TESIS

PENGADOPSIAN TEKNOLOGI BLOCKCHAIN DALAM PENGATURAN SEKTOR PERBANKAN UNTUK MENCEGAH PENIPUAN ONLINE BERUPA DEEPFAKE

Oleh:

Nama Mahasiswa	: **Christina Natalia Riesty Setyawan**
NIM	: **24912011**
BKU	: **Hukum dan Sistem Peradilan Pidana**

PROGRAM STUDI HUKUM PROGRAM MAGISTER

FAKULTAS HUKUM

UNIVERSITAS ISLAM INDONESIA

2026

PENGADOPSIAN TEKNOLOGI BLOCKCHAIN DALAM PENGATURAN SEKTOR PERBANKAN UNTUK MENCEGAH PENIPUAN ONLINE BERUPA DEEPFAKE

TESIS

Oleh:

NamaMahasiswa : **Christina Natalia Riesty Setyawan**

NIM : **24912011**

BKU : **Hukum dan Sistem Peradilan Pidana**

PROGRAM STUDI HUKUM PROGRAM MAGISTER

FAKULTAS HUKUM

UNIVERSITAS ISLAM INDONESIA

2026

HALAMAN PENGESAHAN

بسم الله الرحمن الرحيم

Pengadopsian Teknologi Blockchain Dalam Pengaturan Sektor Perbankan Untuk Mencegah Penipuan Online Berupa Deepfake

Telah diperiksa dan disetujui Dosen Pembimbing Tugas Akhir untuk diajukan ke depan TIM Penguji dalam Ujian Tugas Akhir / Pendadaran

pada tanggal 13 Januari 2026

Yogyakarta, 13 Januari 2026
Dosen Pembimbing Tugas Akhir,

Aroma Elmina Martha, Dr.,S.H., M.H.,

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Pengadopsian Teknologi Blockchain Dalam Pengaturan Sektor Perbankan Untuk Mencegah Penipuan Online Berupa Deepfake

Telah Dipertahankan di Hadapan Tim Penguji dalam
Ujian Tugas Akhir / Pendadaran
pada tanggal dan Dinyatakan LULUS

Yogyakarta, 13 Januari 2026

Tim Penguji		Tanda Tangan
1. Ketua	Aroma Elmina Martha, Dr.,S.H., M.H.,	
2. Anggota	Budi Agus Riswandi, Prof., Dr., S.H., M.Hum.,	
3. Anggota	Muhammad Arif Setiawan, Dr., S.H., M.H.,	

Mengetahui:
Universitas Islam Indonesia
Fakultas Hukum
Dekan,

Budi Agus Riswandi, Prof., Dr., S.H., M.Hum.,
NIK. 014100109

Bukti ACC Dosen Pembimbing

HALAMAN PENGESAHAN

PROPOSAL TESIS

PENGGUNAAN TEKNOLOGI BLOCKCHAIN UNTUK MENCEGAH TINDAK PIDANA PENIPUAN ONLINE

Oleh :

Nama Mahasiswa : **Christina Natalia Riesty Setyawan**

NIM : **24912011**

BKU : **Hukum dan Sistem Peradilan Pidana**

Telah diperiksa dan disetujui oleh Dosen Pembimbing untuk diajukan kepada Tim Penguji dalam ~~Seminar Proposal~~ Tidang Tesis

Pembimbing,

Dr Aroma Elmina Martha, S.H., M.H.

Yogyakarta, 9 Desember 2025

Mengetahui,
Ketua Program Studi Hukum Program Magister
Fakultas Hukum Universitas Islam Indonesia

Prof. Dr. Sefriani, S.H., M.Hum.

HALAMAN MOTTO

“Allah tidak membebani seseorang melainkan sesuai dengan kesanggupannya”

(Q.S Al-Baqarah: 286)

“Allah berfirman: janganlah kamu berdua khawatir, sesungguhnya Aku beserta kamu berdua, Aku mendengar dan melihat”

(Q.S Thaha: 46)

“You need chaos in your soul to give birth to a dancing star”

(Nietzsche)

“Orang yang berdiri di bawah pohon paling rindang hari ini adalah yang dulu menanam benih dengan akar paling dalam”

(Timothyronald)

“To be yourself, you have to trust yourself, trust in the process of becoming”

(Riasw)

HALAMAN PERSEMBAHAN

Tugas Akhir ini saya persembahkan untuk:

Tesis ini saya persembahkan kepada:

1. Allah SWT dan Nabi Muhammad SAW
2. Orangtua yang saya sayangi yang selalu mendukung dan medoakan saya
3. Kakak dan adik saya yang saya sayangi
4. Diri saya sendiri
5. Seseorang yang saya sayangi
6. Teman-teman tersayang selama menempuh pendidikan magister
7. Keluarga besar

SURAT PERNYATAAN ORISINALITAS

PENGADOPSIAN TEKNOLOGI BLOCKCHAIN DALAM PENGATURAN SEKTOR PERBANKAN UNTUK MENCEGAH PENIPUAN ONLINE BERUPA DEEPFAKE

بِسْمِ اللهِ الرَّحْمٰنِ الرَّحِيْمِ

Yang bertandatangan di bawah ini, saya:

Nama : Christina Natalia Riesty Setyawan

NIM : 24912011

Adalah benar-benar Mahasiswa Program Studi Magister Hukum Program Magister Fakultas Hukum Universitas Islam Indonesia Yogyakarta yang telah melakukan penulisan Karya Tulis Ilmiah (Tugas Akhir) berupa Tesis dengan judul:

PENGADOPSIAN TEKNOLOGI BLOCKCHAIN DALAM PENGATURAN SEKTOR PERBANKAN UNTUK MENCEGAH PENIPUAN ONLINE BERUPA DEEPFAKE

Karya Tulis Ilmiah ini saya ajukan kepada Tim Penguji dalam Ujian Pendadaran yang akan diselenggarakan oleh Fakultas Hukum Universitas Islam Indonesia.

Sehubungan dengan hal tersebut, dengan ini saya menyatakan:

1. Bahwa karya tulis ilmiah ini adalah benar-benar karya saya sendiri yang dalam penyusunannya tunduk dan patuh kepada kaidah, etika, dan

norma-norma penulisan sebuah karya ilmiah sesuai dengan ketentuan yang berlaku;

2. Bahwa saya menjamin hasil karya tulis ilmiah ini benar-benar asli (orisinil) bebas dari unsur-unsur yang dapat dikategorikan sebagai melakukan perbuatan "penjiplakan karya ilmiah"
3. Bahwa meskipun secara prinsip hak milik atas karya tulis ilmiah ini ada pada saya, namun demi kepentingan-kepentingan yang bersifat akademik dan pengembangan, saya memberikan kewenangan kepada Perpustakaan Fakultas Hukum Universitas Islam Indonesia dan perpustakaan di lingkungan Universitas Islam Indonesia untuk mempergunakan karya ilmiah saya tersebut.

Selanjutnya berkaitan dengan hal di atas, saya sanggup menerima sanksi, baik sanksi administratif, akademik, bahkan pidana jika terbukti kuat dan meyakinkan telah melakukan perbuatan yang menyimpang dari pernyataan saya tersebut. Saya juga akan bersifat kooperatif untuk hadir, menjawab, dan melakukan pembelaan atas hak-hak saya, serta menandatangani berita acara terakit yang menjadi hak dan kewajiban saya, di depan (Majelis) atau (Tim) Fakultas Hukum Universitas Islam Indonesia yang ditunjuk oleh pimpinan fakultas apabila tanda-tanda plagiasi disinyalir ada terjadi pada karya tulis ilmiah saya ini, oleh pihak Fakultas Hukum Universitas Islam Indonesia.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya, dalam kondisi sehat jasmani dan rohani, dengan sadar serta tidak ada tekanan dalam bentuk apapun dan oleh siapapun.

Yogyakarta, 19 Desember 2025

Christina Natalia Riesty Setyawan

KATA PENGANTAR

بِسْمِ اللهِ الرَّحْمٰنِ الرَّحِيْمِ

Assalamu'alaikum Wr. Wb.

Alhamdulillahirabbil'alamin, segala puji dan syukur atas kehadirat Allah SWT yang Maha Pengasih lagi Maha Penyayang atas segala rahmat, taufik, dan hidayah-Nya sehingga penulis mampu menyelesaikan tugas akhir (tesis) ini dengan baik. Shalawat serta salam penulis haturkan kepada junjungan Nabi besar Muhammad SAW melalui petunjuk dan bimbingannya yang membawa kita dari zaman jahiliyah menuju zaman yang penuh dengan ilmu pengetahuan.

Tesis yang berjudul **Pengadopsian Teknologi Blockchain dalam Pengaturan Sektor Pebankan untuk Mencegah Penipuan Online Berupa Deepfake** dalam rangka menyelsaikan program tugas akhir pada program Strata-2 (S2) Magister Hukum Universitas Islam Indonesia Yogyakarta, untuk meraih gelar Magister Hukum. Sebagai mana manusia lainnya, penulis menyadari segala kekurangan dan ketidak sempurnaan dalam penulisan tesis ini, sehingga kritik dan saran yang bersifat membangun akan selalu penulis terima untuk kemajuan proses belajar penulis kelak dikemudian hari.

Pada kesempatan kali ini pula penulis ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Allah SWT atas segala rahmat, hidayah, dan nikmat yang tiada pernah berhenti bagi umat-Nya.
2. Nabi Muhammad SAW, sosok yang membawa peradaban ilmu pengetahuan menjadi lebih baik.
3. Kedua orangtua, kakak dan adik saya dan keluarga besar lainnya.
4. Prof. Dr. Budi Agus Riswandi, S.H., M.Hum selaku Dekan Fakultas Hukum Universitas Islam Indonesia.
5. Dr. Aroma Elmina Martha, S.H., M.H. selaku Dosen Pembimbing Tugas Akhir yang senantiasa bersabar dan mendukung penuh saya untuk menyelesaikan studi dengan sebaik-baiknya.
6. Kepada seseorang yang tidak kalah penting kehadirannya, Bima Adisatria, S.T. Terima kasih telah menjadi bagian dalam proses perjalanan penulis menyusun tesis. Berkontribusi baik tenaga, waktu, menemani, mendukung, serta menghibur penulis dalam kesedihan, mendengarkan keluh kesah dan meyakinkan penulis untuk pantang menyerah dalam penulisan tesis ini, sehingga penyusunan tesis ini terselesaikan.
7. Ghina, Rayhana, Intan, Yumna, Reva, Uffi, Habibah, Catur, Ouzy, dan teman-teman lainnya yang saya tidak bisa sebutkan satu persatu yang telah menemani saya dalam susah dan senang yang telah menerima keluh kesah saya mengenai pengerjaan tugas akhir ini. Serta telah menjadi teman saya untuk berdiskusi mengenai segala hal.
8. Apresiasi sebesar-besarnya terhadap diri saya sendiri karena telah bertanggung jawab untuk menyelsaikan apa yang telah dimulai. Terima

kasih telah selalu berusaha dan tidak menyerah, serta senantiasa menikmati setiap proses yang bisa di bilang tidak mudah ini. Terima kasih telah bertahan sejauh ini.

Semoga Allah SWT senantiasa membalas semua kebaikan dari bantuan yang diberikan kepada penulis, hingga selesainya penulisan Tugas Akhir ini dan menjadikannya amal ibadah yang mulia disisi-Nya, *Allahuma'amin.*

Yogyakarta, 19 Desember 2025

Penulis,

(Christina Natalia Riesty Setyawan)

NIM. 24912011

Daftar Isi

Abstrak

Perkembangan teknologi digital telah membawa perubahan yang signifikan di dalam sektor perbankan, tetapi di sisi lain perkembangan ini turut meningkatkan risiko terjadinya kejahatan siber, khususnya penipuan online berupa *deepfake*. Modus penipuan ini memanfaatkan teknologi kecerdasan buatan untuk memanipulasi identitas, visual serta audio sehingga berpotensi melemahkan sistem keamanan dan mekanisme autentikasi konvensional dalam layanan perbankan. Hingga saat ini, pengaturan sektor perbankan di Indonesia belum secara spesifik mengakomodasi ancaman penipuan online berupa *deepfake* maupun pemanfaatan teknologi blockchain sebagai instrument pencegahan. Penelitian ini bertujuan untuk menganalisis pengaturan sektor perbankan terkait penggunaan teknologi blockchain dalam mencegah penipuan online berupa *deepfake*, serta mengkaji pengadopsian teknologi blockchain ke dalam kerangka regulasi perbankan di Indonesia. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan peraturan perundang-undangan dan konseptual. Hasil penelitian menunjukkan bahwa teknologi blockchain memiliki potensi sebagai sarana preventif dalam mencegah penipuan online melalui karakteristik desentralisasi, transparansi, immutabilitas, serta keamanan kriptografi yang mampu memperkuat verifikasi identitas dan integritas transaksi digital. Oleh karena itu, diperlukan pembaharuan regulasi perbankan yang adaptif dan komprehensif guna mengintegrasikan teknologi blockchain sebagai bagian dari sistem keamanan perbankan dalam menghadapi penipuan online berupa *deepfake.*

Kata kunci : teknologi blockchain, sektor perbankan, penipuan online, *deepfake*.

BAB I

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi informasi pada era saat ini sudah membawa perubahan yang cukup signifikan di dalam berbagai aspek kehidupan masyarakat, terkhusus lagi pada bidang ekonomi. Dimana transaksi online saat ini, baik melalui *e-commerce* ataupun platform digital yang lain, sudah menjadi bagian integral dari gaya hidup masyarakat modern. Namun sayangnya, kemajuan teknologi ini justru diikuti dengan mingkatnya tindak pidana penipuan online, seperti contohnya adalah pencurian identitas, manipulasi data, hingga sampai transaksi palsu yang sangat merugikan banyak pihak.[1]

Pada era digital, penipuan online telah menjadi salah satu kejahatan yang marak terjadi. Seiring dengan meningkatnya adopsi teknologi internet, jumlah pengguna yang melakukan transaksi online juga meningkat secara drastis. Hal ini membuat kejahatan di ruang digital semakin marak terjadi terutama dalam bentuk penipuan. Berdasarkan data selama periode 2017 sampai 2022, dari layanan Cekrekening.id dari kominfo telah menerima kurang lebih 486 ribu laporan dari masyarakat terkait dengan tindak pidana informasi dan transaksi elektronik (ITE). Sebanyak 83% dari laporan tersebut atau 405 ribu laporannya merupakan laporan dari korban penipuan

[1] Brian Krebs, *Cybersecurity in the Era of Digital Economy*, Cmabridge Press, 2021, hlm. 45.

transaksi online.[2] Selain itu statistika beradsarkan laporan dari *Cybercrime* Report 2023, menunjukkan peningkatan kasus penipuan online, dimana kerugian yang diakibatkan oleh kejahatan siber ini, termasuk penipuan online, mencapai kerugian kurang lebih USD 8,5 Milliar di tahun 2022.[3]

Tindak pidana penipuan online kini menjadi salah satu ancaman yang serius yang terus meningkat seiring dengan di adopsinya teknologi digital. Penipuan ini memiliki jenis-jenis yang meliputi pencurian identitas, manipulasi data, penyalahgunaan informasi pribadi, hingga transaksi palsu yang sudah kerap menimbulkan kerugiian secara finansial yang signifikan untuk korban[4]. Pelaku kejahatan siber saat ini semakin canggih di dalam mengeploitasi kelemahan suatu sistem keamanan digital, hal ini yang mengakibatkan meningkatnya tingkat kejahatan siber secara global.

Selain adanya penipuan online dari transaksi elektronik terdapat juga penipuan online berupa investasi daring yang fiktif dimana dari tindak pidana penipuan investasi ini mencapai 19 ribu laporan yang masuk. Kemudian penipuan yang berkedok memberikan penawaran yang menggiurkan dari oknum atau pelaku kepada korban dengan mengatasnamakan institusi atau suatu Perusahaan tertentu juga membayang-bayangi kegiatan belanja online masyarakat.

---

[2] Agus Tri Haryanto, *Kominfo Sebut 486 Ribu Laporan Masyarakat Kena Penipuan Online, Ini Solusinya*, detikInet, diakses pada 16/12/2024.

