



POTENSI KEBOCORAN DAN PELINDUNGAN HUKUM DATA PRIBADI PADA *SMART CONTRACT* DALAM TRANSAKSI JUAL BELI ASET KRIPTO (Studi Kasus pada Aplikasi Pluang)

Swarnajhoti Sangkar* dan R.A. Antari Innaka Turingsih

Fakultas Hukum, Universitas Gadjah Mada,
Jl. Sosio Justicia No. 1, Bulaksumur, Kab. Sleman, D.I. Yogyakarta, 55281

Abstract

This research aims to seek knowledge about the potential of personal data leakage and its legal protection for users and parties involved in smart contracts on crypto assets transactions. The increasing use of blockchain-based smart contracts in crypto asset trading, despite lacking specific regulation, raises urgent concerns about how personal data is processed and protected within these transactions. The research method that the authors used is a combination of normative and empirical legal research. The conclusions of this research are: First, there are still some potentials for personal data leakage from smart contracts. Second, there is no specific regulation governing smart contracts and the protection of personal data on smart contracts, but we still can find internal and external legal protection for the parties in various legal instruments in Indonesia. Third, Pluang Application collaborates with third parties, namely liquidity providers, in organizing crypto asset transactions, so these third parties are the ones who use smart contracts.

Keywords: *Potential of Personal Data Leakage, Personal Data Protection, Smart Contract, Crypto Asset.*

Abstrak

Penelitian ini bertujuan untuk memperoleh pengetahuan mengenai potensi kebocoran data pribadi dan perlindungan hukumnya bagi pengguna dan para pihak yang terlibat pada perjanjian jenis *smart contract* dalam transaksi jual beli aset kripto. Meningkatnya penggunaan *smart contract* berbasis *blockchain* dalam transaksi aset kripto di Indonesia, yang belum diimbangi dengan regulasi khusus, menimbulkan urgensi terkait perlindungan data pribadi dalam transaksi tersebut. Metode penelitian yang penulis gunakan adalah gabungan antara metode penelitian hukum normatif dan penelitian hukum empiris. Kesimpulan dari hasil penelitian ini adalah: Pertama, masih terdapat beberapa potensi kebocoran data pribadi yang berasal dari *smart contract*. Kedua, belum ada pengaturan hukum yang spesifik mengatur mengenai *smart contract* dan perlindungan data pribadinya namun perlindungan hukum secara internal dan eksternal bagi para pihak dapat dilihat dalam berbagai instrumen hukum di Indonesia. Ketiga, Aplikasi Pluang bekerja sama dengan Pihak Ketiga yaitu *liquidity provider* dalam penyelenggaraan transaksi jual beli aset kripto, sehingga yang menggunakan *smart contract* adalah pihak ketiga tersebut.

Kata Kunci: Potensi Kebocoran Data Pribadi, Pelindungan Data Pribadi, *Smart Contract*, Aset Kripto.

* Alamat korespondensi: swarnaajhoti@mail.ugm.ac.id

A. PENDAHULUAN

Perkembangan teknologi telah menciptakan terobosan baru dalam dunia perjanjian yaitu dengan munculnya kontrak pintar (*smart contract*). Konsep dari *smart contract* sendiri diperkenalkan pertama kali pada tahun 1994 oleh Nick Szabo, seorang sarjana hukum, ilmuwan komputer dan ahli kriptografi. Nick Szabo mendefinisikan *smart contract* sebagai berikut.

“A *smart contract* is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart-contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimise exceptions both malicious and accidental, and minimise the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs.”¹

Konsep dari *smart contract* sendiri terinspirasi dari cara kerja *vending machine* (mesin jual otomatis). Apabila mesin bekerja dengan baik dan uang dimasukkan kedalam mesin, maka kontrak untuk penjualan akan dieksekusi secara otomatis.² Hadirnya konsep *smart contract* yang sederhana ini diharapkan dapat menghemat biaya dan waktu karena tidak perlu mengeluarkan biaya yang besar untuk jasa pihak ketiga seperti pengacara atau agen khusus lainnya, serta meminimalisir kemungkinan adanya kerugian yang timbul dari penipuan. Walaupun konsepnya terdengar sederhana, *smart contract* sendiri baru berhasil diterapkan pada tahun 2008 bersamaan dengan munculnya mata uang digital *Bitcoin*. Berkaca dari keberhasilan tersebut, berbicara tentang *smart contract* tidak dapat dipisahkan dengan pembahasan mengenai teknologi *blockchain*. *Blockchain* itu sendiri pada dasarnya adalah *database* catatan yang didistribusikan, atau buku besar publik dari semua transaksi atau peristiwa digital yang telah dieksekusi dan dibagikan di antara pihak-pihak yang berpartisipasi.³ Fitur penting yang berkaitan dengan *blockchain* adalah desentralisasi (*decentralization*), tidak dapat diubah-ubah (*immutability*), dan tautan kriptografi (*cryptographic link*).⁴ Ketiga fitur inilah yang membuat teknologi *blockchain* dapat beroperasi

¹ Maria G. Vigliotti, "What Do We Mean by Smart Contracts? Open Challenges in Smart Contracts," *Frontiers in Blockchain* 3 (2021): 2, <https://doi.org/10.3389/fbloc.2020.553671>.

² Max Raskin, "The Law and Legality of Smart Contracts," *Georgetown Law Technology Review* 1, no. 2 (2017): 36, <https://heinonline.org/HOL/License>.

³ Chandra Lukita, "Penerapan Sistem Pendataan Hak Cipta Content Menggunakan Blockchain," *ADI Bisnis Digital Interdisiplin Jurnal* 1, no. 2 (Desember 2020): 41, <https://doi.org/10.34306/abdi.v1i2.120>.

⁴ Tharaka Hewa, Mika Ylianttila, dan Madhusanka Liyanage, "Survey on Blockchain Based Smart Contracts: Applications, Opportunities and Challenges," *Journal of Network and Computer Applications* 177 (2021): 1, <https://doi.org/10.1016/J.JNCA.2020.102857>.

dengan cepat, aman, dan transparan sehingga menjadi kunci keberhasilan dari penerapan konsep *smart contract*.

