L., Kokosioulis, G., Mukkamala, A., Mukkamala, R. R., & Avital, M. (2021). Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation. *Blockchain: Research and Applications*, 2(2). <https://doi.org/10.1016/j.bcra.2021.100014>
- Sugiono, S. (2021). Peran E-Government dalam Membangun *Society 5.0*: Tinjauan Konseptual terhadap Aspek Keberlanjutan Ekonomi, Sosial, dan Lingkungan. *Matra Pembaruan*, 5(2), 115–125. <https://doi.org/10.21787/mp.5.2.2021.115-125>
- Surfshark. (2022). *Data breach statistics by country 2022*’Q3. <https://surfshark.com/blog/data-breach-statistics-2022-q3>
- Suryaputra, V. (2023). *Analisis Persepsi Masyarakat Kota Bandung Terkait Prinsip Kesederhanaan dan Kemanfaatan Pengintegrasian NIK dan NPWP dalam Mewujudkan Single Identity Number di Indonesia*. 7, 21507–21516.
- Tauperta Siregar. (2017). *PENGARUH PENETAPAN single identity number DALAM RANGKA PEMENUHAN KEPATUHAN KEWAJIBAN PERPAJAKAN* | *Jurnal Akuntansi*. INSTITUT BISNIS DAN INFORMATIKA KWI KIAN GIE. <https://jurnal.kwikkiangie.ac.id/index.php/JA/article/view/388/191>
- Tiara Laurence. (2019). *Introduction to Blockchain Technology: The many faces of blockchain technology in the 21st century* (Vol. 1). Van Haren Publishing.
- Tobing, E. G. L., & Kusmono, K. (2022). Modernisasi Administrasi Perpajakan: NIK Menjadi NPWP. *JURNAL PAJAK INDONESIA (Indonesian Tax Review)*, 6(2), 183–193. <https://doi.org/10.31092/jpi.v6i2.1674>
- Twesige, D., Gsheja, F., Hategikimana, U., Ndikubwimana, P., Mwiza, Y., & Hitayezu, I. (2020). Smart Taxation (4Taxation): Effect of Fourth Industrial Revolution (4IR) on tax compliance in Rwanda. *Journal of Business and Administrative Studies*, 12(1), 1–27.
- Waluyo, T. (2020). Pemeriksaan Terhadap Wajib Pajak yang Tidak Menyampaikan SPT, Ketentuan dan Pemilihannya sesuai SE-15/PJ/2018. *Simposium Nasional Keuangan Negara 2020*