[3] Cybercrime Report 2023, *Annual Report on Global Cybersecurity Trends*, diakses melalui www.cyberreport.com pada 10/12/2024

[4] Kementerian Komunikasi dan Informatika, *Laporan Tahunan Penanganan Kejahatan Siber di Indonesia 2022*, diakses melalui www.kominfo.go,id pada 10/12/2024

Selain kasus penipuan online yang bermodus investasi terdapat juga kasus penipuan dengan modus deep fake yang berarti manipulasi foto maupun video dengan menggunakan bantuan dari teknologi kecerdasan buatan atau *artificial intelligence* (AI). Kapolda Jatim Irjen Pol Nanang Avianto, menyatakan bahwa pengungkapan kasus ini bermula dari adanya laporan pegawai dari Kominfo Jatim pada tanggal 15 April 2025 lalu, kemudian dari laporan tersebut Direktorat Reserse Siber (Ditressiber) melakukan patroli siber. Kemudian dari hasil patrol tersebut polisi dapat menangkap 3 (tiga) orang pelaku, yakni HMP (32), UP (24), serta AH (34), dimana ketiganya dalam melakukan penipuan menggunakan modus operandi yang dilakukan oleh pelaku adalah mengedit video dari Gurbernur Jatim yaitu Khofifah Indar Parawansa, dengan bantuan teknologi kecerdasan buatan atau *artificial intelligence* (AI). Selain dari Gurbernur Jatim pelaku juga membuat video yang sama dengan narasi penipuan yang mengatas namakan Gurbernur Jawa Tengah yaitu Ahmad Luthfi serta Jawa Barat yaitu Dedi Mulyadi. Dalam hal ini video yang para pelaku buat mereka unggah pada platform Tiktok yang kemudian mereka gunakan untuk menipu masyarakat dengan modus menawarkan bantuan fiktif. Dari kasus ini kerugian yang ditafsir mencapai nominal Rp 87.600.000 (delapan puluh tujuh juta enam ratus rupiah)[5].

[5] Bangun Santoso & Faqih Fathurrahman Suara.com, *Polisi Bongkar Penipuan Modus Deep Fake Catut Nama Dedi Mulyadi hingga Khofifah,* diakses melalui https://www.suara.com/news/2025/04/29/192551/polisi-bongkar-penipuan-modus-deep-fake-catut-nama-dedi-mulyadi-hingga-khofifah pada 08/05/2025.

Dengan adanya tantangan seperti yang terjadi pada saat ini, teknologi blockchain muncul sebagai salah satu solusi yang potensial untuk meningkatkan keamanan transaksi digital. Teknologi blockchain ialah mekanisme yang berbasis data lanjutan yang dapat memungkinkan berbagi informasi secara transparan di dalam jaringan bisnis. Basis data dalam blockchain ini menyimpan data dalam bentuk blok yang dihubungkan secara bersama dalam sebuah rantai. Blockchain adalah suatu system yang dibuat atau didesain untuk menciptakan suatu system transaksi yang aman dan juga transparan, muncul sebagai salah satu solusi yang inovatif. Teknologi blockchain ini bekerja berdasarkan dari prinsip desentralisasi, sehingga tidak ada otoritas Tunggal yang dapat mengendalikan data. Selain itu, fitur transparansi yang terdapat di blockchain dapat memungkinkan setiap transaksi tercatat di dalam buku besar digital yang bernama *distributed ledger* yang dapat diaudit oleh semua pihak.[6] Dalam blockchain, setiap transaksi akan direkam dalam blok yang saling terhubung dan dienkripsi, sehingga hampir tidak mungkin untuk memanipulasi data tanpa persetujuan mayoritas jaringan. Sistem ini meminimalkan risiko penipuan, seperti manipulasi data dan pencurian identitas, yang sering terjadi dalam transaksi online.

Teknologi blockchain tidak hanya memberikan solusi terhadap kelemahan sistem kemanan tradisional, namun teknologi ini juga

[6] Don Tapscott, *Blockchain Revolution: How Technology is Changing Money, Business, and the World*, Penguin Books, 2016, hlm. 87.

menawarkan pendekatan baru melalui penggunaan smart contracts. Smart contracts ini memungkinkan otomatisasi serta validasi transaksi digital tanpa perlu pihak ketiga, sehingga dapat meminimalisasi risiko manipulasi atau penipuan[7].

Teknologi blockchain memiliki beberapa kelebihan yang membuatnya menjadi unggul di dalam berbagai bidang, baik itu disektor keuangan, hukum, logistic, serta keamanan data, berikut adalah beberapa kelebihan dari teknologi blockchain yaitu:

1. Keamanan tinggi, dimana dalam teknologi blockchain digunakan sistem keamanan kriptografi untuk mengamankan data, sehingga hal ini menyulitkan data untuk dimanipulasi maupun diretas.
2. Transparansi, dalam konteks ini seluruh transaksi yang dilakukan di dalam blockchain dapat dilihat oleh semua pihak yang berada dalam jaringan (dalam sistem publik).
3. Desentralisasi, tidak ada otoritas tertentu atau otoritas pusat yang mengontrol seluruh jaringan pada blockchain.
4. Immutability, apabila data yang telah dicatat di dalam blockchain maka data tersebut tidak dapat diubah maupun dihapus tanpa consensus dari seluruh jaringan, sehingga dalam konteks ini hal ini dapat mencegah penipuan, manipulasi data, serta penghapusan bukti.

[7] Gavin Wood, *Ethereum: A Secure Decentralised Generalised Transaction Ledger*, diakses melalui www.ethereum.org,

Dan masih terdapat kelebihan-kelebihan dari teknologi blockchain yang lain.

Dalam penipuan online blockchain tidak dapat menghilangkan penipuan itu secara total, tetapi secara signifikan teknologi ini dapat mengurangi ruang gerak bagi pelaku untuk melakukan manipulasi, pemalsuan, serta penghilangan jejak secara digital. Dengan penggunaan yang tepat terutama dibidang e-commerce, fintech, serta perlindungan data, teknologi blockchain ini bisa digunakan sebagai alat untuk pencegahan penipuan online yang kuat.

Peraturan sektor perbankan ialah sebuah rangkaian kebijakan serta ketentuan hukum yang dibuat oleh pemerintah dan lembaga pengawas seperti Otoritas Jasa Keuangan (OJK) serta Bank Indonesia (BI) untuk mengatur mengenai operasional, tata kelola, serta pengawasan institusi perbankan, dengan tujuan untuk menjaga stabilitas sistem keuangan nasional, melindungi kepentingan nasabah, serta untuk memastikan bahwa aktivitas perbankan berjalan sesuai dengan prinsip yang ada dalam sektor perbankan yaitu prinsip kehati-hatian (prudential principle)[8]. Prinsip kehati-hatian dalam sektor perbankan merupakan asas fundamental di dalam penyelenggaraan kegiatan perbankan di Indonesia yang mewajibkan lembaga bank untuk mengelola risiko secara cermat untuk menjaga

[8] Otoritas Jasa Keuangan, *Buku Saku OJK: Perbankan*, OJK, Jakarta, 2022, hlm. 3

kepercayaan masyarakat[9]. Regulasi sektor perbankan yang ada mencakup mengenai aspek modal minimum, manajemen resiko, perlindungan konsumen, dan keamanan teknologi informasi yang digunakan di dalam operasional bank, termasuk di dalamnya pengaturan mengenai sistem pembayaran digital[10]. Tetapi, di dalam praktiknya, regulasi pada sektor perbankan menghadapi berbagai tantangan yang signifikan dengan adanya bentuk kejahatan baru yang menggunakan teknologi canggih, seperti contohnya penipuan online yang berbasis deepfake[11]. Regulasi di Indonesia saat ini, termasuk Undang-Undang Nomor 10 Tahun 1998 mengenai Perbankan, serta Peraturan OJK dan BI, belum secara menyeluruh mengakomodasi risiko serta modus operandi baru ini secara spesifik[12].

Permasalahan yang membuat maraknya terjadi tindak pidana penipuan online berbasis deepfake ini antara lain ialah karena kurangnya mekanisme autentikasi serta verifikasi identitas yang kuat di dalam sektor perbankan, sehingga terdapat celah di dalam pengaturan kemanan digital yang belum mengadopsi teknologi terbaru secara optimal, dan kekosongan regulasi (regulasi vacuum) terkait dengan penggunaan teknologi blockchain

[9] Rachmadi Usman, *Aspek-Aspek Hukum Perbankan di Indonesia*, Gramedia Pustaka Utama, Jakarta, 2018, hlm. 45.

[10] Bank Indonesia, *Blueprint Sistem Pembayaran Indonesia 2025*, Bank Indonesia, Jakarta, 2019, hlm. 12.

[11] Danielle Keats Citron dan Robert Chesney, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *California Law Review*, Vol. 107, No. 6, 2019, hlm. 1753.

[12] Barda Nawawi Arief, *Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan Teknologi*, Kencana, Jakarta, 2020, hlm. 89.

sebagai salah satu alat pencegahan[13]. Sistem regulasi yang ada saat ini juga belum secara menyeluruh mengatur mengenai kolaborasi antara lembaga seperti Kepolisian, Kementerian Komunikasi dan Informatika, dan Penyedia Teknologi Keamanan di dalam mengatasi ancaman digital yang terus berkembang saat ini. Sehingga hal ini, menyebabkan bank serta lembaga keuangan yang lainnya rentan terhadap akses illegal serta manipulasi yang dilakukan dengan menggunakan teknologi deepfake, yang dimana hal ini sangat merugikan nasabah serta menciptakan risiko sistemik di dalam sektor perbankan.

Sebagai respons terhadap permasalahan yang ada ini, perlu adanya pembaharuan regulasi yang adaptif serta komprehensif yang mengintegrasikan teknologi blockchain untuk dapat memperkuat sistem keamanan digital. Teknologi blockchain sendiri menawarkan karakteristik seperti desentralisasi, transparansi, immutabilitas, serta keamanan kriptografi yang dapat memperkuat mekanisme verifikasi identitas, mengurangi peluang untuk manipulasi data, dan menyediakan jejak audit yang dapat dipertanggung jawabkan secara hukum. Regulasi ini juga harus mengadopsi kebijakan seperti multi-factor authentication yang berbasis AI, audit algoritma, dan edukasi digital untuk nasabah serta pegawai bank untuk dapat memperkuat pertahanan terhadap penipuan online berbasis deepfake tersebut. Di Indonesia sendiri, adopsi dari teknologi blockchain ini masih

[13] Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3rd ed., Wiley, 2020, hlm. 112.

berada pada tahap awal, terutama pada sektor keuangan dan logistik. Tetapi, potensi dari teknologi ini untuk dapat diterapkan di dalam pencegahan tindak pidana penipuan online sangat besar. Dengan adanya penguatan di bagian regulasi serta peningkatan literasi digital, blockchain dapat menjadi sebuah pilar utama di dalam meningkatkan keamanan dalam transaksi digital di Indonesia.

B. Rumusan Masalah

1. Bagaimana pengaturan sektor perbankan atas penggunaan teknologi blockchain yang dapat berfungsi untuk mencegah penipuan online berupa deepfake?
2. Bagaimana pengadopsian teknologi blockchain ke dalam pengaturan sektor perbankan untuk mencegah penipuan online berupa deepfake?

C. Tujuan Penelitian

1. Menganalisis serta menjelaskan mengenai penggunaan teknologi blockchain ke dalam sektor perbankan dalam mencegah penipuan online berupa deepfake.
2. Mengidentifikasi serta menganalisis pengadopsian teknologi blockchain dalam pengaturan sektor perbankan untuk mencegah penipuan online berupa deepfake.

D. Manfaat Penelitian

1. Secara teoritis: memberikan kontribusi pada pengembangan ilmu hukum di bidang hukum siber dan teknologi, melalui analisis pada

regulasi yang ada serta integrasinya dengan kemajuan teknologi seperti blockchain serta bidang keamanan digital. Selain itu juga dapat menambah literatur bagi akademik terhadap penerapan teknologi informasi di dalam sistem hukum guna untuk mencegah tindak pidana.

2. Secara praktis: dapat memberikan rekomendasi kepada para pemangku kebijakan di dalam menyusun atau pun merevisi regulasi yang terkait dengan pencegahan penipuan online dengan mempertimbangkan penggunaan teknologi blockchain. Serta menjadi referensi untuk apparat penegak hukum, regulator, dan para penyedia layanan digital di dalam meningkatkan suatu sistem keamanan identitas para pengguna online.

E. **Tinjauan Pustaka**

Untuk memberikan kontribusi terhadap ilmu pengetahuan, memberikan solusi dan menunjukkan orisinalitas, penulis membandingkan dengan penelitian terdahulu yang ada kaitannya dengan Teknologi Blockchain yang berhubungan dengan tindak pidana. Adapun hasil penelitian yang pernah dilakukan sebagai berikut:

No.	Nama Peneliti	Judul Penelitian	Imti Penelitian
1.	Blassyus Bevry Sinaga, Raia Putri Noer Azzura	Pengaturan Teknologi Blockchain sebagai Instrumen Pembangunan Penegakan Hukum Berbasis Digital &	Penelitian ini membahas mengenai teknologi seperti *smart contracts*, sistem identitas

		Mewujudkan Masyarakat Berkeadilan di Era Society 5.0	terdesentralisasi, dan tokenisasi hak privasi menawarkan kemajuan, namun juga memunculkan tantangan seperti peningkatan *Cybercrime* dan penipuan online. Meskipun blockchain memiliki potensi besar sebagai sarana transparansi hukum, belum ada regulasi spesifik di Indonesia yang mengoptimalkan teknologi ini. Regulasi holistic yang mendukung adaptasi blockchain diperlukan untuk menciptakan penegakan hukum yang lebih adil, efektif,

			dan humanis, serta mendorong kemajuan Indonesia dalam Era Society 5.0.
2.	Andi Ahmad Munajat, Hudi Yusuf	Peran Teknologi Informasi Dalam Pencegahan Dan Pengungkapan Tindak Pidana Ekonomi Khusus: Studi Tentang Kejahatan Keuangan Berbasis Digital	Penelitian ini menganalisis mengenai peran penting dari teknologi informasi seperti kecerdasan buatan, big data, serta blockchain di dalam mencegah serta mengungkap tindak pidana ekonomi digital di sektor keuangan. Studi dalam penelitian ini mengkaji mengenai kerangka hukum Indonesia, terutama UU ITE serta regulasi Pencucian

			Uang, yang mengatur penggunaan teknologi dalam penegakan hukum.
3.	Muhammad Syafiq Wafi, Aloysius Wisnubroto, Yudi Prayudi	Kejahatan Deepfake Berbasis Artificial Intellegence: Suatu Konsepsi pada Penggunaan Asas Culpabilitas Sebagai Pembaharuan Pertanggungjawaban Pidana.	Penelitian ini membahas, mengenai pembaruan konsep pertanggungjawaban pidana, terkhusus melalui perluasan asas culpabilitas. Penelitian ini merekomendasikan pembetukan regulasi terkait tata kelola teknologi berbasis risk assessment, risk management, serta impact assessment.
4.	Debora	Penegakan Hukum Pidana Terhadap Pelaku Tindak Pidana Penipuan	Penelitian ini membahas pengaturan dan

		Investasi Ilegal Dengan Cryptocurrency Pada Pasar Komoditi.	penegakan hukum terhadap pelaku penipuan investasi illegal yang melibatkan cryptocurrency di pasar komoditi (Bappebti), sesuai dengan Undang-Undang Nomor 32 Tahun 1997 tentang Perdagangan Berjangka Komoditi. Tetapi, kemudahan investasi dalam cryptocurrency juga memunculkan tindakan penipuan.

Berdasarkan empat penelitian terdahulu jelas bahwa regulasi mengenai teknologi blockchain di Indonesia belum ada. Sedangkan penelitian ini menfokuskan pada pertanyaan mengenai Bagaimana pengaturan sektor perbankan atas penggunaan teknologi blockchain yang

dapat berfungsi untuk mencegah penipuan online berupa deepfake, kedua mengenai bagaimana pengadopsian teknologi blockchain ke dalam pengaturan sektor perbankan untuk mencegah penipuan online berupa deepfake.. Namun, empat peneliti terdahulu belum membahas mengenai pertanyaan yang akan di teliti oleh peneliti saat ini.

F. Teori atau Doktrin

1. Teori Blockchain

Blockchain ini berasal atau berakar melalui pengembangan sebuah sistem distributed ledger yang dimana memungkinkan untuk pencatatan transaksi secara terbuka, terdesentralisasi, serta tidak dapat diubah atau dimanipulasi. Dalam sistem blockchain memanfaatkan jaringan yang bernama *peer-to-peer* serta kriptografi yang digunakan untuk menjaga keamanan dan keaslian suatu data.

Blockchain ini pertama kali diperkenalkan secara meluas oleh tokoh yang bernama Satoshi Nakamoto di dalam makalahnya pada tahun 2008 dengan judul *Bitcoin: A Peer-to-peer Electronic Cash System.*[14] Tetapi, pada saat ini penerapan dari blockchain ini telah meluas ke berbagai sektor tidak hanya pada sektor mata uang kripto Bitcoin, termasuk sistem identitas digital, smart contracts (kontrak pintar), hingga pada pencegahan kejahatan digital seperti penipuan identitas serta manipulasi data saat ini sudah menggunakan sistem blockchain.