Terobosan yang dipersembahkan oleh teknologi *blockchain* dan *smart contract* telah membawa banyak kemudahan khususnya dalam perdagangan jual beli aset kripto (*crypto asset*). Aset Kripto adalah komoditi tidak berwujud yang berbentuk digital, menggunakan kriptografi, jaringan informasi teknologi, dan buku besar yang terdistribusi untuk mengatur penciptaan unit baru, memverifikasi transaksi, dan mengamankan transaksi tanpa campur tangan pihak lain.⁵ Singkatnya aset kripto adalah mata uang digital yang dapat diperdagangkan secara virtual dengan menggunakan teknologi *blockchain*. Di Indonesia sendiri, jumlah pelanggan aset kripto per akhir Juni 2022 telah menembus angka 15,1 juta. Jumlah itu naik 3,9 juta selama semester I, dari periode akhir tahun 2021 yang mencapai 11,2 juta.⁶ Transaksi jual beli aset kripto telah menjadi salah satu sumber pendapatan dan pilihan investasi yang banyak digemari masyarakat global terutama generasi milenial karena proses transaksinya yang mudah, aman, cepat, dan memiliki potensi keuntungan yang besar.

Tingginya minat dan atensi dari masyarakat terhadap transaksi jual beli aset kripto juga secara tidak langsung telah membawa dampak positif seperti meningkatnya literasi keuangan dan literasi digital masyarakat. Namun, bagai dua sisi koin, dibalik kemajuan teknologi *blockchain* yang menjadi basis dari *smart contract* dan tulang punggung dari perdagangan aset kripto, masih terdapat kemungkinan dari adanya penyalahgunaan informasi dan masalah teknis. Perlu menjadi perhatian bahwa sistem *blockchain* terbagi menjadi 3 (tiga) jenis yaitu *private blockchain*, *consortium blockchain*, dan *public blockchain*. Perbedaan antara ketiga jenis sistem *blockchain* ini terletak pada kepemilikan akses terhadap sistem. Pada *private* dan *consortium blockchain*, akses dan kendali terhadap sistem hanya dimiliki oleh satu dan/atau beberapa orang saja, sedangkan pada *public blockchain*, siapa saja memiliki akses terhadap sistem dan dapat melihat data transaksi. Hampir seluruh *platform* perdagangan aset kripto bergerak dengan menggunakan sistem *public blockchain*. Terlepas dari kemudahan yang diberikan sistem *public blockchain* untuk pergerakan perdagangan aset kripto, sebagian besar masalah hukum (termasuk yang privasi) muncul sehubungan dengan *public blockchain*.⁷ Sulit

⁵ Peraturan Badan Pengawas Perdagangan Berjangka Komoditi Nomor 8 Tahun 2021 tentang Pendoman Penyelenggaraan Perdagangan Pasar Fisik Aset Kripto (Crypto Asset) Di Bursa Berjangka, Pasal 1, butir 7.

⁶ Lona Olivia, "Jumlah Pelanggan Tumbuh Lebih Banyak, Akankah Transaksi Kripto Bisa Salip Saham?," Investor.id, diakses 13 September 2022, <https://investor.id/market-and-corporate/300115/jumlah-pelanggan-tumbuh-lebih-banyak-akankah-transaksi-kripto-bisa-salip-saham>.

⁷ E. Mik, "Blockchains: A Technology for Decentralized Marketplaces," dalam The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms, ed. L.A. DiMatteo, M. Cannarsa, dan C. Poncibò (Cambridge: Cambridge University Press, 2020), 80.

untuk dapat menjaga privasi atau kerahasiaan isi perjanjian dalam *smart contract* pada *public blockchain*, karena *smart contract* yang telah dimasukkan ke dalam sistem *blockchain* tersebar ke seluruh jaringan dan dapat dilihat oleh seluruh orang. Walaupun isi *smart contract* disajikan dalam bentuk kode atau *pseudonym*, *smart contract* belum mampu untuk merahasiakan semua isi perjanjian yang ada di dalam kontrak. Hal ini dikarenakan terdapat beberapa perusahaan yang menawarkan layanan untuk mengidentifikasi pengguna dengan menggunakan *public keys*, transaksi *blockchain*, dan data lainnya yang tersedia.⁸ Selain dengan adanya perusahaan yang menawarkan jasa untuk mengidentifikasi pengguna menggunakan *public keys*, beberapa peristiwa dan penelitian menunjukkan bahwa masih memungkinkan untuk melakukan deanomisasi (*deanonymize*) pada sebuah transaksi dan mengungkapkan identitas di balik nama samaran.⁹ Pada penulisan yang dilakukan oleh Alex Biryukov dan rekan, disebutkan bahwa Koshy dan para rekannya berhasil untuk melakukan deanomiasi terhadap 1162 nama samaran dalam jangka waktu 5 (lima) bulan, namun pada percobaan ini tidak semua transaksi berhasil untuk tidak dianonimkan dan metode yang digunakan hanya memungkinkan untuk mendapat alamat IP.¹⁰ Kendati demikian, alamat IP (*internet protocol*) sudah tergolong ke dalam jenis data pribadi dan dapat disalahgunakan untuk mengunduh konten ilegal, mengetahui lokasi pemilik alamat IP, dan masih banyak lagi.

Ari Juels dan rekan, dengan mengadopsi konsep yang dikemukakan Kosba, menyatakan bahwa *blockchain* dapat dipercayakan untuk ketepatan atau kebenarannya namun tidak untuk privasi.¹¹ Hal ini tentu menimbulkan banyak pertanyaan terkait keamanan privasi terutama data pribadi pengguna, karena hampir semua perdagangan aset kripto bergerak pada sistem *public blockchain*. Tidak hanya dari teknologi *blockchain* dan *smart contract*, kasus kebocoran data pribadi yang berasal dari aplikasi jual beli aset kripto pun telah beberapa kali terjadi. Pada tahun 2020, *BTC Markets*, salah satu *platform* perdagangan aset kripto terbesar di Australia pernah dengan tidak sengaja mengekspos 270.000 data pribadi pengguna berupa nama dan alamat *e-mail*, walaupun kebocoran data tidak meliputi kata sandi atau data lainnya, alamat *e-*

⁸ Pritesh Shah et al., "Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies," (Laporan, Davis Polk & Wardwell LLP, 2019), 4, [https://www.davispolk.com/sites/default/files/blockchain technology data privacy issues and potential mitigation strategies_w-021-8235.pdf](https://www.davispolk.com/sites/default/files/blockchain%20technology%20data%20privacy%20issues%20and%20potential%20mitigation%20strategies_w-021-8235.pdf).

⁹ Murat Osmanoglu dan Ali Aydin Selçuk, "Privacy in Blockchain Systems," *Turkish Journal of Electrical Engineering and Computer Sciences* 30, no. 2 (Februari 2022): 344, <https://doi.org/10.3906/elk-2105-183>.

¹⁰ Alex Biryukov, Dmitry Khovratovich, dan Ivan Pustogarov, "Deanonymisation of Clients in Bitcoin P2P Network," dalam *Proceedings of the ACM Conference on Computer and Communications Security* (2014): 1, <https://doi.org/10.1145/2660267.2660379>.