[14] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008, https://bitcoin.org/bitcoin.pdf. , diakses pada tanggal 25 Mei 2025

Blockchain sendiri memiliki beberapa karakteristik, yaitu meliputi :

a. Desentralisasi
b. Immutability
c. Transparansi
d. Keamanan Kriptografi

Dalam penelitian ini yang mengenai pencegahan penipuan berbasis deepfake, teknologi blockchain memiliki potensi untuk dapat digunakan untuk menyimpan metadata otentik dari sebuah file video/audio, melacak jejak digital seseorang, serta menjamin keaslian suatu identitas. Sehingga teknologi ini dapat berperan sebagai sistem *notarization digital* untuk menunjukkan apakah sebuah konten itu telah dimodifikasi atau tidak sejak konten itu diunggah pertama kalinya.

Blockchain adalah suatu teknologi yang dirancang untuk mencatat serta menyimpan data ke dalam bentuk buku besar digital (distributed ledger), dimana setiap transaksi akan dicatat secara permanen dan tidak dapat dirubah (immutable). Teknologi blockchain berbasis kepada prinsip desentralisasi, dimana tidak ada otoritas tunggal yang mengendalikan jaringan, melainkan seluruh node atau pengguna di dalam sistem ini dapat berperan dalam validasi dan pencatatan transaksi[15].

[15] Don Tapscott, *Blockchain Revolution: How Technology is Changing Money, Business, and the World*, Penguin Books, 2016, hlm. 45.

Blockchain memiliki fitur utama yang meliputi transparansi, keamanan, dan efisiensi. Transparansi dalam blockchain dicapai dari sistem pencatatan terbuka yang dapat memungkinkan semua pengguna di dalam jaringan untuk dapat memverifikasi data secara real-time. Kemanan di dalam blockchain didukung oleh penggunaan teknologi enkripsi kriptografi, yang membuat data sulit untuk diretas atau dimanipulasi[16]. Blockchain juga memungkinkan efisiensi yang tinggi dalam proses transaksi melalui otomatisasi yang berbasis smart contracts, yaitu suatu protocol yang mengeksekusi perjanjian secara otomatis tanpa perlunya pihak ketiga[17].

Aplikasi blockchain tidak hanya terbatas pada mata uang kripto *(cryptocurrency)* seperti contohnya Bitcoin atau Ethereum, namun juga meluas ke bergaia sektor, termasuk keuangan, logistic, kesehatan, dan hukum. Di dalam konteks pencegahan tindak pidana penipuan online, blockchain memberikan solusi untuk meminimalisasikan risiko penipuan melalui transparansi dan akuntabilitas transaksi digital[18].

Di Indonesia saat ini, adopsi teknologi blockchain masih dalam tahap pengembangan, tetapi potensi untuk meningkatkan keamanan pada transaksi digital ini semakin disadari. Dengan adanya regulasi yang mendukung dan penguatan literasi digital, blockchain ini diharapkan

[16] Nakamoto, Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System*, diakses melalui www.bitcoin.org,

[17] Gavin Wood, *Ethereum: A Secure Decentralised Generalised Transaction Ledger*, Ethereum Research Publications, 2014, hlm. 25.

[18] Brian Krebs*, Cybersecurity and Online Fraud: A Comprehensive Guide,* Cambridge Press, 2021, hlm. 87.

dapat menjadi teknologi kunci di dalam membangun ekosistem digital yang lebih aman[19].

2. Teori Hukum Pidana Preventif dan Represif

Penegakan hukum di dalam hukum pidana memiliki dua dimensi utama, yaitu yang pertama adalah preventif yang berarti sebuah pencegahan dan kedua adalah represif yang berarti penindakan. Pada aspek preventif ini ia menitik beratkan kepada tujuannya untuk mencegah terjadinya suatu tindak pidana dengan cara memberikan edukasi hukum, pengawasan, serta penerapan teknologi untuk sarana pencegahan. Sedangkan pada aspek represif lebih menitik beratkan kepada fungsinya yaitu sebagai sarana untuk penindakan terhadap pelaku yang telah melakukan tindak pidana. Dimana hal ini mencakup kepada proses penyelidikan, penuntutan, peradilan, dan pada proses pemidanaan.

Barda Nawawi Arief merupakan dalah satu tokoh hukum Indonesia yang menjelaskan mengenai penegakan hukum pidana idealnya lebih mengedepankan kepada aspek preventif dan represif agar tidak terjadinya "overkriminilasasi". Selain itu, ia juga mengemukakan bahwa hukum pidana harus ditempatkan secara proporsional, tidak hanya sebagai sebuah alat yang represif, namun juga sebagai instrument dalam mencegah kejahatan sejak dini dengan pendekatan yang adaptif

[19] Kementerian Komunikasi dan Informatika, *Potensi Blockchain di Indonesia: Peluang dan Tantangan Tahun 2023,* diakses melalui www.kominfo.go.id, pada 14/12/2024.

serta efisien.[20] Dalam penelitian ini penggunaan teknologi blockchain menjadi salah satu bentuk pendekatan preventif yang modern untuk mencegah kejahatan digital sebagai sistem pelacakan serta verifikasi data. Sehingga penggunaan teknologi blockchain di dalam mencegah tindak pidana penipuan deepfake ini merupakan bentuk dari preventif criminal law enforcement, yaitu upaya hukum untuk dapat mencegah kejahatan sebelum kejahatan itu terjadi. Akan tetapi, sistem ini tetap dapat mendukung pendekatan represif karena blockchain dapat menyimpan bukti yaitu sebagai bukti digital yang nantinya dapat dipertanggungjawabkan secara hukum.

3. Teori Hukum dan Teknologi

Teori mengenai hukum dan teknologi untuk berasal dari kesadaran akan perkembangan teknologi yang seringkali lebih cepat dibandingkan dengan hukum, sehingga hukum perlu terus melakukan adaptasi. Dalam teori ini mempelajari mengenai bagaimana hukum merespons dari adanya perkembangan teknologi dan bagaimana teknologi ini dapat digunakan untuk memperkuat fungsi dari hukum itu sendiri.

Salah seorang ahli hukum yang berasal dari Amerika, bernama Lawrence Lessig di dalam bukunya yang berjudul *Code and Other Laws of Cyberspace* ia menyatakan bahwa di dalam dunia digital, kode atau

[20] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Jakarta: Kencana, 2008, hlm. 23.

software ini dapat berfungsi seperti hukum. Dimana struktur di dalam teknologi ini membentuk perilaku pengguna seperti halnya norma hukum membentuk masyarakat[21]. Dengan kata lain, desain pada sistem teknologi seperti contohnya blockchain ini dapat menggantikan atau memperkuat sebuah norma hukum. Dalam hal ini blockchain tidak hanya dilihat sebagai sebuah alat bantu, namun juga sebagai bagian dari ekosistem hukum yang baru di dalam dunia digital. Hukum perlu mengakomodasi penggunaan teknologi di dalam melindungi masyarakat dari kejahatan kejahatan di dunia siber salah satunya adalah kejahatan deepfake. Sehingga teori ini dapat memperkuat landasan bahwa "teknologi sebagai sarana regulatif" dapat digunakan untuk mencegah terjadinya kejahatan di dunia digital yang bersifat disruptif.

4. Penipuan online

Penipuan online merupakan suatu bentuk kejahatan siber atau disebut *Cybercrime* yang terus saja meningkat dengan seiring perkembangan teknologi digital. Penipuan terjadi disaat individua tau suatu kelompok secara sengaja memanfaatkan internet untuk menipu korban demi untuk mendapatkan keuntungan finansial atau tujuan lain yang dianggap merugikan pihak korban. Bentuk-bentuk penipuan sangatlah beragam mulai dari pencurian identitas, manipulasi data, penipuan e-commerce, phishing, dan juga skema investasi palsu[22].

[21] Lawrence Lessig, *Code and Other Laws of Cyberspace*, New York: Basic Books, 1999, hlm. 6-7.

[22] Brian Krebs*, Cybercrime and Online Fraud: A Comprehensive Guide*, Cmabridge Press, 2021, hlm. 30.

Karakteristik utama dalam penipuan online adalah sifatnya yang lintas batas serta anonim, sehingga hal ini yang mempersulit penegakan hukum serta pelacakan pelaku[23]. Penipuan kerap kali menggunakan kelemahan di dalam sistem keamanan digital, seperti kurangnya enkripsi data, rendahnya kesadaran pengguna terhadap ancaman siber yang ada, serta celah pada regulasi yang mengatur mengenai perlindungan transaksi daring[24].

Dari data global menunjukkan bahwa tindak pidana penipuan online saat ini terus terjadi peningkatan secara signifikan. Dilansir melalui laporan *Cybercrime* report 2023, ada sekitar 36 % dari semua kejahatan siber yang dilaporkan berhubungan dengan penipuan online[25]. Di negara Indonesia, penipuan online menjadi salah satu bentuk kejatahan siber yang paling sering terjadi, sebagaimana tercatat pada laman Kementerian Komunikasi dan Informatika. Kasus seperti phishing, manipulasi pembayaran di dalam transaksi e-commerce, dan skema investasi illegal sering kali dilaporkan[26].

5. Teori Peraturan Perbankan

Regulasi mengenai perbankan di Indonesia dibuat dengan tujuan untuk menjaga stabilitas sistem keuangan, melindungi nasabah, dan

[23] Don Tapscott, *Digital Economy and Cybersecurity Challenges*, Penguin Books, 2018, hlm. 95.

[24] Gavin Woods, *Cybersecurity Trends in the Age of Blockchain*, Ethereum Research Publications, 2020, hlm. 56.

[25] *Cybercrime Report 2023, Annual Report on Global Cybersecurity Trends*, diakses melalui www.cyberreport.com pada 10/12/2024

[26] Kementerian Komunikasi dan Informatika, *Laporan Tahunan Penanganan Kejahatan Siber di Indonesia 2022*, diakses melalui www.kominfo.go,id pada 10/12/2024

memastikan kepatuhan terhadap standar internasional. Peraturan perbankan yang relevan antara lain yaitu Undang-Undang Nomor 10 Tahun 1998 mengenai Perbankan, Undang-Undang Nomor 21 Tahun 2011 mengenai Otoritas Jasa Keuangan atau OJK, Undang-Undang Nomor 8 Tahun 2010 mengenai Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, dan Peraturan OJK serta Bank Indonesia terkait dengan keamanan sistem pembayaran. Dalam konteks inovasi teknologi saat ini, Otoritas Jasa Keuangan mengeluaskan kebijakan berupa *regulator sandbox* yang digunakan untuk menguji produk atau layanan yang berbasis teknologi finansial, termasuk di dalamnya teknologi blockchain.

Pengaturan pada sektor perbankan terkait dengan kerangka pencegahan penipuan online yang berbasis deepfake harus didasarkan pada teori regulasi yang komprehensif serta adaptif terhadap perkembangan teknologi digital. Teori ini menenkankan kepada pentingnya pembuatan kebijakan yang tidak hanya mengacu kepada aspek hukum formal saja, namun juga mengintegrasikan inovasi teknologi seperti *blockchain* serta kecerdasan buatan atau *AI* sebagai salah satu alat utama yang digunakan dalam penguatan sistem keamanan serta verifikasi identitas digital. Di dalam kerangka ini, prinsip kehati-hatian atau prudential principle menjadi landasan utama yang mengarahkan lembaga bank dan regulator untuk mengelola risiko secara menyeluruh, termasuk dengan risiko tambahan yang timbul dari

penggunaan teknologi deepfake, seperti contohnya manipulasi data serta identitas yang palsu.

Regulasi harus mendorong adanya implementasi teknologi keamanan canggih, seperti *multi-factor authentication* berbasis kecerdasan buatan atau *AI* serta *Blockchain* yang dapat memverifikasi keaslian sebuah data transaksi secara real-time, sehingga hal ini dapat mendeteksi setiap upaya manipulasi data serta pencegahan dini terhadap kejahatan berbasis deepfake. Selain dari aspek teknologi, terdapat aspek perlindungan konsumen juga yang menjadi fokus utama, dimana lembaga bank wajib untuk memberikan transparansi, edukasi, dan mekanisme perlindungan terhadap risiko yang dihadirkan oleh ancaman digital saat ini. Regulasi yang responsif serta fleksibel akan memastikan bahwa sistem pengaturan dapat mengikuti perkembangan teknologi ribuan mile di dalam mengantisipasi modus kejahatan baru yang semakin hari semakin canggih. Senggiha dengan demikian, teori terkait pengaturan perbankan ini memiliki peran sebagai kerangka normatif serta operasional yang mampu menciptakan ekosistem digital yang aman, terjamin, serta mampu menumbuhkan kepercayaan publik terhadap sistem keuangan nasional. Pendekatan ini juga dapat mendukung terciptanya ekosistem inovatif yang mengedepankan keberlanjutan, pengelolaan risiko, dan perlindungan hak-hak nasabah di era digital ini, di mana keseluruhan ini penting di dalam menghadapi tantangan dari kejahatan cyber yang semakin kompleks serta maju. Ti

njauan pustaka ini penting untuk memahami sejauh mana regulasi yang ada untuk dapat mengakomodasi penerapan teknologi blockchain di dalam sistem perbankan serta pencegahan tindak pidana penipuan online berbasis deepfake.

G. **Definisi Operasional**

1. Teknologi Blockchain

   Teknologi blockchain ialah suatu sistem yang berbasis data yang terdistribusi untuk menyimpan data dalam bentuk blok-blok, dimana blok-blok ini saling terhubung satu sama lain dan diamankan dengan menggunakan kriptografi. Pada setiap block berisikan Kumpulan transaksi yang sudah diverifikasi serta tidak dapat diubah setelah tercatat pada sistem, menciptakan struktur data yang bersifat *immutable* serta *transparent*.

   Teknologi blockchain memiliki beberapa ciri-ciri operasionalnya, yaitu:

   a. Desentralisasi, yang dimaksud dengan desentralisasi dalam blockchain ialah transfer control serta pengambilan keputusan dari entitas terpusat (individu, organisasi, atau grup) ke dalam jaringan terdistribusi. Dimana jaringan terdesentralisasi ini bertujuan atau berusaha untuk dapat mengurangi tingkat kepercayaan yang harus diberikan oleh perserta satu sama lain atau antar perserta, serta untuk mencegah kemampuan mereka untuk mengerahkan otoritas atau control satu sama lain dengan cara yang menurunkan fungsi jaringan.

b. Immutability, dalam blockchain immutability ialah kemampuan teknologi blockchain digunakan untuk memastikan data transaksi lama tidak dapat diubah. Sehingga semua transaksi menggunakan bitcoin maupun asset kripto yang lain dicatat secara permanen serta dapat dilihat oleh semua orang, maka dari itu mustahil bagi entitas mana pun untuk dapat mengubahnya, mengganti, ataupun memalsukan data yang telah disimpan pada blockchain. Immutability di dalam blockchain dapat digunakan untuk membantu meningkatkan kepercayaan serta sistem audit pada saat ini.

c. Transparansi, dalam teknologi blockchain hal ini merujuk kepada sifat keterbukaan data transaksi yang tercatat pada sistem blockchain. Dimana dalam hal ini semua pihak di dalam jaringan dapat melihat serta memverifikasi data yang tercatat, meskipun identitas pengguna tetap anonim. Transparansi ini dapat menciptakan akuntabilitas serta dapat mengurangi resiko manipulasi data yang disebabkan oleh informasi tidak dapat dirubah secara sepihak tanpa adanya persetujuan dari consensus jaringan.

d. Smart Contract, merupakan suatu program atau sebuah kode computer yang berjalan secara otomatis di atas jaringan blockchain serta akan mengeksekusi perintah secara otomatis ketika syarat-syarat tertentu sudah terpenuhi. Dalam smart contract tidak diperlukannya pihak ketiga seperti contohnya notaris atau lembaga keuangan, untuk dapat memastikan berjalannya perjanjian karena

sistem blockchain sudah menjamin pelaksanaannya secara otomatis serta aman.

e. Keamanan Kriptografi, ialah mekanisme perlindungan data yang digunakan di dalam blockchain untuk menjaga integritas, autentikasi, serta kerahasiaan informasi. Teknologi yang digunakan dalam hal ini ialah menggunakan algoritma matematika kompleks untuk mengenkripsi data serta mengamankan sebuah proses transaksi, maka sulit untuk diretas atau dimanipulasi.

Ruang lingkup operasional yang digunakan dalam penelitian ini terbatas pada teknologi blockchain yang digunakan sebagai alat bantu di dalam mendeteksi, mencatat, serta mengautentikasi transaksi digital untuk dapat meminimalkan potensi terjadinya penipuan online, khususnya di dalam platform yang berbasis digital seperti contohnya e-commerce, keuangan daring, serta sistem identitas digital.