¹¹ Ari Juels, Ahmed Kosba, dan Elaine Shi, "The Ring of Gyges: Investigating the Future of Criminal Smart Contracts," dalam *Proceedings of the ACM Conference on Computer and Communications Security* (2016): 5, <https://doi.org/10.1145/2976749.2978362>.

mail dapat menjadi target untuk *phishing attacks*.¹² Adanya kasus kebocoran data pribadi seperti ini tentu mengkhawatirkan, terlebih lagi dengan angka pengguna dan penyelenggara aplikasi investasi penyedia aset kripto di Indonesia kian bertambah setiap harinya. Hadirnya UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi telah memberikan payung hukum baru untuk data pribadi masyarakat, namun tetap timbul beberapa pertanyaan yang berkaitan dengan pelindungan data pribadi pada *smart contract* yaitu apakah UU No. 27 Tahun 2022 telah turut mengakomodir data yang disetorkan pada *smart contract*. Ketentuan *a quo* belum secara khusus mengatur pelindungan data dalam konteks *smart contract* dan *blockchain*. Hal ini menjadi penting karena karakteristik teknologi berikut, seperti keterbukaan sistem dan sulitnya penghapusan data, menciptakan tantangan hukum baru. Di sinilah muncul kesenjangan antara ketentuan normatif yang berlaku dan realitas teknis yang berkembang, yang belum sepenuhnya diakomodir oleh hukum positif di Indonesia. Mengingat, teknologi *blockchain* dan *smart contract* akan banyak dimanfaatkan pada kemudian hari dan belum ada pengaturan yang secara spesifik mengatur kedua teknologi tersebut, maka penting untuk mengetahui cara untuk memitigasi potensi kebocoran data pribadi dan pelindungan hukum yang tersedia.

Berkaitan dengan hal tersebut, penulis telah melakukan penelitian normatif dan empiris yaitu dengan wawancara serta pengamatan pada salah satu aplikasi investasi daring, yaitu Aplikasi Pluang, yang turut menyediakan layanan jual beli aset kripto dan telah digunakan oleh lebih dari 8.8 juta pengguna¹³ di Indonesia.

Rumusan masalah yang dibahas dalam penelitian ini adalah bagaimana dengan potensi kebocoran data pribadi dan pelindungan hukum bagi para pihak pada perjanjian jenis *smart contract* yang digunakan Aplikasi Pluang berdasarkan hukum positif Indonesia?

¹² "Australian Crypto Exchange Exposes Personal Data of 270K Users," CoinDesk, 2 Desember 2020, <https://www.coindesk.com/business/2020/12/02/australian-crypto-exchange-exposes-personal-data-of-270k-users/>.

¹³ "Pluang, Platform Investasi Multi Aset Paling Inovatif," CNBC Indonesia, 12 Desember 2022, <https://www.cnbcindonesia.com/market/20221212195050-17-396226/pluang-platform-investasi-multi-aset-paling-inovatif>.

B. POTENSI KEBOCORAN DATA PRIBADI DAN PELINDUNGAN HUKUM PADA *SMART CONTRACT*

1. Hasil Penelitian Mengenai Aplikasi Pluang

Aplikasi Pluang merupakan salah satu aplikasi investasi yang telah mengantongi izin dari Kementerian Komunikasi dan Informatika sebagai Penyelenggara Sistem Elektronik, serta bekerja sama dengan PT Bumi Santosa Cemerlang (BSC) sebagai Calon Pedagang Fisik Aset Kripto yang diawasi oleh BAPPEBTI. Dalam operasionalnya, Pluang berperan sebagai platform perantara atau bursa bagi pengguna dalam melakukan jual beli aset kripto,¹⁴ sementara proses transaksi menggunakan smart contract sepenuhnya dijalankan oleh pihak ketiga, yaitu *liquidity provider* yang bekerja sama dengan PT BSC. Dengan demikian, Pluang sendiri tidak membangun sistem berbasis *blockchain*, melainkan menyerahkannya kepada pihak *liquidity provider* yang mengelola *liquidity pools* dan mengeksekusi smart contract. *Liquidity provider* adalah penyedia likuiditas dalam *liquidity pools* (kumpulan aset kripto yang terkunci dalam teknologi smart contract). Dengan kata lain, *liquidity provider* adalah investor (baik perorangan atau perusahaan) yang mendanai *liquidity pools* (kumpulan likuiditas) dengan aset kripto yang dimilikinya untuk memfasilitasi perdagangan di platform (seperti Aplikasi Pluang) dan mendapatkan penghasilan pasif dari setorannya.

Pada pelaksanaannya, PT BSC bekerja sama dengan Fireblocks sebagai lembaga kustodian yang menyimpan aset-aset kripto pengguna.¹⁵ Pada *white paper* yang dipublikasikan oleh Fireblocks, disebutkan bahwa Fireblocks sendiri menciptakan *multi-layer security matrix* yang meliputi MPC, Intel SGX, Fireblocks *signature policy engine* dan otentikasi alamat setoran (*a deposit address authentication*) untuk membangun sistem yang paling sulit ditembus di pasar.¹⁶ Selain sistem keamanan yang berlapis-lapis tersebut, Fireblock juga menyimpan aset kripto pengguna secara *one-to-one* pada *warm wallet*. *Warm wallet* merupakan gabungan antara kecepatan transaksi pada *hot wallet* namun dengan tingkat keamanan yang mirip dengan *cold wallet*. *Keys* yang ada pada *warm wallet* disimpan secara *online* dan transaksi dapat dibuat secara otomatis, akan tetapi *warm wallet* masih membutuhkan keterlibatan manusia untuk menandatangani transaksi dan mengirimkannya ke *blockchain*. Walaupun Fireblocks menawarkan tingkat

¹⁴ Wyndo Buwana (Product Manager Lead for Crypto, Aplikasi Pluang), wawancara dengan penulis, 1 Maret 2023, secara daring.

¹⁵ Pluang, "Mengapa Harga Aset Kripto Pluang Berbeda Dari Platform Lain? Simak Penjelasannya!," Pluang Blog, diakses 9 Maret 2023, <https://pluang.com/id/blog/resource/perbedaan-harga-aset-kripto-pluang>.

¹⁶ Fireblocks, "Fireblock' Multi-Layer Philosophy for Securing Digital Assets," n.d., 18.

keamanan yang tinggi, masih ada potensi dari kebocoran data pribadi karena apabila *warm wallet* tidak diamankan dengan baik atau memiliki pengawasan yang lemah maka ia juga rentan diserang para *hacker* untuk mencuri identitas pengguna, *private keys*, dan data sensitif lainnya.

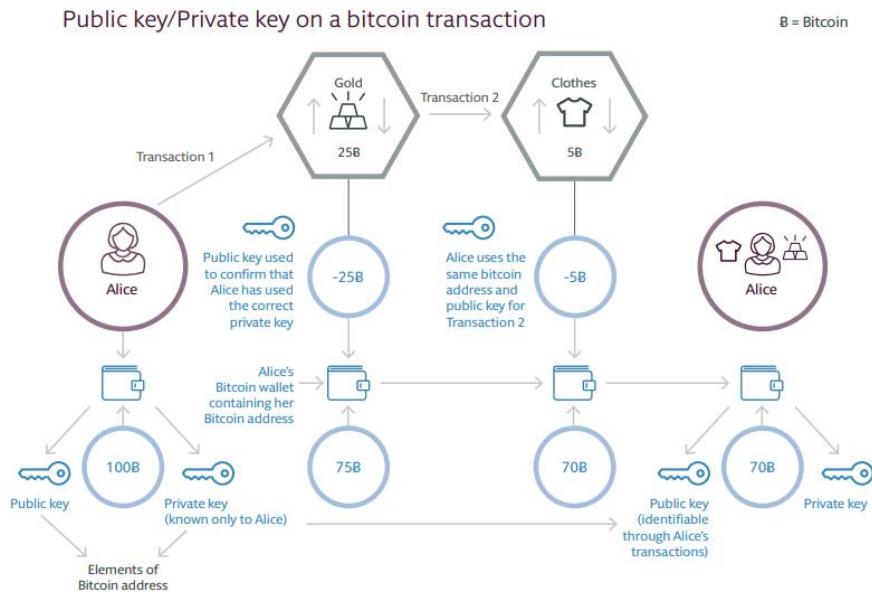
2. Potensi Kebocoran Data Pribadi pada *Smart Contract*

Berbeda dengan perjanjian konvensional yang mengutamakan privasi dari pihak-pihak dalam perjanjian, isi dari *smart contract* dapat dilihat publik pada teknologi *blockchain*, contohnya adalah *smart contract* yang tersaji pada laman *blockchain etherscan.io*. Walaupun isi dari *smart contract* ditampilkan dalam bentuk bahasa pemrograman komputer, masih terdapat celah dimana isi dari *smart contract* disalahgunakan oleh pihak-pihak tertentu. Berikut adalah beberapa potensi kebocoran data pribadi yang dapat terjadi pada *smart contract*:

- a) Potensi kebocoran data pribadi pada *smart contract* bisa terjadi ketika pengguna memberikan informasi pribadi pada *smart contract* yang kemudian disimpan secara permanen dalam *blockchain*. Meskipun *blockchain* dikenal memiliki keamanan yang kuat, namun data yang disimpan di dalam *blockchain* bersifat publik dan tidak dapat dihapus. Jika data pribadi disimpan di dalam *smart contract*, maka data tersebut dapat dilihat oleh siapa saja yang memiliki akses ke *blockchain*.
- b) Data yang disetorkan dalam *smart contract* berbentuk *pseudonym* yaitu sebuah samaran sehingga tidak menunjukkan identitas para pihak secara eksplisit. Kendati demikian, data berbentuk *pseudonym* masih dapat dideanonimisasi sehingga menunjukkan identitas asli dari nama samaran tersebut.
- c) Sebuah *private key* adalah kode rahasia yang memberikan akses ke *wallet* yang terhubung dengan *blockchain*. Jika seseorang mendapatkan *private key* pengguna, maka mereka dapat mengakses seluruh aset kripto dan informasi pribadi lainnya yang terkait dengan akun pengguna.
- d) Peretas/*hacker* dapat memanipulasi teknologi *blockchain* dengan menggunakan “*hard fork*” untuk membuat salinan dari *blockchain* yang pada

dasarnya dapat memungkinkan pihak-pihak yang tidak bertanggungjawab untuk memanipulasi data dan mencuri informasi.¹⁷

- e) *Public key* dari pengguna dapat diidentifikasi jika terdapat beberapa transaksi dari satu *public key*, sehingga memungkinkan untuk memperoleh identitas asli dari pengguna. Contoh dari *public key* yang dapat diidentifikasi dapat dilihat pada diagram di bawah ini:¹⁸



Alice sebagai pembeli mempunyai *private key* (hanya dapat dilihat Alice) dan *public key* yang dapat dilihat publik. Setiap ada transaksi pembelian, *public key* Alice muncul untuk memastikan bahwa pembelian nantinya akan dikirimkan ke orang yang benar yaitu Alice. Namun *public key* ini tidak berubah-ubah dan dapat digunakan berulang kali seperti username sehingga nantinya *public key* Alice tetap dapat teridentifikasi melalui transaksi-transaksi yang dilakukannya. Walaupun memang tidak menunjukkan identitas asli Alice, *public key* dapat digunakan untuk mengambil informasi dari pemilik *public key* seperti baik karena dipegang oleh penyedia layanan atau karena seseorang dapat menghubungkan kunci *public key* ke individu atau organisasi, (misalnya, melalui alamat IP mereka atau koneksinya dengan situs web).¹⁹

Potensi deanomisasi data dalam *smart contract* menunjukkan bahwa data *pseudonym* tetap rentan terhadap pelanggaran privasi, terlebih karena sifat *blockchain*

¹⁷ J. Amy Schmitz dan Colin Rule, "Online Dispute Resolution for Smart Contracts," *Journal of Dispute Resolution* 2019, no. 2 (2019): 108.

¹⁸ W. Maxwell dan J. Salmon, *A Guide to Block Chain and Data Protection* (London: Hogan Lovells, 2017), 7.

¹⁹ *Ibid*

yang tidak memungkinkan perubahan atau penghapusan data. Kondisi ini berseberangan dengan prinsip-prinsip perlindungan data pribadi dalam UU No. 27 Tahun 2022, seperti hak atas pembatasan pemrosesan dan penghapusan data. Karakteristik teknologi *blockchain* yang bersifat publik dan *immutable* menjadikan pelaksanaan prinsip-prinsip tersebut sulit untuk diimplementasikan dalam konteks *smart contract*. Selain itu, pelibatan pihak ketiga dalam transaksi juga menambah risiko kebocoran data karena kontrol tidak sepenuhnya berada di tangan penyedia layanan utama. Hal ini menunjukkan bahwa perlindungan hukum yang diatur dalam UU No. 27 Tahun 2022 masih dirancang untuk sistem elektronik yang terpusat dan belum sepenuhnya menjawab tantangan perlindungan data pribadi dalam sistem terdesentralisasi. Oleh karena itu, diperlukan analisis terhadap bentuk perlindungan hukum, baik melalui perlindungan hukum internal maupun eksternal, yang relevan dan adaptif terhadap perkembangan teknologi seperti *smart contract* dan *blockchain*.