2. Tindak pidana penipuan online, ialah segala bentuk dari perbuatan yang dilakukan menggunakan atau melalui sarana elektronik atau jaringan internet, yang bertujuan untuk menguntungkan diri sendiri maupun orang lain yang dilakukan secara melawan hukum, serta merugikan korban baik secara finansial maupun psikologis. Penipuan online ini masuk ke dalam golongan kejahatan siber dan diatur di dalam peraturan perundang-undangan yaitu KUHP dan UU No. 19 Tahun 2016 mengenai Informasi dan Transaksi Elektronik (UU ITE).

3. Pencegahan, merupakan suatu serangkaian tindakan atau kebijakan yang bersifat proaktif untuk mengurangi potensi terjadinya suatu tindak pidana. Di dalam hal ini, pencegahan dimaksudkan sebagai langkah-langkah secara teknologis serta regulative yang dapat diterapkan sebelum terjadinya kejahatan penipuan online, dengan cara memanfaatkan teknologi blockchain sebagai instrument utamanya.
4. Pengaturan sektor perbankan, ialah merupakan suatu rangkaian kebijakan, peraturan, serta mekanisme control yang dirancang serta diterapkan secara sistematis oleh lembaga-lembaga yang berwenang di bidang keuangan, khususnya Otoritas Jasa Keuangan atau OJK serta Bank Indonesia. Dengan tujuan untuk memastikan bahwa seluruh aktivitas perbankan, mulai dari pembukaan serta pengelolaan rekening, pemberian kredit, transaksi pembayaran, sampai kegiatan investasi berjalan sesuai dengan ketentuan hukum yang berlaku serta prinsip kehati-hatian. Pengaturan sektor perbankan sendiri meliputi beberapa aspek, yaitu aspek hukum, teknis, serta pengawasan yang diimplementasikan untuk menjaga stabilitas dan integritas sistem perbankan nasional. Pengaturan ini juga bertujuan untuk melindungi kepentingan para nasabah, menjaga kepercayaan publik terhadap perbankan, dan mencegah praktik-praktik illegal serta merugikan seperti contohnya pencucian uang, penipuan, serta kecurangan digital termasuk di dalamnya jenis-jenis dari penipuan online seperti yang sedang ramai saat ini yaitu deepfake.

H. **Metode Penelitian**

Penelitian ini menggunakan metode pendekatan yuridis normatif untuk mengkaji peran teknologi blockchain dalam mencegah tindak pidana penipuan online. Fokus pendekatan ini pada analisis terhadap peraturan perundang-undangan yang relevan, prinsip hukum, serta doktrin hukum yang terkait dengan teknologi blockchain dan kejahatan cyber.

1. Sumber data pada penelitian ini memanfaatkan:
    a. Data primer, berupa perundang-undangan terkait dengan teknologi informasi, seperti Undang-undang No. 11 Tahun 2008 tentang informasi dan transaksi elektronik (UU ITE) serta peraturan tambahan terkait teknologi blockchain.
    b. Data sekunder, berupa literatur, jurnal hukum, dan laporan dari Lembaga internasional terkait keamanan digital dan penggunaan blockchain.
2. Teknik pengumpulan data

    Pengumpulan data melalui studi Pustaka, yang mencakup penelaahan literatur hukum dan dokumen resmi, serta studi kasus untuk menganalisis implementasi blockchain dalam pencegahan kejahatan cyber.
3. Teknik analisis data

    menginterpretasikan data hukum dan menghubungkannya dengan fenomena tindak pidana penipuan online serta untuk menganalisis relevansi blockchain dalam pencegahan penipuan online.

Metode penelitian ini diharapkan mampu memberikan gambaran komprehensif tentang potensi blockchain sebagai Solusi hukum yang inovatif dalam mencegah kejahatan di ruang digital.

I. **Sistematika Penulisan**

BAB I PENDAHULUAN : Pada bagian ini berisikan tentang latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, tinjauan pustaka, teori atau doktrin, definisi operasional, metode penelitian, sistematika penulisan.

BAB II LANDASAN TEORI : Bagian BAB II akan berisi mengenai tinjauan umum terkait pengadopsian, teknologi blockchain dalam pengaturan sektor perbankan, dan penipuan online berupa deepfake.

BAB III PEMBAHASAN : Membahas mengenai hasil dari penelitian dan pembahasan yang terdiri atas bagaimana pengaturan sektor perbankan atas penggunaan teknologi blockchain yang dapat berfungsi untuk mencegah penipuan online berupa deepfake dan bagaimana pengadopsian teknologi blockchain ke dalam pengaturan sektor perbankan untuk mencegah penipuan online berupa deepfake.

BAB IV PENUTUP : Berisi penutup pembahasan tesis yang berisi mengenai kesimpulan dan saran dari teori atau doktrin dan rumusan masalah yang dituangkan ke dalam pembahasan BAB III.

BAB II

TINJAUAN UMUM PENGADOPSIAN, TEKNOLOGI BLOCKCHAIN DALAM PENGATURAN SEKTOR PERBANKAN, PENIPUAN ONLINE BERUPA DEEPFAKE

A. Pengadopsian

Pengadopsian ialah proses pengangkatan atau penerimaan formal, seperti contohnya pengadopsian anak secara hukum ataupun penerapan inovasi. Selain itu pengadopsian juga merupakan sebuah proses adaptasi serta integrasi elemen baru secara formal ke dalam sebuah sistem yang telah ada, baik itu secara sosial, hukum, ataupun teknologi[27], yang digunakan untuk mencapai manfaat dalam jangka panjang seperti peningkatan efisiensi maupun perlindungan. Pada dasarnya, pengadopsian ini melibatkan adaptasi permanen dengan melalui tahapan identifikasi kebutuhan, persetujuan para pihak terkait, verifikasi, dan pengesahan yang dilakukan oleh otoritas yang berwenang. Dilihat secara historis, pengadopsian muncul dari konsep hukum seperti pengakatan anak berdasarkan Undang-Undang Nomor 23 Tahun 2002 mengenai perlindungan anak, di mana prosesnya ini melibatkan persetujuan, verifikasi, serta pengadilan untuk transfer hak asuh[28], sehingga anak mendapatkan perlindungan hukum, waris, serta keluarga baru. Sementara itu, pengadopsian terkait dengan inovasi teknologi baru mengikuti teori Diffusion of Innovations oleh Everett

[27] Everett M. Rogers, *Diffusion of Innovations*, 5th Edition, Free Press, New York, 2003, hlm. 12

[28] Undang-Undang Nomor 23 Tahun 2002 tentang Perlindungan Anak.

Rongers, yang meliputi tahapan pengetahuan, persuasi, keputusan, implementasi, serta konfirmasi, seperti contohnya UMKM di Yogyakarta yang mengadopsi e-commerce yang berfungsi untuk meningkatkan penjualan hingga 20-30%. Sehingga secara historisnya, konsep pengadopsian ini berakar dari hukum romawi kuno serta adat jawa seperti "anak piara", yang berkembang melalui burgelijk wetboek pada era Belanda, hingga pada modernisasi pasca kemerdekaan yang menekankan pada hak prioritas anak, dan program seperti making Indonesia 4.0 untuk mengadopsi mengenai AI serta Blockchain. Manfaat dari pengadopsian ini mencakup stabilitas keluarga dilihat dari pengadopsian anak, produktivitas yang lebih tinggi dimana perdagangan menggunakan Gojek mengalami kenaikan pendapatan hingga 40% serta integrasi sosial inklusif, meskipun demikian tetap terdapat tantangan dalam pengadopsian ini seperti resistensi budaya, birokrasi yang panjang (6-12 bulan), dan risiko kegagalan integrasi yang disebabkan oleh kurangnya pelatihan.

Pengadopsian teknologi blockchain dalam pengaturan sektor perbankan di Indonesia, mengintegrasikan desentralisasi ledger untuk digunakan sebagai audit trail anti-manipulasi, smart contracts otomatis, serta kriptografi[29] untuk deteksi deepfake melalui metadata video atau audio autentik. Regulasi POJK No.12/POJK.03/2021 mengenai Sandbox regulasi yang mendukung uji coba dari inovasi-inovasi teknologi baru dalam sektor

[29] Don Tapscott & Alex Tapscott, *Blockchain Revolution*, Penguin Random House, New York, 2016, hlm. 32-35.

keuangan, sementara itu UU No. 10/1998 mengenai Perbankan menekankan kepada prinsip kehati-hatian terhadap risiko kejahatan siber. Manfaat dari pengadopsian teknologi blockchain ke dalam pengaturan sektor perbankan ini salah satunya ialah pengurangan kerugian USD 8,5 miliar global dari cybercrime berdasarkan data tahun 2022 melalui pencegahan proaktif[30].

Pengadopsian teknologi blockchain dalam pengaturan sektor perbankan di Indonesia memiliki tantangan yang mencakup mengenai regulasi vacuum atau kekosongan regulasi, resistensi SDM, serta skalabilitas jaringan[31], di mana kurangnya aturan khusus seperti POJK No. 13/POJK.03/2021 yang dianggap masih abu-abu terkait dengan asset kripto serta smart contracts sehingga hal tersebut memicu adanya ketidakpastian hukum, sementara itu survei BI pada tahun 2024 menunjukkan bahwa hanya 35% dari pegawai perbank di Indonesia yang melek terhadap teknologi blockchain, yang disebabkan oleh buadaya hierarkis pada bank BUMN sepertu contohnya BRI serta Mandiri, ditambah juga dengan bottleneck transaksi per detik (TPS) yang rendah di Blockchain publik seperti Ethereum yang tak bisa menangani jutaan nasabah harian di negara dengan 300 juta penduduk. Tantangan yang ada ini diatasi melalui kolaborasi antara OJK-BI-Kominfo, pelatihan literasi digital, dan hybrid model on-chain/off-chain. Strategi dalam pengadopsian teknologi blockchain ke dalam pengaturan sektor perbankan harus dilakukan secara bertahap yaitu dengan

[30] Cybersecurity Ventures*, Cybercrime Report 2022*
[31] World Economic Forum, *Blockchain Beyond the Hype: A Practical Framework*, 2018.

pilot project di KYC (Know Your Customer), ekspansi ke transaksi real-time, serta evaluasi yang berbasiskan risk assessment untuk sinergi preventif-represif. Secara keseluruhan. Manfaat dari pengadopsian teknologi blockchain dalam sektor perbankan jangka panjang mencakup transparansi audit trail permanen, efisiensi biaya operasional 20-30% serta inklusi finansial untuk 100 juta unbanked, dengan prospek full adopsi di angkat 50% oleh bank besar melalui Indonesia Blockchain Consortium menjelang adanya UU Fintech baru pada tahun 2026 mendatang.

Sehingga dalam penelitian ini pengadopsian yang dimaksud lebih menitik beratkan kepada pengadopsian dari teknologi blockchain ke dalam regulasi perbankan untuk mencegah tindak pidana penipuan online berupa deepfake melalui verifikasi identitas immutable serta transparansi transaksi. Di mana secara hukum, pengadopsian teknologi ini dapat memperkuat Pasal 5 dalam UU ITE untuk bukti digital serta untuk mendukung teori Lessig yaitu code as law, di mana blockchain ini berfungsi sebagai norma regulatif[32]. Oleh karena itu, diperlukannya pembaharuan regulasi yang spesifik mengenai deepfake-blockchain, insentif fiskal untuk bank adopter dini, serta monitoring yang berbasis kecerdasan buatan atau AI yang digunakan untuk adaptasi berkelanjutan[33].

[32] Lawrence Lessig, *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999, hlm. 6-8

[33] OECD, *Regulatory Approaches to Artificial Intelligence*, OECD Publishing, Paris, 2021.

B. Teknologi Blockchain dalam Pengaturan Sektor Perbankan

Sektor perbankan di Indonesia pada era digital ini menghadapi tantangan yang cukup besar mengenai efisiensi, keamanan, serta transparansi[34]. Oleh sebab itu, diperlukannya teknologi yang dapat digunakan untuk meningkatkan sistem keamanan pada sektor perbankan, salah satu teknologi yang dirasa cocok yaitu teknologi blockchain. Teknologi blockchain di dalam pengaturan sektor perbankan ini merujuk kepada integrasi distributed ledger desentralisasi yang berfungsi untuk meningkatkan keamanan transaksi, verifikasi identitas[35], serta pencegahan tindak pidana penipuan online berupa deepfake, yang sesuai dengan regulasi OJK serta BI. Proses penggunaan teknologi blockchain dalam sektor perbankan ini didukung oleh UU No. 10/1998 mengenai Perbankan serta POJK No. 38/POJK.03/2016 mengenai risiko TI, dengan menggunakan sandbox regulasi untuk uji coba fintech.

Teknologi blockchain dalam sektor perbankan menawarkan potensi untuk perubahan cara transaksi yang dilakukan dalam sistem perbankan, meningkatkan efisiensi, serta dapat memperkuat sistem keamanan data pada sektor perbankan[36]. Pada sistem nasional dalam transaksi keuangan atau transaksi perbankan memerlukan bantuan dari pihak ketiga, sehingga hal ini

[34] Bank Indonesia, *Blueprint Sistem Pembayaran Indonesiaa (BSPI) 2025*, BI, Jakarta, 2019, hlm. 3-5

[35] Melanie Swan, *Blockchain: Blueprint for a New Economy*, O'Reilly Media, Sebastopol, 2015, hlm. 1-4.

[36] Don Tapscott & Alex Tapscott, *Blockchain Revolution*, Penguin Random House, New York, 2016, hlm. 45-48.

dinilai memakan waktu lama, serta meninggalkan celah keamanan[37]. Sedangkan dengan menggunakan teknologi blockchain transaksi keuangan bisa dilakukan secara langsung antara pihak-pihak yang bersangkutan tanpa memerlukan perantara pihak lain, kemudian segala transaksi dalam teknologi blockchain dicatat dalam bentuk blok yang terhubung secara kronologis, sehingga membentuk rantai blok yang aman dan transparan[38]. Keamanan di dalam teknologi blockchain ini di dasarkan pada kemanan kriptografi yang kuat serta prinsip konsensus yang melibatkan partisipasi dari banyak pihak[39].

Blockchain merupakan sistem pencatatan data permanen (immutable) dalam bentuk blok yang terhubung kriptografi, yang menawarkan desentralisasi, transparansi, immutability, serta konsensus terdistribusi seperti PoW/PoS[40]. Dalam sektor perbankan hal ini, meminimalkan single point of failure, menyediakan audit trail untuk digunakan oleh OJK/BI, serta selaras dengan prinsip kehati-hatian dalam sektor perbankan atau prudential principle). Namun selain kelebihan yang ditawarkan oleh teknologi blockchain untuk sektor perbankan seperti di atas, terdapat juga kekurangan dari teknologi blockchain tersebut yaitu skalabilitas yang rendah serta penggunaan energi yang tinggi, sehingga

[37] Andreas M. Antonopoulus, *Mastering Bitcoin*, O'Reilly Media, Sebastopol, 2017, hlm. 15-17.

[38] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, hlm. 2-3

[39] Arvind Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, Princeton University Press, 2016, hlm. 27-30.

[40] World Economic Forum, *Blockchain Beyond the Hype: A Practical Framework*, WEF, 2018.

memerlukan hybrid model dengan sistem legacy. Namun dalam pengaturan sektor perbankan belum terdapat regulasi yang secara spesifik mengatur mengenai deepfake-blockchain, sehingga hal ini menyebabkan terjadinya regulasi vacuum. Regulasi yang ada saat ini seperti UU No. 21/2011 mengenai OJK, UU No. 19/2016 mengenai ITE yaitu Pasal 5 UU ITE terkait bukti digital, serta POJK No. 12/POJK.03/2021 mengenai sandbox untuk blockchain pada KYC atau transaksi semata.

Teknologi blockchain dalam pengaturan sektor perbankan di dalam pencegahan tindak pidana penipuan online berupa deepfake, berfungsi preventif melalui smart contracts otomatis verifikasi, metadata autentikasi video atau audio anti-deepfake, serta ledger transparan yang digunakan untuk deteksi terhadap manipulasi real-time[41]. Akan tetapi, penerapan ini menghadapi berbagai tantangan di antaranya ialah regulasi vacuum atau kekosongan regulasi, resistensi SDM, serta privasi ledger publik. Sehingga diperlukannya regulasi khusus dari OJK/BI yang mengatur mengenai penggunaan teknologi blockchain dalam sektor perbankan agar dapat di implementasikan secara baik oleh lembaga perbankan di Indonesia, pelatihan literasi digital, serta sinergi AI-Blockchain. Selain itu juga, diperluakannya pengaturan dalam sektor perbankan terkait kewajiban standar blockchain di dalam verifikasi data nasabah, insentif adopter dini, serta edukasi pada nasabah terkait dengan budaya keamanan digital.

[41] Europol, *Facing Reality? Law Enforcement and the Challenge of Deepfakes*, Europol Innovation Lab, 2022.