3. Pelindungan Hukum bagi Data Pribadi Pengguna dan Aplikasi Pluang pada *Smart Contract*

Pelindungan hukum berdasarkan sumbernya dapat dibedakan menjadi dua macam, yakni pelindungan hukum eksternal dan pelindungan hukum internal”.²⁰ Moch Isnaeni berpendapat bahwa Pelindungan Hukum Internal pada hakekatnya untuk melindungi kepentingan para pihak yang dibangun berdasarkan kata sepakat, dituangkan dalam klausula-klausula kontrak.²¹ Sedangkan, Pelindungan hukum eksternal adalah pelindungan hukum yang dibuat oleh penguasa lewat regulasi mengenai pelindungan hukum yang seimbang.²² Berdasarkan pengertian tersebut, pelindungan hukum bagi data pribadi pengguna Aplikasi Pluang dan Aplikasi Pluang dapat diklasifikasikan menjadi pelindungan hukum eksternal dan internal, hal ini dikarenakan para pihak terikat pada kontrak elektronik yang disediakan oleh aplikasi.

²⁰ Moch. Isnaeni, *Seberkas Diorama Hukum Kontrak* (Surabaya: Revka Petra Media, 2018), 41, dikutip dalam Subekti dan Suyanto, "Pelindungan Hukum Bagi Konsumen pada Jual Beli Rumah Deret dengan Sistem Pre Project Selling berdasarkan PPJB," *Lex Journal: Kajian Hukum & Keadilan* 4, no. 1 (2021): 6, <https://doi.org/10.25139/lex.v4i1.3367>.

²¹ Moch. Isnaeni, *Seberkas Diorama Hukum Kontrak* (Surabaya: Revka Petra Media, 2017), 41-42, dikutip dalam Subekti dan Veronika Nugraheni Sri Lestari, *Perlindungan Hukum Bagi Konsumen Rumah Tapak Dalam Kontrak Jual Beli Berdasarkan Perjanjian Pengikatan Jual Beli* (Jakad Media Publishing, n.d.), 60, https://www.google.co.id/books/edition/Perlindungan_Hukum_bagi_Konsumen_Rumah_T/sBH5DwAAQB_AJ?hl=en&gbpv=0.

²² Moch. Isnaeni, *Pengantar Hukum Jaminan Kebendaan*, 159-163, dikutip dalam Miando P. Parapat et al., *Hukum Kenotariatan Indonesia Jilid 2* (Media Sains Indonesia, 2022), 117, https://www.google.co.id/books/edition/Hukum_Kenotariatan_Indonesia_Jilid_2/ItxfEAAAQBAJ?hl=en&gbpv=0.

a. Pelindungan Hukum Internal

1) Bagi Pengguna Aplikasi Pluang

Kesadaran dan pemahaman literasi digital pengguna Aplikasi Pluang menjadi aspek penting dalam pelindungan hukum internal bagi pengguna. Sebelum melakukan pendaftaran pada aplikasi Pluang atau aplikasi investasi digital yang lain, pengguna harus terlebih dahulu memastikan perizinan dari aplikasi yang bersangkutan. Pengguna dapat memeriksa terlebih dahulu apakah aplikasi yang bersangkutan telah terdaftar dan diawasi oleh Kementerian Komunikasi dan Informatika Republik Indonesia, Badan Pengawas Perdagangan Berjangka Komoditi dan Otoritas Jasa Keuangan. Setelah memeriksa legalitas dari aplikasi, pengguna dianjurkan untuk mempelajari syarat dan ketentuan serta kebijakan privasi yang telah disiapkan oleh aplikasi sebelum mendaftarkan diri pada aplikasi. Pada kebijakan privasi Aplikasi Pluang, telah disebutkan bahwa Pluang mungkin mengumpulkan berbagai data pribadi seperti nama, nomor induk kependudukan (NIK), jenis kelamin, alamat rumah, nomor ponsel, alamat e-mail, daftar kontak, nomor rekening tabungan, dan nama akun media sosial (*Facebook*).²³ Hal ini penting untuk dipelajari oleh pengguna terlebih dahulu agar mengetahui data pribadi tersebut akan digunakan untuk tujuan apa dan siapa saja yang dapat mengakses data pribadi tersebut. Jika di kemudian hari dapat dibuktikan bahwa Aplikasi Pluang telah lalai dalam menjaga data pribadi pengguna atau menggunakan data pribadi untuk hal yang tidak diatur dalam syarat dan ketentuan serta kebijakan privasi maka pengguna dapat memintakan pertanggungjawaban kepada Aplikasi Pluang. Adapun beberapa saran yang diberikan oleh Kementerian Komunikasi dan Informasi yaitu :²⁴

- a) Gunakan perangkat lunak (*software*) yang legal, sehingga selalu ada pembaruan (*update*) untuk menambal celah keamanan (*bug*) yang mungkin saja muncul.
- b) Ganti kata sandi (*password*) beragam akun secara berkala. Pastikan password terdiri dari gabungan nomor, huruf kapital, frasa, dan lain sebagainya yang tidak menjurus kepada data

²³ Pluang, "Kebijakan Privasi," diakses 9 Maret 2023, <https://pluang.com/privacy-policy>.

²⁴ Uty Yustiawati (Aplikasi Pluang), wawancara dengan penulis, 29 Desember 2022, wawancara asinkronus.

pribadi agar tidak mudah ditebak. Contoh: BellMartabak50Ribu!

- c) Jangan membuka tautan (*link*) mencurigakan di dalam e-mail, SMS, atau kanal lain. Sebab, *link* tersebut bisa saja berupa tautan palsu seperti *phising* dan sebagainya.
 - d) Hindari penggunaan koneksi *internet wireless* (Wi-Fi) di sembarang tempat. Sebab, tak jarang jaringan Wi-Fi di tempat umum tidak terjamin keamanannya.
 - e) Tidak menunjukkan data pribadi seperti *e-mail*, *password*, OTP dan lain sebagainya kepada orang lain di media sosial atau media komunikasi lainnya. Dengan begitu, akun-akun pengguna akan tetap rahasia.
- 2) Bagi Aplikasi Pluang sebagai Pengembang Aplikasi serta Pengendali Data Pribadi

Sebagai pengembang aplikasi keuangan tentunya Aplikasi Pluang membutuhkan beberapa data nasabahnya untuk keperluan KYC (*Know Your Customer*) sebagai persyaratan untuk melakukan transaksi. Data nasabah tersebut kemudian akan disimpan selama diperlukan untuk memenuhi tujuan pengumpulannya, atau selama penyimpanan tersebut diwajibkan atau diizinkan oleh hukum yang berlaku.²⁵ Dalam memitigasi adanya insiden kebocoran data pribadi yang disebabkan oleh pengguna atau pihak lainnya, Aplikasi Pluang telah membuat ketentuan pada bagian Retensi Informasi Pribadi yang dapat dilihat pada Kebijakan Privasi Aplikasi Pluang yang berbunyi: ²⁶

“Harap perhatikan bahwa masih ada kemungkinan bahwa beberapa Informasi Pribadi Anda mungkin disimpan oleh pihak lain atau Pengguna dengan cara tertentu (seperti, melalui tangkapan layar). Informasi yang disampaikan melalui komunikasi antara Pengguna dan Pihak Ketiga, yang dilakukan selain melalui penggunaan Aplikasi (seperti melalui telepon, pesan seluler, atau mode komunikasi lainnya) juga dapat disimpan dengan beberapa cara. Kami tidak mengizinkan penyimpanan Informasi Pribadi dengan cara tersebut dan kami tidak bertanggung jawab kepada Anda untuk hal yang sama. Sejauh diizinkan oleh Hukum yang Berlaku, kami tidak akan bertanggung jawab atas penyimpanan Informasi Pribadi Anda tersebut. Anda setuju untuk

²⁵ Pluang, "Kebijakan Privasi."

²⁶ *Ibid*

membebaskan kami, maupun pejabat, direktur, karyawan, agen, pemasok, kontraktor, dan Afiliasi kami dari dan terhadap setiap dan semua klaim, kerugian, kewajiban, pengeluaran, kerusakan, dan biaya (termasuk tetapi tidak terbatas pada biaya hukum dan pengeluaran atas dasar ganti rugi penuh) yang dihasilkan secara langsung atau tidak langsung dari penyimpanan Informasi Pribadi Anda yang tidak sah.”

Dengan ketentuan tersebut Aplikasi Pluang telah memperoleh Pelindungan Hukum Internal apabila terdapat insiden data pribadi yang disebabkan oleh kelalaian pengguna. Selain dari ketentuan tersebut, Aplikasi Pluang juga mengambil tindakan pencegahan yang diperlukan secara administratif dan teknis, untuk melindungi informasi pribadi pengguna terhadap kehilangan, pencurian, penyalahgunaan dan akses yang tidak sah, pengungkapan, penggunaan, perubahan atau perusakan.²⁷ Ketentuan dalam Kebijakan Privasi Aplikasi Pluang menunjukkan upaya mitigasi risiko terhadap penyalahgunaan data pribadi, terutama yang disebabkan oleh pihak ketiga maupun kelalaian pengguna. Namun demikian, dalam praktiknya, mekanisme pelimpahan tanggung jawab ini tetap memerlukan kehati-hatian. Mengingat peran Aplikasi Pluang sebagai pengendali data, diperlukan penguatan dalam hal transparansi dan akuntabilitas untuk memastikan bahwa pelindungan data tetap terjaga di seluruh rantai pemrosesan, termasuk saat melibatkan pihak ketiga. Dengan demikian, pendekatan internal melalui kebijakan privasi sebaiknya juga dilengkapi dengan standar teknis dan audit keamanan yang konsisten agar pelindungan data tidak hanya bersifat normatif, tetapi juga implementatif.

b. Pelindungan Hukum Eksternal

1) Bagi Pengguna Aplikasi Pluang

Data pribadi yang disetorkan dalam *smart contract* tidak berwujud dalam bahasa yang jelas dan eksplisit namun sudah berbentuk psedonim. *Pseudonymization* merupakan salah satu cara untuk menyamarkan data pribadi. Metode yang dapat digunakan salah satunya dengan data masking, seperti dengan melakukan enkripsi data, pengacakan data, substitusi data dan teknik lainnya. Namun data *pseudonym* ini jika digabungkan dengan

²⁷ *Ibid*

informasi lainnya atau jika melalui mekanisme/metode/teknik tertentu dapat dipulihkan kembali. Misalnya, suatu data yang disamarkan dengan teknik enkripsi dapat dipulihkan dengan teknik dekripsi, dan data yang telah dipulihkan tersebut kembali dapat mengidentifikasi seseorang. Sehingga data *pseudonym* tetap dapat disebut sebagai data pribadi.²⁸ Berdasarkan pernyataan tersebut maka dapat dikatakan bahwa data pribadi pengguna yang berbentuk pseudonim tetap dilindungi oleh UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi berdasarkan Pasal 1 ayat (1) yang menjelaskan bahwa Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.²⁹ Sedangkan untuk informasi yang dikemas dalam bentuk *anonym*, tidak mendapat pelindungan sesuai dengan ketentuan Pasal *a quo*. *General Data Protection Regulation* (GDPR) menjelaskan bahwa prinsip-prinsip pelindungan data seharusnya tidak berlaku untuk informasi anonim, yaitu informasi yang tidak berhubungan dengan orang yang teridentifikasi atau dapat diidentifikasi atau data pribadi yang dibuat anonim dengan cara sedemikian rupa sehingga subjek data tidak dapat diidentifikasi lagi.³⁰ Data *anonym* tidak termasuk ke dalam data pribadi selama data *anonym* ini, dengan mekanisme/metode/teknik apapun, sangat sulit untuk dipulihkan kembali dan tidak dapat lagi mengidentifikasi atau merujuk kepada seseorang.

Setelah mengetahui bahwa data pribadi yang berbentuk *pseudonym* memperoleh pelindungan dari UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi, maka selanjutnya terdapat beberapa bentuk pelindungan hukum eksternal bagi pengguna yang telah diatur dalam berbagai pengaturan antara lain:

- a) UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi telah mengatur secara rinci mengenai kewajiban Pengendali Data Pribadi dan Prosesor Data Pribadi. Berdasarkan wawancara yang

²⁸ Wawancara Uty Yustiawati.

²⁹ Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pasal 1, ayat (1).

³⁰ European Union, General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), 2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>.

penulis lakukan dengan narasumber dari Kementerian Komunikasi dan Informatika dengan mengacu pada Undang-Undang *a quo*, perbedaan antara Pengendali Data Pribadi dan Prosesor Data Pribadi terletak pada tujuannya, jika pengembang Aplikasi Pluang yang dimaksud merupakan penentu tujuan dan kendali pemrosesan data pribadi maka dapat disebut sebagai Pengendali Data Pribadi. Jika pengembang Aplikasi Pluang yang dimaksud merupakan pihak *developer* yang membangun/mengembangkan sistem berdasarkan perintah atau kontrak dengan pemilik tujuan pemrosesan data pribadi (Pengendali Data Pribadi), maka pengembang Aplikasi Pluang disebut sebagai Prosesor Data Pribadi. Berdasarkan syarat dan ketentuan yang ada pada aplikasi dan laman Pluang, dapat dikatakan bahwa Pluang atau PT Bumi Santosa Cemerlang merupakan Pengendali Data Pribadi yang menentukan tujuan dan kendali pemrosesan data pribadi. Pada pelaksanaannya, Aplikasi Pluang bekerja sama dengan PT Privy Identitas Digital dalam rangka pelaksanaan proses verifikasi dan pemrosesan data pribadi, sehingga dapat disebutkan bahwa PT Privy Identitas Digital adalah Prosesor Data Pribadi. PT Bumi Santosa Cemerlang dan PT Privy Identitas Digital tunduk kepada kewajiban yang telah diatur pada Pasal 20 sampai dengan Pasal 52 UU Pelindungan Data Pribadi;