C. Penipuan online berupa deepfake

Tindak pidana penipuan tidak hanya diatur dalam KUHP saja, akibat kemajuan perkembangan masyarakat yang sudah semakin canggih serta banyaknya modus operandi yang digunakan bermacam-macam, terdapat aturan khusus yang mengatur serta merumuskan mengenai tindak pidana penipuan[42] dalam Undang-Undang Nomor 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik yang sering disebut UU ITE. Kemudian Undang-Undang ITE ini direvisi ulang pada tahun 2016 sehingga menjadi Undang-Undang Nomor 19 Tahun 2016 mengenai ITE. Undang-Undang ini membahas terkait tindak penipuan yang dilakukan dengan cara atau menggunakan modus melalui jaringan daring atau "online"[43]. Undang-undang ini mengatur mulai dari informasi, transaksi elektronik sampai dengan hal-hal yang dilarang yang secara hukum berlawanan dengan peraturan yang dilakukan pada dunia maya[44]. Dalam UU ITE tindak pidana penipuan online tidak dijelaskan secara spesifik, begitu juga dengan tindak pidana penipuan online yang bermodus deepfake[45]. Selain UU ITE tersebut tindak pidana penipuan juga diatur di dalam KUHP yaitu Pasal 378, unsur serta penjelasan dalam Pasal 378 KUHP ialah dimana adanya kerugian yang merupakan tujuan maupun target utama dari pelaku tindak pidana dengan

[42] Barda Nawawi Arief, *Perkembangan Sistem Pemidanaan di Indonesia*, Kencana, Jakarta, 2019, hlm. 112.

[43] Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016.

[44] Josua Sitompul, *Cybercrime, Cyberlaw, dan Cybersecurity*, Tatanusa, Jakarta, 2012, hlm. 54.

[45] Edmon Makarim, *Pengantar Hukum Telematika*, RajaGrafindo Persada, Jakarta, 2014, hlm. 167.

mengakibatkan kerugian terhadap korban atau konsumen[46]. Dari rumusan di atas dalam kasus yang terjadi di Jawa Timur tersebut dilakukan secara sengaja berdasarkan niat dari pelaku untuk memperdaya orang lain dengan menggunakan cara menyebarkan sebuah video deepfake yang menyesatkan para korban[47].

Penipuan berbasis deepfake ini merupakan bentuk dari penipuan online yang paling mutakhir, menggunakan bantuan teknologi *artificial intelligence* (AI) yang digunakan untuk memanipulasi video, gambar, maupun audio seseorang sehingga tampak asli atau realistis[48]. Teknologi deepfake menggunakan algoritma *machine learning* serta *generative adversarial networks* (GANs) untuk menciptakan wajah, suara, maupun ekspresi yang menyerupai individu nyata. Dalam kejahatan siber, *deepfake* digunakan untuk tujuan memalsukan pernyataan tokoh publik, meniru identitas pejabat, maupun menyebarkan konten bohong dengan maksud menipu masyarakat luas[49].

Kasus yang sempat ramai dan terjadi di Jawa Timur pada awal tahun 2025 menjadi salah satu bukti nyata eskalasi bentuk penipuan online berbasis deepfake. Para pelaku berhasil memanipulasi video Gubernur Khofifah Indar Parawansa, dan beberapa pejabat lain seperti contohnya

---

[46] R. Soesilo, *Kitab Undang-Undang Hukum Pidana serta Komentar-Komentarnya*, Politeia, Bogor, 1996, hlm. 262.

[47] Moeljatno, *Asas-Asas Hukum Pidana*, Rineka Cipta, Jakarta, 2018, hlm. 75.

[48] Hendrawan, "Tantangan Hukum terhadap Deepfake dan AI dalam Perspektif Pembuktian," *Jurnal Hukum Teknologi,* Vol. 5 No. 2 (2024), hlm. 66.

[49] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana*, Kencana, Jakarta, 2020, hlm. 143.

Ahmad Luthfi (Jawa Tengah) serta Dedi Mulyadi (Jawa Barat), untuk menawarkan bantuan fiktif melalui platform TikTok[50]. Video hasil dari deepfake ini digunakan untuk mengelabuhi masyarakat serta meraup keuntungan hingga mencapai Rp 87,6 juta (delapan puluh tujuh enam ratus juat rupiah). Dari kasus ini menunjukkan bahwa penipuan berbasis deepfake bukan hanya kejahatan terhadap individu, melainkan ancaman terhadap integritas infromasi publik serta kepercayaan masayarakat terhadap institusi pemerintahan maupun keuangan.

Teknologi deepfake tersebut menimbulkan tantangan yang serius dalam pembuktian hukum karena sulitnya dibedakan antara mana konten asli dengan mana hasil rekayasa. Oleh sebab itu, dibutuhkannya inovasi hukum dan teknologi, salah satunya dengan penggunaan teknologi blockchain untuk menyimpan metadata asli serta memastikan keaslian konten digital. Dengan sistem dalam blockchain yang bersifat transaparan serta tidak dapat diubah (immutable), maka setiap perubahan dalam file video akan dapat dilacak, sehingga hal ini mencegah pemalsuan serta memperkuat aspek pembuktian hukum digital di Indonesia[51].

Penyelesaian kasus penipuan online berupa deepfake di Indonesia, masih menggunakan beberapa Pasal di dalam UU ITE seperti Pasal 27 ayat (1) jo. Psal 45 ayat (1) yang mengatur mengenai distribusi dan/atau

[50] Kompas.com, "Kasus Penipuan Deepfake Gubernur Khofifah Rugikan Masyarakat hingga Puluhan Juta," 15 Januari 2025.

[51] Nuryanto, "Blockchain sebagai Solusi Otentikasi Digital terhadap Kejahatan Deepfake," *Jurnal Cyber Law Review, Vol. 8 No. 1 (2024), hlm. 33.*

transmisi konten elektronik yang dianggap melanggar kesusilaan. Pasal 27 ayat (3) jo. Pasal 45 ayat (3) yang mengatur terkait konten elektronik yang mencemarkan nama baik dan/atau reputasi seseorang. Pasal 28 ayat (1) yang mengatur mengenai informasi elektronik yang berisikan kebohongan serta menyesatkan masyarakat. Pasal 35 jo. Pasal 51 ayat (1) yang mengatur terkait manipulasi dan/atau penciptaan infromasi elektronik agar dapat terlihat otentik. Kemudian dapat juga menggunakan Pasal 378 KUHP mengenai penipuan atau Pasal 492 UU No.1/2023 KUHP baru terkait penipuan.

D. Pengadopsian Teknologi dalam Hukum Islam

Pengadopsian teknologi di dalam hukum islam pada dasarnya diperbolehkan atau mubah karena hukum asal semua muamalah duniawi ialah boleh kecuali terdapat dalil yang mengharamkannya, sebagaimana prinsip fiqh, bahwa teknologi seperti contohnya kecerdasan buatan atau AI, Blockchain, Internet, serta Fintech menjadi anugerah yang diberikan oleh Allah untuk dimanfaatkan dengan bijak guna kemaslahatan umat. Sehingga teknologi dalam hukum islam boleh digunakan jika memiliki manfaat yang lebih besar daripada mudaratnya, seperti meningkatkan transparansi transaksi halal, efisiensi hifz-al mal, atau mencegah riba serta gharar, namun dilarang jika teknologi tersebut menimbulkan penipuan, perjudian, atau taghyir khalqillah seperti contohnya cloning manusia yang semata-mata hanya untuk kesenangan.

Menurut perspektif islam, teknologi blockchain dapat diartikan sebagai sebuah instrument atau sarana yang digunakan untuk mencatat transaksi (kitabah al-mu'amalat) yang berbasis digital serta terdesentralisasi[52]. Prinsip dalam islam sendiri tidak menolak adanya inovasi teknologi selama hal tersebut tidak bertentangan dengan ketentuan dalam syariah[53]. Al-Qur'an (QS. Al-Baqarah: 282) mengajurkan untuk pencatatan transaksi dilakukan agar menghindari perselisihan. Teknologi blockchain yang menyimpan catatan transaksi secara permanen serta transparansi sejalan dengan prinsip islam tersebut, sehingga hal ini secara konseptual dapat diterima sebagai alat bantu muamalah.

Terdapat beberapa karakteristik dari blockchain yang dapat dipandang selaras dengan prinsip syariah, yaitu:

a. Transparansi (Syafafiyyah)

   Dalam islam dianjurkan keterbukaan dalam akad agar tidak terjadi yang namanya gharar (ketidakjelasan)[54]. Teknologi blockchain menyediakan catatan transaksi yang transparan serta dapat diverifikasi.

b. Keamanan dan Kejujuran (Amanah)

[52] Ahmad Hasan, *Fiqh Muamalah Kontemporer*, (Jakarta: RajaGrafindo Persada, 2021), hlm. 56.

[53] Yusuf al-Qaradawi, *Fiqh al-'Aulawiyyat: Dirasah Jadidah fi Daw' al-Qur'an wa al-Sunnah*, (Kairo: Maktabah Wahbah, 1995), hlm. 77.

[54] Nuruddin dan Akmal Tarigan, *Hukum Ekonomi Syariah di Indonesia*, (Jakarta: Kencana, 2019), hlm. 120.

Kriptografi dalam blockchain serta sistem konsensus yang menjaga keaslian transaksi, selaras dengan prinsip Amanah dalam islam[55].

c. Pencatatan Permanen

Pencatatan transaksi yang permanen sesuai dengan anjuran pencatatan dalam muamalah[56].

Meskipun teknologi blockchain digunakan sebagai sistem pencatatan yang pada dasarnya netral, penggunaannya bisa mengandung unsur-unsur yang dilarang, apabila:

a. Teknologi blockchain digunakan untuk memfasilitasi transaksi yang mengandung riba, maisir (judi), atau gharar (ketidakpastian berlebihan).
b. Menggunakan asset digital yang belum jelas status hukumnya (misalnya cryptocurrency spekulatif).

Selain itu, terdapat tantangan lain yang perlu di perhatikan ialah masalah mengenai regulasi yang belum matang, kesiapan infrastruktur teknologi, serta kurangnya pemhaman dan edukasi mengenai penerapan blockchain di dalam konteks keuangan syariah. Lembaga berwenang seperti contohnya Otoritas Jasa Keuangan (OJK), Majelis Ulama Indonesia (MUI), serta lembaga yang terkait lainnya harus secara sinergis mengatur serta mengawasi teknologi blockchain ini untuk

[55] Ibid., hlm. 123.
[56] Al-Qur'an, Surah Al- Baqarah (2): Ayat 282.

memastikan bahwa setiap adopsi blockchain di sektor perbankan syariah tidak melanggar prinsip-prinsip syariah serta memberikan kepastian hukum dan keamanan transaksi. Pengaturan yang tepat juga harus mengakomodasi pelatihan sumber daya manusia serta edukasi untuk nasabah agar teknologi ini dapat diimplementasikan secara optimal serta sesuai syariah. Oleh sebab itu, pemanfaatan dari blockchain dalam sistem perbankan syariah harus melalui mekanisme shariah compliance yang ketat, misalnya smart contract yang mengimplementasikan akad syariah secara benar. Dengan demikian, maka blockchain dapat menjadi sebuah alat yang mendukung transparansi serta keamanan perbankan syariah, asalkan pemnfaatannya tidak bertentang dengan riba, maisir, gharar, serta penggunaan asset digital yang tidak sesuai dengan syariah.

BAB III

PEMBAHASAN

A. Sektor Perbankan Atas Penggunaan Teknologi Blockchain Yang Berfungsi Untuk Mencegah Penipuan Online Berupa Deepfake

Peraturan perbankan di Indonesia merupakan landasan hukum yang mengatur mengenai aktivitas serta tata kelola bank untuk menjaga stabilitas sistem keuangan nasional dan melindungi kepentingan nasabah serta masyarakat luas. Terdapat beberapa peraturan mengenai perbankan diantara ialah Undang-Undang Nomor 10 Tahun 1998 mengenai Perbankan yang memuat kerangka umum terkait tata kelola bank, kemudian Undang-Undang Nomor 21 Tahun 2011 mengenai pemberian kewenangan pengawasan kepada Otoritas Jasa Keuangan atau OJK sebagai regulator terkait industri jasa keuangan. Selain itu, terdapat juga Undang-Undang Nomor 19 Tahun 2016 mengenai Informasi dan Transaksi Elektronik atau UU ITE yang menjadi payung hukum utama di dalam mengatur transaksi elektronik serta perlindungan data digital.

Meskipun telah ada kerangka regulasi terkait perbankan ini yang dirasa sudah cukup kuat di dalam mengatur perbankan serta aktivitas digital, namun belum ada ketentuan yang secara khusus mengatur mengenai pemanfaatan teknologi blockchain sebagai salah satu alat untuk mencegah dan menangkal penipuan online yang berbasis deepfake[57]. Sehingga,

[57] Sylvia Janisriwati, "Legal Analysis on the Use of Deepfake Technology: Threats to Indonesian Banking Institutions", *e-ISSN* Vol. 8 No. 2 (2023): Law and Justice. hlm. 2549-8282.

pengaturan pada sektor perbankan terkait dengan penggunaan teknologi blockchain untuk mencegah penipuan online berupa deepfake saat ini masih dalam tahap pengembangan, terutama di Indonesia. Teknologi deepfake sendiri yang menggunakan kecerdasan buatan atau AI untuk memanipulasi suara serta wajah di dalam video maupun audio dengan tingkat keaslian yang sangat tinggi menjadi sebuah ancaman baru yang cukup serius terhadap keamanan transaksi serta identitas digital dari para nasabah[58]. Selain itu dalam praktiknya, penggunaan teknologi blockchain dalam perbankan masih bersifat eksperimen inovatif atau sandboxing yang difasilitasi oleh OJK melalui regulatory sandbox untuk financial technology atau fintech. Maka dari itu inovasi seperti teknologi blockchain telah diakui potensinya, akan tetapi belum mendapatkan legitimasi hukum yang memadai untuk diimplementasikan secara luas.

Teknologi Blockchain sendiri memiliki karakteristik yang unggul seperti desentralisasi, transparansi, immutabilitas atau data yang tidak dapat dirubah, keamanan kriptografi, serta kemampuan auditabilitas yang dapat memperkuat sistem keamanan perbankan[59]. Desentralisasi dalam teknologi blockchain dapat menghilangkan otoritas pusat dari kerentanan terhadap manipulasi, sementara immutability dapat berfungsi untuk memastikan metadata dari video atau audio deepfake tidak bisa dirubah, hal ini selaras dengan distributed legder yang digunakan untuk verifikasi real-time.

[58] Digital Insight, B2B Insight, Cybersecurity Trend 2025 with AI: How Can Banks Survive the Threat of Deepfake, https://www.binar.co.id/blog/cybersecurity-trend-2025-dengan-ai-bagaimana-perbankan-bisa-bertahan-dari-ancaman-deepfake diakses pada 20 September 2025

[59] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, (2008).

Sehingga hal ini, dapat melengkapi UU No. 10/1998 jo. POJK No. 12/POJK.03/2021 mengenai keamanan IT Perbankan, dimana smart contracts otomatisasi transaksi dapat mencegah phishing deepfake seperti kasus yang melibatkan Gubernur Jawa Timur yang sempat ramai pada awal tahun ini dengan kerugian yang mencapai Rp. 87,6 juta (Delapan puluh tujuh enam ratus rupiah). Setiap karakteristik utama dari teknologi blockchain ini memiliki resepresentasi nilai-nilai fundamental di dalam sistem hukum perbankan yang berorientasi pada prinsip kehati-hatian atau prudential banking principle. Keterkaitan antara karakteristik utama Blockchain dengan asas-asas hukum perbankan dapat dijelaskan sebagai berikut:

1. Desentralisasi

   Desentralisasi di dalam teknologi blockchain berarti bahwa sistem tidak lagi bergantung kepada satu otoritas pusat atau single point of control, melainkan dibangun di atas jaringan yang terdesentral atau distributed ledger. Dimana setiap node di dalam jaringan memiliki Salinan data transaksi yang identic serta diperbarui secara simultan melalui mekanisme konsensus.

   Dalam konteks hukum perbankan, karakteristik dari blockchain ini memiliki keselarasan dengan asas kehati-hatian atau prudential principle yang mengharuskan bank untuk mengelola risiko operasional secara hati-hati serta sistematis. Dengan adanya sistem yang terdesentralisasi, potensi akan kegagalan sistem akibat serangan siber.

Korupsi data, atau kesalahan administrative dapat diminimalisirkan. Selain itu juga, desentralisasi dalam blockchain mendukung prinsip kemandirian serta integritas operasional bank sebagimana yang telah diatur dalam *Peraturan OJK Nomor* 38/POJK.03/2016 mengenai *Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum*, dikarenakan setiap transaksi dapat diverifikasi oleh jaringan tanpa harus bergantung kepada satu entitas pengendali. Dengan demikian, maka desentralisasi dalam blockchain menciptakan sebuah struktur tata kelola yang lebih Tangguh serta selaras dengan tujuan hukum perbankan untuk menjaga stabilitas sistem keuangan.

2. Transparansi

Selain desentralisasi, blockchain juga memiliki karakteristik utama yaitu transparansi, yang berarti keterbukaan data yang dapat diakses oleh semua pemgguna dalam jaringan atau seluruh pihak yang memiliki otoritas dalam jaringan. Transparansi ini tidak berarti meniadakan sebuah kerahasiaan, melainkan menyeimbangkan antara *accountability* serta *privacy* melalui mekanisme izin akses atau permissioned blockchain. Dalam perspektif hukum perbankan, karakteristik transparansi ini sejalan dengan asas akuntabilitas (accountability) serta asas keterbukaan informasi (disclosure principle) yang menjadi dasar di dalam pengawasan internal maupun eksternal dari lembaga keuangan. Dimana Bank diwajibkan untuk menyelenggarakan kegiatan usaha secara terbuka serta dapat diaudit

oleh regulator, tanpa mengorbankan kerahasian dari nasabah sebagaimana telah diatur dalam Pasal 40 UU No. 10 Tahun 1998 mengenai Perbankan. Dengan teknologi blockchain, setiap transaksi akan tercatat secara kronologis serta tidak dapat dihapus, sehingga audit trail menjadi lebih ditelusuri oleh OJK atau auditor independent. Dengan demikian, maka transparansi dalam teknologi blockchain mendukung prinsip akuntabilitas hukum di dalam perbankan sekaligus dapat memperkuat kepercayaan publik terhadap sistem keuangan nasional.

3. Immutability

Prinsip *immutability* ialah bahwa setiap data maupun transaksi yang telah tercatat di dalam blockchain tidak dapat diubah maupun dihapus tanpa adanya persetujuan dari mayoritas jaringan atau konsensus. Karakteristik ini akan menjamin keaslian serta kontinuitas dari waktu ke waktu. Dalam konteks perbankan, prinsip immutability ini memperkuat asas integritas data (data integrity), yaitu kewajiban bank unyuk menjaga keakuratan, keaslian, serta keutuhan informasi dari transaksi keuangan. Hal ini berkaitan erat dengan prinsip keandalan administratif perbankan (administrative realibility) yang merupakan bagian dari prinsip kehati-hatian.

Dengan sifatnya yang permanen serta terverifikasi, maka blockchain dapat berfungsi sebagai sistem pencatatan hukum yang otentik (legal record system). Setiap transaksi yang tercatat di dalam

blockchain memiliki nilai pembuktian hukum (evidentiary value) sebagaimana hal ini telah diatur dalam Pasal 5 ayat (1) UU ITE, yang menyatakan bahwa informasi elektronik dapat dijadikan sebagai alat bukti hukum yang sah. Dengan demikian, prinsip *immutability* tidak hanya berfungsi sebagai mekanisme teknis, namun juga memberikan kepastian hukum (legal certainty) bagi lembaga perbankan di dalam menghadapi potensi adanya sengketa digital.

4. Keamanan Kriptografi

Blockchain menggunakan sistem kriptografi asimetris untuk melindungi data transaksi, dimana setiap transaksi dienkripsi dengan sebuah *private key* serta diverifikasi dengan *public key*. Keamanan kriptografi ini menjamin akan kerahasiaan (confidentiality), keaslian (authenticity), dan non-repudiation (tidak dapat disangkal) dari setiap transaksi digital yang terjadi dalam jaringan.

Dalam hukum perbankan, prinsip keamanan kriptoghrafi ini mencerminkan asas kepercayaan (trust principle) yang menjadi dasar hubungan antara bank dengan nasabah. Keamanan data serta keaslian transaksi merupakan faktor esensial yang melindungi nasabah dari penyalahgunaan identitas, manipulasi data, maupun tindak pidana siber. Dengan menggunakan algoritma kriptografi yang kompleks, teknologi blockchain menjadin bahwa setiap perubahan data dapat dideteksi serta diverifikasi secara real-time, sehingga hal ini, dapat mencegah tindak pidana penipuan online, termasuk yang bermoduskan deepfake. Oleh

sebab itu, penerapan dari kriptografi dalam blockchain ini buakn sekadar fitur teknologis semata, melainkan bentuk aktualisasi dari prinsip perlindungan hukum terhadap nasabah sebagaimana yang telah diatur di dalam Pasal 29 ayat (2) UU Perbankan, yang mewajibkan bank untuk menjaga rahasia serta keamanan dari data nasabah.

Dengan demikian, maka blockchain dapat menjadi sebuah instrument hukum preventif di dalam sistem keuangan digital, sesuai dengan pandangan dari Barda Nawawi Arief mengenai bahwa hukum pidana idealnya tidak hanya bersifat represif, namun juga harus memiliki fungsi pencegahan atau preventif. Dalam sektor perbankan, blockchain dapat diadopsi untuk mencatat transaksi dan metadata autentik secara permanen serta dapat diverifikasi, sehingga dapat digunakan untuk memverifikasi keaslian identitas serta aktivitas transaksi digital, termasuk digunakan untuk mengidektifikasi serta meminimalkan risiko adanya penipuan online berupa deepfake.

Kasus penipuan deepfake yang terjadi di Jawa Timur, dimana dalam video palsu yang mengatas namakan Gubernur Khofifah tersebut digunakan untuk menipu masyarakat dengan menawarkan bantuan fiktif, hal tersebut menunjukkan betapa serius serta nyata ancaman dari modus penipuan ini. Dalam konteks tersebut, teknologi blockchain dapat berperan sebagai sistem digital notarization yang merekam metadata asli dari video atau audio sehingga apabila terdapat modifikasi, keberadaan serta perubahan tersebut dapat terdeteksi dengan mudah. Regulasi perbankan perlu

mendorong adanya adopsi teknologi blockchain ini agar bank dapat menerapkan mekanisme verifikasi yang kuat serta transparan untuk mencegah penyalahgunaan identitas nasabah akibat deepfake.

Selain itu kasus penipuan deepfake yang terjadi dengan mengatasnamakan Gubernur Khofifah di Jawa Timur menjadi salah satu contoh nyata bagaimana teknologi manipulasi digital itu dapat mengancam keamanan publik serta kredibilitas dari suatu lembaga. Di dalam skala perbankan, ancaman seperti ini dapat dimanfaatkan untuk mengelabui sistem verifikasi konvensional, sehingga hal ini mengakibatkan kerugian finansial serta pelanggaran data pribadi dari nasabah. Dengan memanfaatkan teknologi blockchain, bank bisa melakukan pencatatan serta verifikasi metadata yang asli dari setiap rekaman audio maupun video yang digunakan di dalam proses autentikasi, sehingga perubahan sekecil apapun akan dapat segera diketahui atau terdeteksi.

Sebagai langkah yang strategis, terhadap regulasi pada sektor perbankan perlu dimuat mengenai ketentuan yang mendorong pengadopsian teknologi blockchain di dalam mekanisme keamanan serta verifikasi transaksi digital, terutama mengenai identitas digital dari nasabah. Hal ini dapat dilakukan dengan beberapa langkah yaitu:

1. Menetapkan standar operasional terkait teknologi blockchain di dalam sistem perbankan, di dalamnya termasuk tata cara pencatatan, validasi, serta audit data digital untuk memastikan keakuratan serta keamanan informasi.

2. Kewajiban terhadap transaparansi serta pelaporan kepada OJK, hal ini terkait dengan mekanisme deteksi serta penanganan penipuan online, sehingga regulator yang ada dapat memantau efektivitas teknologi yang diadopsi secara berkelanjutan.
3. Pengembangan mengenai kerangka hukum khusus yang mengakui bukti autentikasi berbasis blockchain, dalam sebuah proses penyelidikan terhadap kasus penipuan, baik itu dalam ranah perdata maupun pidana, sehingga hal ini dapat mendorong kepercayaan hukum terhadap teknologi blockchain ini.
4. Penguatan kolaborasi lintas sektor antara bank, penyedia teknologi, pemangku kebijakan, serta penegak hukum untuk dapat membangun sebuah sistem deteksi dini serta respons cepat terhadap tindak pidana penipuan yang berbasis deepfake.
5. Inisiatif edukasi serta kampanye kesadaran untuk nasabah serta seluruh pelaku industri jasa keuangan terkait risiko penipuan online yang berbasis deepfake dan pentingnya teknologi blockchain sebagai salah satu alat proteksi.

Maka dari itu untuk dapat memperkuat sistem keamanan dari perbankan terhadap ancaman penipuan online yang berbasiskan deepfake, perlunya pembaharuan regulasi pada sektor perbankan yang diselaraskan dengan perkembangan teknologi blockchain. Regulasi tersebut harus memuat mengenai aturan penggunaan teknologi blockchain secara jelas serta komprehensif, kemudian mencakup aspek standar operasional,

validasi hukum, kolaborasi antar pemangku kepentingan, serta adanya edukasi publik. Dengan langkah ini, maka sektor perbankan dapat meningkatkan keandalan serta transparansi sistem verifikasi mereka, sekaligus memberikan perlindungan yang optimal kepada para nasabah dari risiko digital modern yang semakin hari semakin kompleks.

B. **Pengadopsian Teknologi Blockchain Ke Dalam Pengaturan Sektor Perbankan Untuk Mencegah Penipuan Online Berupa Deepfake.**

Pengadopsian teknologi blockchain di dalam sektor perbankan mencerminkan teori hukum pidana preventif, yang dimana teori ini mengedepankan pencegahan overkriminalisasi. Pendekatan preventif dari teknologi blockchain yaitu berupa verifikasi identitas melalui ledger transparan untuk mencegah penipuan berupa deepfake sebelum transaksi (Pasal 378 KUHP & UU ITE), sementara represif disediakan melalui audit trail immutable sebagai bukti untuk digital forensik. Reformasi regulasi yang ada yaitu BI/OJK melalui regulatory sandbox (POJK No. 13/POJK.02/2018) diperlukan untuk integrasi ini, agar dapat mengurangi 405 ribu laporan mengenai penipuan online. Selain itu pengadopsian teknologi blockchain ke dalam pengaturan sektor perbankan juga merupakan sebuah langkah yang strategis dalam memperkuat sistem keamanan digital serta menjaga integritas transaksi finansial, terkhusus di dalam menghadapi fenomena penipuan online yang bermoduskan deepfake. Teknologi deepfake, ialah teknologi yang memanfaatkan kecerdasan buatan atau AI untuk memanipulasi sebuah data visual serta suara, yang telah

menimbulkan ancaman serius terhadap kepercayaan publik terhadap sistem perbankan yang ada. Oleh sebab itu, dibutuhkannya sistem yang tidak hanya mampu mendeteksi manipulasi tersebut, namun juga mampu mencegahnya dari tahap awal transaksi. Dalam konteks ini, teknologi blockchain mempunyai peran penting karenan blockchain memiliki karakteristik *immutability* (terdesentralisasi) yang dapat memperkuat keandalan dari sistem keuangan digital.[60]

Otoritas jasa keuangan akhir-akhir ini terus mencermati perkembangan dari teknologi blockchain di dalam sektor perbankan. Hal ini, sejalan dengan adanya transformasi digital yang berlangsung pada industri global, Otoritas Jasa Keuangan sendiri sedang menyiapkan berbagai regulasi yang dapat mendukung adopsi teknologi blockchain di Indonesia. Kepala Eksekutif Pengawas Perbankan Otoritas Jasa Keuangan yaitu Dian Ediana Rae dalam konferensi pers Hasil RDKB OJK pada tanggal 04 Maret 2025 mengungkapkan "bahwa teknologi blockchain telah menjadi bagian dari inovasi yang telah diterapkan oleh perbankan di berbagai negara. Implementasi berbagai emerging technology ini bertujuan untuk mendukung kegiatan usaha bank agar dapat tetap kompetitif di era digital[61]." Otoritas Jasa Keuangan dalam rangka akselerasi transformasi digital telah menerbitkan berbagai roadmap, panduan, serta regulasi, seperti Roadmap Transformasi Digital Perbankan, Buku Pnaduan Resiliensi Digital

[60] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (White Paper, 2008).

[61] Pipit Ika Ramadhani, "OJK Siapkan Regulasi untuk Adopsi Blockchain dalam Perbankan", diakses melalui https://www.liputan6.com/bisnis/read/5944941/ojk-siapkan-regulasi-untuk-adopsi-blockchain-dalam-perbankan pada tanggal 16 Januari 2026.

Perbankan, dan Surat Edaran OJK mengenai ketahanan serta keamanan siber bagi bank umum. Otoritas Jasa Keuangan juga akan menerbitkan regulasi terkait dengan teknologi kecerdasan buatan atau AI yang saat ini masih dalam tahap perumusan. Kepala Eksekutif Pengawas Perbankan Otoritas Jasa Keuangan yaitu Dian, menekankan bahwa manfaat dari teknologi blockchain ini sangat signifikan, terutama di dalam mendorong perkembangan decentralized finance (DeFi), dimana hal ini dapat memungkinkan masyarakat untuk mengakses layanan keuangan tanpa melalui perantara bank maupun lembaga keuangan tradisional. DeFi diharapkan dapat meningkatkan efisiensi, fleksibelitas, transparansi, serta aksesibilitas terhadap produk keuangan. Tetapi, kita juga patut mewaspadai adanya risiko yang muncul, seperti contohnya pencucian uang, pendanaan terorisme, manipulasi pasar, dan perlindungan konsumen. Menurut Kepala Eksekutif Pengawasan Perbankan Otoritas Jasa Keuangan, saat ini OJK terus melakukan pemantauan terhadap regulasi di berbagai negara, termasuk salah satunya Uni Eropa yang telah maju lebih dalam terkait pengaturan AI serta Teknologi Blockchain. Akan tetapi, regulasi di Indonesia akan tetap disesuaikan dengan kebutuhan domestik. Dalam hal ini, OJK akan terus mengkaji terkait dampak serta risiko dari blockchain dalam perbankan dan berfokus pada peningkatan literasi masyarakat. Dengan demikian, ketika saatnya telah tiba, para pengguna perbankan di Indonesia siap memanfaatkan kemajuan dari teknologi blockchain ini.

Otoritas Jasa Keuangan secara resmi menunjuk Asosiasi Blockchain Indonesia atau ABI sebagai asosiasi yang menyelenggarakan Inovasi Teknologi Sektor Keuangan (ITSK). Keputusan OJK tersebut tertuang dalam Surat Nomor S-335/IK.01/2025 yang dikeluarkan pada tanggal 25 Juni 2025, serta berlaku efektif sejak tanggal dikeluarkannya[62]. Penunjukan ini menegaskan bahwa peran ABI sebagai mitra strategis dari OJK dalam memperkuat pengawasan, pembinaan, dan pengembangan inovasi teknologi keuangan di Indonesia, terkhusus pada bidang blockchain. Oleh karena itu, dari penunjukan ini, kini teknologi blockchain secara resmi telah masuk ke dalam kategori ITSK yang berada di bawah pengawasan langsung OJK. Selain itu, ABI mendapatkan mandat atau perintah besar untuk tidak hanya mendorong inovasi dalam sektor ini, namun juga memastikan kepatuhan industry terhadap regulasi, menyusun standar praktik, dan memberikan perlindungan untuk konsumen. Ketua Umum ABI, yaitu Robby dalam keterangan tertulis kepada Tempo.co pada tanggal 8 Juli 2025 menekankan bahwa penunjukan ABI ini tidak hanya sebatas pada pengakuan formal, namun juga memberikan tanggung jawab nyata di dalam membina industry, menjembatani komunikasi antara pelaku usaha dengan regulator, dan memastikan penerapan praktik terbaik di sektor inovasi teknologi keuangan. ABI dalam hal ini juga menegaskan pentingnya literasi publik sebagai salah satu prioritas kerja dari Asosiasi ke depan. Wakil Ketua Umum Bidang

[62] Tempo, "OJK Tunjuk Asosiasi Blockchain Indonesia sebagai Penyelenggara Sektor Keuangan Digital", diakses melalui https://www.tempo.co/ekonomi/ojk-tunjuk-asosiasi-blockchain-indonesia-sebagai-penyelenggara-sektor-keuangan-digital-1935265 pada tanggal 16 Januari 2026.

Literasi dan Edukasi ABI yaitu Steven, menegaskan bahwa program literasi akan diperluas agar masyarakat dapat memahami manfaat, risiko, dan praktik terbaik terkait dengan inovasi teknologi keuangan berbasis blockchain. Selain itu, Wakil Ketua Umum Bidang Blockchain, Tigran Adiwirya, melihat bahwa penunjukan ini sebagai momentum untuk memperkuat integrasi teknologi blockchain di dalam sistem keuangan yang lebih aman serta efisien. Keputusan yang dilakukan oleh Otoritas Jasa Keuangan ini sejalan dengan pertumbuhan pesat adopsi blockchain di Indonesia.