- b) Pasal 26 ayat (1) dan (2) UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- c) Peraturan Bappebti Nomor 13 Tahun 2022 tentang Perubahan atas Peraturan Bappebti Nomor 8 Tahun 2022 tentang Pedoman Penyelenggaraan Perdagangan Pasar Fisik Aset Kripto (*Crypto Asset*) di Bursa Berjangka. Padal Pasal 31D dari ketentuan *a quo* disebutkan bahwa Calon Pedagang Fisik Aset Kripto atau Pedagang Fisik Aset Kripto wajib menjaga kerahasiaan data dan/atau informasi mengenai Pelanggan Aset Kripto.

2) Bagi Aplikasi Pluang sebagai Pengembang Aplikasi serta Pengendali Data Pribadi

Pelindungan Hukum eksternal bagi penyelenggara sistem elektronik memang tidak secara eksplisit diatur dalam hukum positif di Indonesia. Kendati demikian, dalam Peraturan Menteri Kementerian Komunikasi dan Informatika telah disebutkan bahwa baik setiap pemilik data pribadi dan penyelenggara sistem elektronik dapat mengajukan pengaduan kepada Menteri atas kegagalan pelindungan kerahasiaan Data Pribadi. Adanya ketentuan tersebut, secara implisit memfasilitasi penyelenggara sistem elektronik apabila telah terjadi kebocoran data pribadi yang tidak disebabkan oleh kelalaian atau ketidakhati-hatiannya sendiri melainkan perbuatan pihak lain yang berusaha melakukan peretasan terhadap sistem atau berusaha merugikan penyelenggara sistem elektronik.

Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik telah menyediakan pengaturan untuk menangani terjadi kegagalan Pelindungan Data Pribadi yang tertuang pada Pasal 24 ayat (3) disebutkan bahwa “Dalam hal terjadi kegagalan atau gangguan sistem yang berdampak serius sebagai akibat perbuatan dari pihak lain terhadap Sistem Elektronik, Penyelenggara Sistem Elektronik wajib mengamankan Informasi Elektronik dan/ atau Dokumen Elektronik dan segera melaporkan dalam kesempatan pertama kepada aparat penegak hukum dan Kementerian atau Lembaga terkait.” Selain itu Badan Pengawas Perdagangan Berjangka Komoditi juga mewajibkan penyelenggara sistem elektronik untuk menerapkan SNI ISO/IEC 27001 (*information security management system*).³¹ Tujuan dari penerapan SNI ISO/IEC 27001 sendiri adalah untuk melindungi perusahaan dari ancaman keamanan terhadap data pribadi pengguna dan juga data perusahaan.

Keberadaan UU No. 27 Tahun 2022 merupakan langkah penting dalam pelindungan data pribadi di Indonesia. Namun, karakteristik teknologi seperti *blockchain* dan *smart contract* yang bersifat *immutable* dan terdesentralisasi menimbulkan tantangan tersendiri dalam penerapan ketentuan hukum *a quo*.

³¹ Rio Ramadhani dan Yovian Andri P (Badan Pengawas Perdagangan Berjangka Komoditi), wawancara dengan penulis, 4 Januari 2023, secara daring.

Sebagai contoh, implementasi hak atas penghapusan data dalam sistem *blockchain* memerlukan pendekatan teknis dan yuridis yang berbeda dari sistem elektronik pada umumnya. Oleh karena itu, dibutuhkan pemikiran regulatif yang adaptif dan kontekstual agar perlindungan hukum terhadap data pribadi dalam ekosistem digital dapat berjalan seiring dengan perkembangan teknologi.

C. PENUTUP

1. Kesimpulan

Terdapat beberapa potensi kebocoran data pribadi yang berasal dari teknologi *blockchain* dan *smart contract* yaitu apabila ada pihak-pihak yang melakukan dekripsi pada data-data psedonim yang sudah dienkrupsi, apabila terdapat data pribadi yang tidak sengaja disetorkan pada kedua teknologi tersebut karena data tersebut tidak dapat dihilangkan atau diubah-ubah, apabila *private key* pengguna didapatkan oleh pihak yang tidak bertanggung jawab dan menyalahgunakannya, serta apabila ada pihak yang melacak informasi pengguna dari *public key*.

Adapun dua jenis perlindungan hukum bagi data pribadi para pihak pada perjanjian jenis *smart contract* yang digunakan Aplikasi Pluang yaitu perlindungan hukum secara internal dan eksternal. Pelindungan hukum internal bagi pengguna adalah dengan mempelajari terlebih dahulu kebijakan privasi serta syarat dan ketentuan terkait aplikasi penyedia jasa jual beli aset kripto sebelum memberikan data pribadi yang diminta oleh Aplikasi, hal ini penting untuk dilakukan agar pengguna memahami tujuan penggunaan data pribadi dan keamanan yang telah disiapkan oleh Aplikasi. Sedangkan untuk Aplikasi Pluang, pelindungan hukum internal yang dapat dilakukan adalah dengan membatasi data pribadi yang akan diberikan oleh pihak ketiga, hal ini ditujukan sebagai bentuk mitigasi dari adanya kebocoran data pribadi atau penyalahgunaan data pribadi yang disebabkan oleh pihak ketiga. Selanjutnya, walaupun belum ada pengaturan yang secara spesifik mengatur tentang *blockchain* dan *smart contract*, Pelindungan hukum eksternal bagi pengguna dapat dilihat pada berbagai pengaturan yang berlaku saat ini seperti UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi, Peraturan Bappebti, Peraturan Kementerian Komunikasi dan Informatika, dan masih banyak lagi. Sedangkan Pelindungan hukum eksternal bagi Aplikasi Pluang dapat dilihat pada UU No. 27 Tahun 2022 yang turut menyediakan fasilitas pengaduan bagi penyelenggara sistem elektronik apabila mengalami kegagalan dalam pemrosesan data pribadi pengguna.