Pengadopsian teknologi blockchain dalam sektor perbankan dalam upaya untuk mencegah penipuan online berbasis deepfake memerlukan integrasi teknologi dengan regulasi yang mendukung, serta edukasi literasi digital pada nasabah dan pelaku industri. Integrasi antara blockchain dengan sistem perbankan tidak hanya dapat berjalan tanpa adanya dukungan regulasi, kebijakan pengawasan, serta literasi digital dari para pemangku kepentingan. Pengadopsian teknologi blockchain harus disertai juga dengan kerangka hukum yang jelas agar penerapannya tidak menimbulkan ketidakpastian hukum serta tetap berada di dalam perlindungan konsumen dan pencegahan tindak pidana.[63] Oleh kerena itu, terdapat beberapa aspek penting di dalam pengaturan serta implementasi teknologi blockchain di dalam sektor perbankan antara lain, yaitu:

[63] Lawrence Lessig*, Code and Other Law of Cyberspace* (Basic Books, 1999), hlm. 25.

1. Penguatan regulasi oleh Otoritas Jasa Keuangan (OJK) serta Bank Indonesia (BI)

   Langkah awal yang perlu dilakukan dalam pengadopsian teknologi *blockchain* dalam sektor perbankan ini ialah memperkuat regulasi yang mewajibkan lembaga perbakan untuk mengadopsi teknologi keamanan digital berbasiskan *blockchain* ke dalam mekanisme autentikasi serta verifikasi transaksi. Kemudian, regulasi ini perlu dituangkan ke dalam peraturan OJK maupun kebijakan Bank Indonesia sebagai otoritas moneter nasional. Ketentuan ini tidak hanya bertujuan untuk meningkatkan standar keamanan digital perbankan nasional, namun juga bertujuan untuk menjadi dasar hukum bagi lembaga keuangan untuk melakukan inovasi teknologi secara terukur.[64]

   Selain itu, perlu juga dilakukan sinkronisasi dengan ketentuan yang terdapat di dalam Undang-Undang Nomor 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik atau UU ITE beserta perubahannya, dan Peraturan OJK Nomor 38/POJK.03/2016 mengenai Penerapan Manajemen Resiko dalam Penggunaan Teknologi Informasi oleh Bank Umum.[65] Dengan demikian, adanya sinergi regulative ini, pengawasan dapat dilakukan secara preventif melalui mekanisme *compliance technology* (regtech) yang memanfaatkan teknologi

[64] Otoritas Jasa Keuangan, *Roadmap Pengembangan dan Penguatan Perbankan Indonesia 2021-2025* (OJK, 2021), hlm. 63.

[65] Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016: Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum.

blockchain untuk pelaporan serta audit otomatis, sehingga hal ini mempersempit peluang terjadinya manipulasi data maupun identitas yang palsu.

2. Penerapan smart contracts di dalam proses transaksi

Smart contracts ialah sebuah kontrak digital yang dapat diseksekusi secara otomatis sesuai dengan ketentuan yang telah ditetapkan sebelumnya tanpa adanya campur tangan manusia. Dalam konteks perbankan, penerapan dari smart contracts dapat digunakan untuk melakukan otomatisasi proses persetujuan, verifikasi, serta eksekusi transaksi. Dengan digunakannya sistem otomatisasi yang bersifat transparan serta dapat diverifikasi, maka tindakan manipulative dari pelaku kejahatan siber dapat diminimalisasikan.[66]

Sebagai contohnya, ketika seorang nasabah melakukan transaksi finansial, maka *smart contracts* akan mengeksekusi ketentuan keamanan yang ada seperti verifikasi biometric, kecocokan data identitas, serta validasi sumber dana berdasarkan dari catatan yang tersimpan di dalam *ledger blockchain*. Proses ini berlangsung secara real-time serta tidak memungkinkan adanya perubahan data setelah transaksi terjadi. Sehingga hal ini, memberikan kepastian hukum serta keamanan yang lebih tinggi dibandingkan dengan sistem konvensional

[66] Primavera De Filippi & Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press, 2018), hlm. 91.

yang masih bergantung pada validasi manual serta rentan terhadap kesalahan manusia atau *human error*.[67]

3. Kolaborasi dengan penyedia teknologi AI-Blockchain

Kasus penipuan online yang bermoduskan deepfake memerlukan pendekatan yang multidispliner antara hukum, teknologi informasi, serta kebijakan publik. Oleh karena itu, sektor perbankan perlu menjalin kemitraan startegis dengan perusahaan teknologi yang mengembangkan sistem deteksi deepfake yang berbasis kecerdasan buatan atau AI yang diintegrasikan dengan teknologi *blockchain*.[68] Integrasi ini dapat memungkinkan deteksi otomatis terhadap sebuah aktivitas yang mencurigakan seperti upaya pemalsuan identitas, video, ataupun suara yang digunakan untuk melakukan transaksi keuangan secara illegal.

Dengan sistem yang berbasis AI-Blockchain, maka setiap data yang masuk ke dalam sistem dapat diverifikasi menggunakan model pembelajaran mesin *(machine learning)* yang dapat mengidentifikasi pola manipulasi digital. Hasil dari verifikasi tersebut kemudian akan dicatat secara permanen di dalam *ledger blockchain*, sehingga hal ini memberikan bukti autentik apabila terjadi sengketa hukum ataupun proses penyidikan pidana siber.[69]

---

[67] Jaya Putra, "Implementasi Smart Contracts dalam Sistem Keuangan Digital di Indonesia." *Jurnal Hukum dan Teknologi* Vol. 4 No. 2 (2022), hlm. 118.

[68] Shoshana Zuboff*, The Age of Surveillance Capitalism* (PublicAffairs, 2019), hlm. 71.

[69] Alket Cecaj et al., "Blockchain Meets Artificial Intelligence: Opportunities and Challenges," *IEEE Access* Vol. 9 (2021), hlm. 13005-13020.

4. Pengelolaan data secara terdesentralisasi

Penerapan teknologi blockchain di dalam pengelolaan data perbankan memungkinkan sistem penyimpanan yang terdesentralisasi untuk menghindari risiko *single point of failure* (titik kegagalan tunggal). Dalam sistem konvensional, apabila server utama diretas ataupun rusak, maka seluruh data dalam sistem tersebut berpotensi hilang atau dimanipulasi. Tetapi, dengan sistem *distributed ledger*, setiap transaksi dalam sistem akan disalin ke dalam ribuan node di jaringan yang berbeda, sehigga hal ini menjadikannya lebih sulit untuk diubah tanpa jejak.[70]

Selain untuk meningkatkan keamanan, sistem ini juga dapat memudahkan proses audit serta pelacakan kejahatan digital, karena setiap perubahan data dalam sistem dapat ditelusuri secara transparan. Hal ini, relevan dengan prinsip accountability (akuntabilitas) di dalam hukum keuangan serta dapat memperkuat sistem pembuktian di dalam perkara pidana siber sebagaimana yang telah diatur dalam Pasal 5 ayat (1) UU ITE, yang menyatakan bahwa informasi elektronik dapat digunakan sebagai alat bukti hukum yang sah.[71]

5. Sinergi teknologi, regulasi, serta edukasi literasi digital

Kasus penipuan online bermodus deepfake yang ditangani oleh Direktorat Reserse Siber Polda Jawa Timur menunjukkan bahwa

[70] Don Tapscott & Alex Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World* (Penguin, 2016), hlm. 78.

[71] Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 5 ayat (1).

teknologi canggih tanpa adanya dukungan regulasi adaptif serta penegakan hukum yang efektif tidak akan memberikan hasil yang optimal.[72] Oleh sebab itu, keberhasilan dari pengadopsian teknologi *blockchain* ke dalam sektor perbankan tidak hanya bergantung kepada teknologi semata, namun juga pada sinergi antara tiga elemen utama, yaitu teknologi, regulasi, serta edukasi.

Bank dalam hal ini perlu berperan aktif di dalam memberikan edukasi literasi digital kepada para nasabah agar memahami mekanisme keemanan transaksi digital, mengenali potensi penipuan, serta mengetahui prosedur hukum ketika menjadi korban dari kejahatan siber. Sementara itu, regulator harus terus menyesuaikan kebijakan dengan perkembangan teknologi yang ada serta memperkuat koordinasi antar instansi seperti contohnya OJK, BI, Kementerian Kominfo, serta Kepolisian di dalam rangka menciptakan ekosistem keuangan digital yang amana, transparan, serta adaptif terhadap risiko baru.[73]

Dengan demikian, maka pengadopsian teknologi blockchain dalam sektor perbankan bukan hanya sekadar transformasi digital semata, melainkan juga bentuk pembaharuan hukum (legal reform) di dalam menghadapi kejahatan siber yang berbasis deepfake. Upaya ini mencerminkan prinsip rule of law in digital transformation, yaitu bahwa setiap inovasi teknologi harus berada di bawah payung

[72] Direktorat Reserse Kriminal Khusus Polda Jawa Timur, *Laporan Penanganan Kasus Penipuan Online Bermodus Deepfake,* 2023.

[73] Bank Indonesia, *Blueprint Sistem Pembayaran Indonesia 2025* (Jakarta: BI, 2019), hlm. 54.

hukum yang jelas serta mampu melindungi kepentingan publik tanpa menghambat inovasi itu sendiri.[74]

Kasus penipuan online bermodus deepfake yang melibatkan Gubernur Jawa Timur yaitu Khofifah Indar Parawansa pada tahun 2025 merupakan salah satu bukti konkret bahwa sistem autentikasi digital konvensional Indonesia yang masih memiliki celah yang cukup signifikan terhadap manipulasi identitas berbasis teknologi kecerdasan buatan atau AI. Dalam kasus tersebut, para pelaku berhasil menciptakan sebuah video palsu dengan meniru wajah serta suara dari Gubernur Khofifah untuk melakukan tindak penipuan melalui media sosial. Dari aksi ini tidak hanya menimbulkan kerugian secara material untuk korban, namun juga menyebabkan rusaknya kepercayaan publik terhadap validatas informasi digital serta institusi pemerintahan. Berdasarkan perspektif siber, kasus penipuan deepfake ini mengindikasikan bahwa mekanisme autentikasi digital yang bersifat sentralistik, seperti adanya verifikasi akun, tanda tangan elektronik, maupun sistem login tunggal, tidak memadai di dalam menghadapi ancaman dari kejahataan siber terutama yang berbasis deepfake. Teknologi deepfake ini dirasa mampu untuk menembus lapisan verifikasi konvensional dikarenakan bersandar pada model pembelajaran mesin (machine learning) yang mampu memanipulasi data visual serta suara dengan tingkat keaslian yang tinggi. Sehingga, keaslian data (data authenticity) serta integritas sistem digital (system integrity) menjadi aspek yang paling terancam.

[74] Richard Susskind, *Tomorrow's Lawyers: An Introduction to Your Future* (Oxford University Press, 2020), hlm. 137.

Sistem autentikasi digital yang saat ini digunakan oleh lembaga keuangan ataupun instansi publik pada umumnya sistem ini masih mengandalkan mekanisme centralized verification, di mana seluruh data disimpan dalam satu server pusat. Sehingga model ini memiliki dua kelemahan utama yaitu pertama, vulnerabilitas terhadap manipulasi eksternal, karena tidak semua proses autentikasi dalam sistem ini tidak memiliki audit trail yang dapat dilacak apabila terdapat atau terjadi perubahan. Kedua, ketergantungan pada otoritas tunggal, yang berarti apabila server pusat disusupi, maka seluruh data dalam sistem berpotensi untuk dimanipulasi atau dicuri. Kondisi ini menegaskan perlunya ada sistem verifikasi yang lebih terdistribusi, transparan, serta tidak dapat dimodifikasi tanpa konsensus, yang di mana hal ini merupakan karakteristik fundamental dari teknologi blockchain.

Di dalam konteks pencegahan tindak pidana digital terkhusus pada tindak pidana penipuan online, blockchain memiliki fungsi yang preventif yuridis serta teknologis. Dengan sifat teknologi blockchain yang immutability atau tidak dapat diubah serta traceability (dapat ditelusuri), blockchain dapat memastikan bahwa setiap data digital memiliki jejak autentik nya masing-masing yang tidak dapat dimanipulasi tanpa meninggalkan rekam jejak forensik. Secara spesifik, di dalam konteks kasus penipuan deepfake yang melibatkan Gubernur Khofifah, teknologi blockchain dapat berfungsi sebagai:

1. Menyimpan metadata dari video autentik pejabat publik untuk deteksi perubahan

Metadata ini seperti waktu perekaman, lokasi, tanda tangan digital, serta hash unik yang dapat dicatat dalam ledger blockchain. Apabila terdapat pihak yang ingin mencoba memodifikasi video tersebut, sistem akan langsung mendeteksi perbedaan hash value serta menolak keaslian dari data tersebut. Dengan demikian, maka blockchain dapat menjadi alat digital watermaking yang efektif untuk melindungi keaslian dari sebuah konten visual publik.

2. Menyediakan traceable digital proof dalam penyidikan kepolisian

   Catatan transaksi serta data autentik yang tersimpan di dalam blockchain bersifat auditable serta tidak dapat dihapus, sehingga hal ini dapat dijadikan sebagai alat bukti digital yang sah sesuai dengan Pasal 5 ayat (1) UU ITE, yang menyatakan bahwa informasi elektronik dapat menjadi alat bukti hukum yang sah di pengadilan. Dalam kasus penipuan deepfake, teknologi blockchain memungkinkan penyidik untuk dapat menelusuri asal-usul data digital, waktu pembuatan, dan perubahannya. Dengan demikian, hal ini dapat memperkuat posisi pembuktian dalam ranah hukum pidana siber.

3. Meningkatkan akuntabilitas lembaga keuangan terhadap keamanan data nasabah

   Lembaga keuangan dapat memanfaatkan teknologi blockchain untuk mencatat setiap proses autentikasi nasabah secara transparan, tanpa perlu mengorbankan kerahasiaan data nasabah. Hal tersebut sejalan dengan asas kehati-hatian atau prudential principle di dalam hukum perbankan, di mana bank wajib menjaga integritas sistem serta kerahasiaan informasi dari nasabah merujuk pada Pasal 29 ayat (2) UU No. 10 Tahun 1998 mengenai Perbankan.

Dengan menggunakan sistem blockchain, maka setiap transaksi atau proses verifikasi akan tercatat secara permanen serta dapat diaudit sewaktu-waktu oleh regulator seperti OJK maupun Bank Indonesia.

Transaparansi dalam blockchain tidak hanya meningkatkan akuntabilitas kelembagaan, namun juga memperkuat kepercayaan publik (public trust) terhadap sistem keuangan nasional Indonesia di tengah-tengah meningkatnya kejahatan digital.

Dilihat dari sudut pandang teori hukum preventif yang dikemukakan oleh Barda Nawawi Arief, fungsi utama dari hukum bukan hanya untuk menindak setelah terjadinya kejahatan, melainkan juga untuk mencegah terjadinya pelanggaran melalui instrument normative serta sistem sosial yang efektif. Penerapan teknologi blockchain dalam sektor perbankan sejalan dengan gagasan dari Barda Nawawi Arief, karena yang pertama, dapat memberikan perlindungan preventif dengan cara menciptakan suatu sistem keamanan transaksi yang tidak dapat dimanipulasi. Kedua, menumbuhkan efek jera sosial kepada pelaku, karena pelaku kejahatan mengetahui bahwa setiap transaksi ataupun data digital terekam permanen serta dapat ditelusuri. Ketiga, dapat memperkuat legitimasi hukum digital, karena teknologi blockchain ini menyediakan bukti autentik yang diakui secara universal. Dalam konteks keuangan digital, teknologi blockchain dapat dianggap sebagai salah satu bentuk penegakan hukum preventif yang berbasis teknologi, di mana pengaturan serta penerapan sistemnya secara langsung berfungsi sebagai “penjaga hukum” atau law guardian yang mencegah terjadinya suatu tindak kejahatan.

Melihat dari tingginya risiko kejahatan siber seperti halnya deepfake, maka pengadopsian blockchain menjadi suatu kebutuhan normative di dalam reformasi sistem keamanan digital perbankan di Indonesia. Kebutuhan normatif dalam hal ini berarti bahwa keberadaan blockchain ini harus diakomodasi serta dilegitimasi oleh peraturan hukum agar memiliki kekuatan mengikat serta dapat dipertanggungjawabkan. Reformasi hukum ini penting, dikarenakan:

1. Hukum yang ada harus menyesuaikan diri dengan adanya kemajuan teknologi untuk dapat menjaga relevansi serta efektivitasnya (law as a dynamic system).
2. Blockchain dapat memberikan jaminan yuridis atas keaslian data serta integritas transaksi, di mana hal ini merupakan pilar utama dalam hukum perbankan.
3. Ketiadaan regulasi yang spesifik dapat menimbulkan kekosongan hukum (legal vacuum) yang akan menghambat inovasi sekaligus memperbesar risiko dari kejahatan digital.

Dengan demikian, maka pengadopsian blockchain ke dalam sistem keamanan digital perbankan tidak sekadar bersifat teknis semata, namun juga merupakan agenda reformasi hukum nasional yang bertujuan untuk memperkuat fungsi hukum sebagai pelindung dari kepentingan publik serta penjamin kepercayaan di dalam era transformasi digital.

Kasus penjaringan terhadap pelaku kejahatan penipuan bermodus deepfake yang telah berhasil dilakukan oleh Direktorat Reserse Siber di Jawa Timur membuktikan bahwa pencegahan menggunakan teknologi blockchain sendiri saja

tidaklah cukup tanpa adanya regulasi yang adaptif serta penegakan hukum yang efektif. Oleh sebab itu, pengadopsian teknologi blockchain harus disertai sinergi dengan kebijakan pengawasan serta penegakan hukum yang mencegah penyalahgunaan teknologi blockchain ini, serta edukasi berkelanjutan kepada para nasabah dan industri agar risiko penipuan online berbasis deepfake ini dapat diminimalisir secara holistic.

BAB IV

PENUTUP

A. Kesimpulan

Berdasarkan dari uraian-uraian diatas maka dapat disimpulkan bahwa:

1. Teknologi blockchain menawarkan sebuah solusi hukum serta teknologi inovatif untuk meningkatkan keamanan transaksi digital dalam sektor perbankan. Blockchain yang menggunakan sistem desentralisasi, transparansi, immutabilitas, serta kemanan kriptografi sehingga data transaksi akan tersimpan secara permanen serta tidak bisa dimanipulasi atau diubah. Hal ini sangat penting di dalam mencegah serta mendeteksi tindak pidana penipuan online yang bermoduskan deepfake yang dapat memanipulasi identitas digital nasabah dalam bentu video serta audio palsu.Pengaturan hukum yang ada di Indonesia saat ini belum secara spesifik mengakomodasi pemanfaatan dari teknologi blockchain ini dalam sektor perbankan sebagai instrument pencegahan kejahatan digital yang berbasis deepfake.
2. Pengadopsian teknologi blockchain dalam sektor perbankan di Indonesia mencerminkan penerapan teori hukum preventif menurut Barda Nawawi Arief, yang mengutamakan pencegahan overkriminalisasi melalui verifikasi identitas transparan via ledger immutable serta audit trail untuk forensik digital, sehingga hal ini dapat menangkal penipuan deepfake sejak pra-transaksi yang sesuai dengan Pasal 378 KUHP serta UU ITE. Selain itu, Otoritas Jasa Keuangan

(OJK) mendukung inisiatif adopsi blockchain melalui regulatory sandbox (POJK No. 13/2018), roadmap transformasi digital, serta penunjukkan Asosiasi Blockchain Indonesia (ABI) sebagai penyelenggara dari Inovasi Teknologi Sektor Keuangan atau ITSK melalui surat S-335/2025. Kepala Eksekutif Pengawasan Perbankan Otoritas Jasa Keuangan yaitu Dian Ediana Rae pada Maret 2025 menekankan bahwa manfaat dari teknologi blockchain ini sangat signifikan, terutama dalam mendorong perkembangan Decentralized Finance (DeFi), dimana hal ini dapat memungkinkan masyarakat untuk mengakses layanan keuangan tanpa melalui perantara bank maupun lembaga keuangan tradisional. DeFi ini diharapkan dapat meningkatkan efisiensi, fleksibelitas, transparansi, dan aksesibilitas terhadap produk keuangan, meskipun tetap patut mewaspadai adanya risiko yang muncul seperti contohnya pencucian uang, dll. Otoritas Jasa Keuangan juga terus melakukan pemantauan terhadap regulasi di berbagai negara terutama Uni Eropa yang telah lebih maju terkait dengan pengaturan AI serta teknologi blockchain. Namun, regulasi di Indonesia nantinya akan tetap disesuaikan dengan kebutuhan dosmetik. OJK akan terus mengkaji terkait dampak serta risiko dari blockchain dalam perbankan serta berfokus pada peningkatan literasi masyarakat. Kemudian dari kasus penipuan deepfake yang terjadi pada awal tahun 2025 yang melibatkan Gubernur Jawa Timur serta pengangkapan yang dilakukan oleh Polda Jatim menggarisbawahi pada kelemahan sistem sentralistik,

sehingga dalam hal ini blockchain muncul dengan fungsi sebagai watermark, bukti forensik sesuai Pasal 5 UU ITE, serta penguat trust perbankan berdasarkan Pasal 29 UU Perbankan 1998, kemudian dari hal ini, menuntut adanya reformasi hukum normative untuk legitimasi, menghindari legal vacuum, serta mewujudkan rule of law in digital transaformation secara holistik.

B. **Saran**

1. Otoritas Jasa Keuangan serta Bank Indonesia perlu merumuskan regulasi khusus yang mengatur mengenai penggunaan teknologi blockchain secara keseluruhan di dalam sektor perbankan, termasuk di dalamnya mengenai standar operasional, validasi, serta audit data digital. Regulasi ini harus mendorong penerapan dari mekanisme verifikasi kuat yang berbasis blockchain untuk mencegah penyalahgunaan identitas digital akibat adanya deepfake. Bank serta lembaga keuangan yang lain sebaiknya mengadopsi teknologi blockchain ini sebagai alat pengamanan utama di dalam sistem verifikasi transaksi serta identitas nasabah. Penerapan smart contracts otomatis dapat mengurangi risiko dari manipulasi serta meningkatkan efisiensi proses transaksi digital.
2. Perlu adanya kemitraan yang startegis antara sektor perbankan, pengembang teknologi AI serta Blockchain, regulator, serta apparat penegak hukum untuk mengembangkan sistem deteksi dini serta respons cepat terhadap penipuan online yang berbasis deepfake.

Teknologi AI-Blockchain terintegrasi dapat meningkatkan kemampuan verifikasi serta pelacakan dokumen digital sekaligus menyediakan bukti autentik saat terjadi sengketa hukum. Edukasi berkelanjutan kepada nasabah serta pelaku industri keuangan sangat penting untuk dapat meningkatkan kesadaran akan risiko penipuan online serta pemahaman teknologi blockchain sebagai salah satu alat proteksi digital. Sehingga hal ini, akan membantu membangun budaya keamanan digital yang kuat di kalangan masyarakat pengguna layanan perbankan. Lembaga keuangan atau bank harus meningkatkan kapasitas dari sumber daya manusia serta infrastruktur teknologi informasi agar implementasi teknologi blockchain dapat berjalan dengan optimal dan sesuai dengan ketentuan hukum. Infastruktur digital yang handal serta sumber daya manusia yang terlatih akan mampu memperkuat mekanisme pengawasan serta audit internal yang berbasis blockchain. Pengembangan kerangka hukum yang mengakui bukti berdasarkan teknologi blockchain sebagai alat bukti elektronik yang sah sangat penting untuk mendukung penegakan hukum terhadap kasus kejahatan digital atau kejahatan siber. Sehingga hal ini akan, memperkuat posisi hukum di dalam penyidikan serta persidangan perkara penipuan online.

Dengan memanfaatkan teknologi blockchain secara optimal, yang diiringi dengan penguatan regulasi, kolaborasi antar pihak, serta edukasi masyarakat, sektor perbankan Indonesia dapat membangun ekosistem

transaksi digital yang lebih aman, transparan, serta berkeadilan, sehingga hal ini, mampu mencegah tindak pidana penipuan online yang bermodus deepfake secara efektif.

Daftar Pustaka

Buku

Al-Qaradawi, Yusuf. *Fiqh al-'Aulawiyyat*: *Dirasah Jadidah fi Daw' al-Qur'an wa al-Sunnah*. Kairo: Maktabah Wahbah, 1995.

Al-Qur'an, Surah Al- Baqarah (2): Ayat 282.

Anderson, Ross. *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3rd ed., Wiley.

Arief, Barda Nawawi. *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*. Jakarta: Kencana, 2008.

Arief Barda Nawawi, *Perkembangan Sistem Pemidanaan di Indonesia*, Jakarta: Kencana, 2019.

Arief Barda Nawawi, *Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan Teknologi*, Jakarta: Kencana, 2020.

Bank Indonesia. *Blueprint Sistem Pembayaran Indonesia 2025*. Jakarta: Bank Indonesia, 2019.

De Filippi, Primavera; and Aaron Wright. *Blockchain and the Law: The Rule of Code*. Cambridge: Harvard University Press, 2018.

Hasan, Ahmad. *Fiqh Muamalah Kontemporer*. Jakarta: RajaGrafindo Persada, 2021.

Hull, J. C. *Risk Management and Financial Institutions* (ed. ke-6). New Jersey: Wiley Finance, 2021.

Krebs, Brian. *Cybersecurity in the Era of Digital Economy*. Cambridge Press, 2021.

Lessig, Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999.

Moeljatno, *Asas-Asas Hukum Pidana*, Jakarta: Rineka Cipta, 2018.

Mougayar, William. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. New Jersey: Wiley, 2016.

Narayanan, A., et al. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. New Jersey: Princeton University Press, 2016.

Nuruddin; dan Ahmad Tarigan. *Hukum Ekonomi Syariah di Indonesia*. Jakarta: Kencana, 2019.

Otoritas Jasa Keuangan*, Buku Saku OJK: Perbankan*, OJK, Jakarta, 2022.

Rudianto, *Kejahatan Siber di Era Digital: Analisis Yuridis dan Kriminologis*,. Jakarta: Sinar Grafika, 2022.

Sitompul, Josua, *Cybercrime, Cyberlaw, dan Cybersecurity*, Tatanusa, Jakarta, 2012.

Soesilo R., *Kitab Undang-Undang Hukum Pidana serta Komentar-Komentarnya*, Politeia, Bogor, 1996.

Susskind, Richard. *Tomorrow's Lawyers: An Introduction to Your Future*. Oxford: Oxford University Press, 2020.

Swan, Melanie. Blockchain: Blueprint for a New Economy. California: O'Reilly Media, 2015.

Tapscott, Don; and Alex Tapscott. *Blockchain Revolution: How Technology is Changing Money, Business, and the World*. New York: Penguin Books, 2016.

Usman, Rachmadi, *Aspek-Aspek Hukum Perbankan di Indonesia*, Jakarta :Gramedia Pustaka Utama, 2018.

Wood, Gavin; et al. *Ethereum: A Secure Decentralised Generalised Transaction Ledger*. Ethereum Research Publications, 2014.

Zuboff*,* Shoshana. *The Age of Surveillance Capitalism*. New York: PublicAffairs, 2019.

Jurnal

Beck, R., Avital, M., Rossi, M., & Thatcher, J. B. (2017). Blockchain Technology in Business and Information Systems Research. *Business & Information Systems Engineering*, 59(6), 381-384.

Cecaj, Alket, et al. (2021) Blockchain Meets Artificial Intelligence: Opportunities and Challenges. *IEEE Access* Vol. 9, hlm. 13005-13020.

Chesney, R., & Citron, D. K. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review, 107(6), 1753-1820.

Citron, DK & Chesney, Robert "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *California Law Review*, Vol. 107, No. 6, 2019, hlm. 1753.

Crosby, M., Pattanayak, P., Verma, S., dan Kalyanaraman, V. (2016). Blockchain Technology: Beyond Bitcoin. *Applied Innovation Review*, 2, hlm. 6-19.

European Banking Authority (2020). EBA Report on the Use of Big Data and Advanced Analyrics in the Banking Sector. *EBA*, hlm. 16.

Gilmour, N., & Allision, F. (2022). AI-Driven Fraud in the Financial Sector: Threats and Countermeasures. *Journal of Financial Regulation and Compliance*, 30(4), 507-523.

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., … & Bengio, Y. (2014). Generative Adversarial Nets. *Advances in Neural Information Processing Systems*, 27, 2672-2680.

Hendrawan. Tantangan Hukum terhadap Deepfake dan AI dalam Perspektif Pembuktian. *Jurnal Hukum Teknologi,* Vol. 5 No. 2 (2024), hlm. 66.

Janisriwati, Sylvia. (2023). Legal Analysis on the Use of Deepfake Technology: Threats to Indonesian Banking Institutions. *Law and Justice e-ISSN* Vol. 8 No. 2, hlm. 2549-8282.

Kietzmann, J., & Pitt, L. (2020). Deepfakes: Trick or Treat? *Business Horizons*, 63(2), 135-146.

Lansiti, M., & Lakhani, K. R. (2017). The Truth About Blockchain. *Harvard Business Review*, 95(1), 118-127.

Lembaga Perlindungan Konsumen Nasional (LPKN), *Kajian Penipuan Online di Marketplace Indonesia*, 2023.

Nuryanto. Blockchain sebagai Solusi Otentikasi Digital terhadap Kejahatan Deepfake. *Jurnal Cyber Law Review, Vol. 8 No. 1 (2024), hlm. 33.*

Peters, G. W., & Panayi, E. (2016). Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing

and Smart Contracts on the Internet of Money. *Banking Beyond Banks and Money,* pp. 239-278.

Putra, Jaya. (2022). Implementasi Smart Contracts dalam Sistem Keuangan Digital di Indonesia." *Jurnal Hukum dan Teknologi* Vol. 4 No. 2, hlm. 118.

Rachmawati. Perlindungan Data Pribadi dalam Perspektif Hukum Siber di Indonesia. *Jurnal Hukum dan HAM*, Vol. 12 No. 3 (2022), hlm. 210.

Rahman, Fitrah. Fenomena Investasi Palsu di Era Digital. *Jurnal Keuangan dan Hukum Ekonomi*, Vol. 10 No. 1 (2023), hlm. 52.

Rahmawati; Aziz, N. Blockchain dan Prospeknya dalam Perbankan Syariah di Indonesia. *Jurnal Ekonomi Syariah dan Teknologi Digital,* Vol. 3 No. 2 (2024), hlm. 67.

Santoso, Budi. Analisis Tindak Pidana Phising dalam Perspektif Hukum Siber. *Jurnal Hukum & Teknologi*, Vol. 7 No. 2 (2023), hlm. 128.

Verdoliva, L. (2020). Media Forensics and Deepfakes: An Overview. *IEEE Journal of Selected Topics in Signal Processing*, 14(5), 910-932.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? —A systematic review. *PLOS ONE*, 11(10): e0163477.

Internet

Cybercrime Report 2023, "Annual Report on Global Cybersecurity Trends", 2024. www.cyberreport.com

Digital Insight, B2B Insight. "Cybersecurity Trend 2025 dengan AI: Bagaimana Perbankan Bisa Bertahan dari Ancaman Deepfake?, 2025. https://www.binar.co.id/blog/cybersecurity-trend-2025-dengan-ai-bagaimana-perbankan-bisa-bertahan-dari-ancaman-deepfake

Direktorat Reserse Kriminal Khusus Polda Jawa Timur, *Laporan Penanganan Kasus Penipuan Online Bermodus Deepfake,* 2023.

Haryanto, Agus Tri. "Kominfo Sebut 486 Ribu Laporan Masyarakat Kena Penipuan Online, Ini Solusinya", 2023. https://inet.detik.com/law-and-policy/d-

7073942/kominfo-sebut-486-ribu-laporan-masyarakat-kena-penipuan-online-ini-solusinya

Kementerian Komunikasi dan Informatika. ”Laporan Tahunan Penanganan Kejahatan Siber di Indonesia 2022”, 2023. www.kominfo.go.id

Kementerian Komunikasi dan Informatika. “Potensi Blockchain di Indonesia: Peluang dan Tantangan Tahun 2023”, 2024. www.kominfo.go.id

Kompas.com, “Kasus Penipuan Deepfake Gubernur Khofifah Rugikan Masyarakat hingga Puluhan Juta,” 15 Januari 2022.

Nakamoto, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008. https://bitcoin.org/bitcoin.pdf.

Otoritas Jasa Keuangan, *Kajian Inovasi Teknologi Blockchain dalam Keuangan Syariah*, Jakarta, 2024.

Santoso, Bangun; dan Faqih Fathurrahman. “Polisi Bongkar Penipuan Modus Deep Fake Catut Nama Dedi Mulyadi hingga Khofifah“, 2025. https://www.suara.com/news/2025/04/29/192551/polisi-bongkar-penipuan-modus-deep-fake-catut-nama-dedi-mulyadi-hingga-khofifah

Peraturan

DSN-MUI, *Fatwa No. 116/DSN-MUI/IX/2017* tentang Uang Elektronik Syariah.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016: Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 5 ayat (1).