2. Saran

- a. Saran untuk pengguna sebagai konsumen dari Aplikasi Pluang adalah untuk selalu menjaga data pribadi milik sendiri dan juga orang lain. Pengguna tidak dianjurkan untuk memberikan data pribadi kepada sembarang pihak dan membagikan data dalam bentuk tangkapan layer pada media sosial atau *platform* publik lainnya, hal ini dikarenakan data tersebut dapat disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab.
- b. Saran untuk Aplikasi Pluang sebagai pengemban amanat dan bertanggung jawab atas pemrosesan data pribadi adalah untuk selalu memastikan agar teknologi yang digunakan pada aplikasi memiliki keamanan yang terbaru dan membatasi data pribadi yang diketahui oleh pihak ketiga, hal ini ditujukan untuk meminimalisir adanya potensi kebocoran data pribadi atau penyalahgunaan data oleh pihak ketiga serta ancaman serangan siber dari pihak yang tidak bertanggung jawab.
- c. Saran untuk Pemerintah sebagai pembentuk Undang-Undang adalah apabila akan membuat regulasi untuk teknologi *blockchain* dan *smart contract* baik secara umum ataupun berkaitan dengan memitigasi adanya potensi kebocoran data pribadi sebaiknya juga turut melibatkan para pihak yang terjun langsung menggunakan atau berkaitan dengan teknologi tersebut serta para pakar teknologi agar kemudian regulasi tersebut dapat betul-betul menjangkau segala kebutuhan yang lahir seiring dengan perkembangannya teknologi tersebut.

D. DAFTAR PUSTAKA

“Australian Crypto Exchange Exposes Personal Data of 270K Users.” CoinDesk. 2 Desember 2020. <https://www.coindesk.com/business/2020/12/02/australian-crypto-exchange-exposes-personal-data-of-270k-users/>.

Badan Pengawas Perdagangan Berjangka Komoditi. “Peraturan Badan Pengawas Perdagangan Berjangka Komoditi Nomor 8 Tahun 2021 Tentang Pendoman Penyelenggaraan Perdagangan Pasar Fisik Aset Kripto (Crypto Asset) Di Bursa Berjangka.” Diakses 2 Oktober 2022. https://bappebti.go.id/resources/docs/peraturan/sk_kep_kepala_bappebti/sk_kep_kepala_bappebti_2021_12_01_bt4tvsg9_id.pdf.

- Biryukov, Alex, Dmitry Khovratovich, and Ivan Pustogarov. "Deanonymisation of Clients in Bitcoin P2P Network." Dalam Proceedings of the ACM Conference on Computer and Communications Security, 2014. <https://doi.org/10.1145/2660267.2660379>.
- European Union. General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). 2016. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>.
- Fireblocks. "Fireblock' Multi-Layer Philosophy for Securing Digital Assets." n.d.
- Hewa, Tharaka, Mika Ylianttila, and Madhusanka Liyanage. "Survey on Blockchain Based Smart Contracts: Applications, Opportunities and Challenges." Journal of Network and Computer Applications 177 (1 Maret 2021): 102857. <https://doi.org/10.1016/J.JNCA.2020.102857>.
- Juels, Ari, Ahmed Kosba, and Elaine Shi. "The Ring of Gyges: Investigating the Future of Criminal Smart Contracts." Dalam Proceedings of the ACM Conference on Computer and Communications Security, 2016. <https://doi.org/10.1145/2976749.2978362>.
- Lukita, Chandra. "Penerapan Sistem Pendataan Hak Cipta Content Menggunakan Blockchain." ADI Bisnis Digital Interdisiplin Jurnal 1, no. 2 (Desember 2020). <https://doi.org/10.34306/abdi.v1i2.120>.
- Olivia, Lona. "Jumlah Pelanggan Tumbuh Lebih Banyak, Akankah Transaksi Kripto Bisa Salip Saham?" Investor.id. Diakses 2 Oktober 2022. <https://investor.id/market-and-corporate/300115/jumlah-pelanggan-tumbuh-lebih-banyak-akankah-transaksi-kripto-bisa-salip-saham>.
- Osmanoğlu, Murat, and Ali Aydın Selçuk. "Privacy in Blockchain Systems." Turkish Journal of Electrical Engineering and Computer Sciences 30, no. 2 (Februari 2022): 344–60. <https://doi.org/10.3906/elk-2105-183>.
- Parapat, Miando P., Satrio Abdillah, Fathul Laila, Muh. Husen Ahmad, Tata Wijayanta, BE Hermawan, and Rado Fridsel Le. Hukum Kenotariatan Indonesia Jilid 2. Media Sains Indonesia, 2022. https://www.google.co.id/books/edition/Hukum_Kenotariatan_Indonesia_Jilid_2/ItxfEAAAQBAJ?hl=en&gbpv=0.
- Pluang. "Kebijakan Privasi." Diakses 9 Maret 2023. <https://pluang.com/privacy-policy>.
- Pluang. "Mengapa Harga Aset Kripto Pluang Berbeda Dari Platform Lain? Simak Penjelasannya!" Pluang Blog. Diakses 9 Maret 2023. <https://pluang.com/id/blog/resource/perbedaan-harga-aset-kripto-pluang>.

- “Pluang, Platform Investasi Multi Aset Paling Inovatif.” CNBC Indonesia. 12 Desember 2022. <https://www.cnbcindonesia.com/market/20221212195050-17-396226/pluang-platform-investasi-multi-aset-paling-inovatif>.
- Raskin, Max. “The Law and Legality of Smart Contracts.” Georgetown Law Technology Review 1, no. 2 (2017). <https://heinonline.org/HOL/License>.
- Schmitz, Amy, and Colin Rule. “Online Dispute Resolution for Smart Contracts.” Journal of Dispute Resolution 2019, no. 2 (2019).
- Shah, Pritesh, Daniel Forester, Matthias Berberich, and Carolin Raspé. “Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies.” Davis Polk & Wardwell LLP, 2019. https://www.davispolk.com/sites/default/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf.
- Subekti, and Veronika Nugraheni Sri Lestari. Perlindungan Hukum Bagi Konsumen Rumah Tapak Dalam Kontrak Jual Beli Berdasarkan Perjanjian Pengikatan Jual Beli. Jakad Media Publishing, n.d. https://www.google.co.id/books/edition/Perlindungan_Hukum_bagi_Konsumen_Rumah_Tapak/sBH5DwAAQBAJ?hl=en&gbpv=0.
- Subekti, Subekti, and Suyanto Suyanto. “Perlindungan Hukum Bagi Konsumen Pada Jual Beli Rumah Deret Dengan Sistem Pre Project Selling Berdasarkan PPJB.” Lex Journal: Kajian Hukum & Keadilan 4, no. 1 (2021). <https://doi.org/10.25139/lex.v4i1.3367>.
- Vigliotti, Maria G. “What Do We Mean by Smart Contracts? Open Challenges in Smart Contracts.” Frontiers in Blockchain 3 (2021). <https://doi.org/10.3389/fbloc.2020.553671>.