

Academia Open

Vol. 10 No. 2 (2025): December

DOI: 10.21070/acopen.10.2025.12855

Table Of Contents

Journal Cover	1
Author[s] Statement.....	3
Editorial Team	4
Article information	5
Check this article update (crossmark)	5
Check this article impact	5
Cite this article.....	5
Title page.....	6
Article Title	6
Author information	6
Abstract	6
Article content	8

Originality Statement

The author[s] declare that this article is their own work and to the best of their knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the published of any other published materials, except where due acknowledgement is made in the article. Any contribution made to the research by others, with whom author[s] have work, is explicitly acknowledged in the article.

Conflict of Interest Statement

The author[s] declare that this article was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Copyright Statement

Copyright © Author(s). This article is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at <http://creativecommons.org/licences/by/4.0/legalcode>

Academia Open

Vol. 10 No. 2 (2025): December
DOI: 10.21070/acopen.10.2025.12855

EDITORIAL TEAM

Editor in Chief

Mochammad Tanzil Multazam, Universitas Muhammadiyah Sidoarjo, Indonesia

Managing Editor

Bobur Sobirov, Samarkand Institute of Economics and Service, Uzbekistan

Editors

Fika Megawati, Universitas Muhammadiyah Sidoarjo, Indonesia

Mahardika Darmawan Kusuma Wardana, Universitas Muhammadiyah Sidoarjo, Indonesia

Wiwit Wahyu Wijayanti, Universitas Muhammadiyah Sidoarjo, Indonesia

Farkhod Abdurakhmonov, Silk Road International Tourism University, Uzbekistan

Dr. Hindarto, Universitas Muhammadiyah Sidoarjo, Indonesia

Evi Rinata, Universitas Muhammadiyah Sidoarjo, Indonesia

M Faisal Amir, Universitas Muhammadiyah Sidoarjo, Indonesia

Dr. Hana Catur Wahyuni, Universitas Muhammadiyah Sidoarjo, Indonesia

Complete list of editorial team ([link](#))

Complete list of indexing services for this journal ([link](#))

How to submit to this journal ([link](#))

Academia Open

Vol. 10 No. 2 (2025): December
DOI: 10.21070/acopen.10.2025.12855

Article information

Check this article update (crossmark)

Check this article impact (*)

Save this article to Mendeley

(*) Time for indexing process is various, depends on indexing database platform

Legal Liability for Force Majeure in Digital Crypto Asset Contracts Reviewed from the Perspective of Legal Rationality in the Digital Age

Tanggung Jawab Hukum atas Keadaan Force Majeure dalam Kontrak Digital Aset Kripto Ditinjau dari Rasionalitas Hukum di Era Digital

Amara Diva Abigail, amaradivaabigail@unmuhjember.ac.id, (1)

Fakultas Hukum, Universitas Jember, Indonesia

Diah Ayuning Tyas, notarisayune@gmail.com, (0)

Fakultas Hukum, Universitas Jember, Indonesia

Fendi Setyawan, fendisetawan.fh@unej.ac.id, (0)

Fakultas Hukum, Universitas Jember, Indonesia

M. Arief Amrullah, arief.fh@unej.ac.id, (0)

Fakultas Hukum, Universitas Jember, Indonesia

⁽¹⁾ Corresponding author

Abstract

General Background: The rapid advancement of digital technology has transformed legal relations through the emergence of smart contracts and crypto asset transactions operating autonomously on blockchain systems. **Specific Background:** Although these digital contracts promise efficiency and certainty, their automated and decentralized nature raises complex legal issues when force majeure events—such as cyberattacks, system failures, or sudden regulatory changes—disrupt contractual performance. **Knowledge Gap:** Existing civil law doctrines on force majeure and contractual liability are primarily designed for human-centered agreements and remain inadequate to address responsibility in algorithm-driven systems, particularly within Indonesia's legal framework. **Aims:** This study aims to analyze legal liability for force majeure in crypto asset digital contracts through a philosophical examination of legal rationality in the digital era. **Results:** Using normative–philosophical analysis, the study finds that traditional fault-based liability and positivistic legal rationality require reconstruction to accommodate technological risks and automated execution. **Novelty:** The research introduces an adaptive, reflective conception of legal rationality that integrates technological realities with principles of justice, certainty, and utility. **Implications:** These findings imply the need for explicit force majeure clauses, shared responsibility models, and adaptive legal interpretation to ensure fair and effective regulation of digital contracts in the evolving crypto ecosystem.

Highlights:

- Force majeure in crypto-based smart contracts involves technological and regulatory risks beyond traditional doctrines.
- Automated and decentralized contract execution challenges fault-based and human-centered legal liability concepts.

- ♦ Adaptive legal rationality is essential to balance legal certainty, justice, and technological innovation in the digital era.

Keywords: Force Majeure, Digital Contracts, Crypto Assets, Legal Liability, Legal Rationality

Published date: 2025-12-19

Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan fundamental dalam berbagai bidang kehidupan manusia, termasuk dalam sistem hukum dan praktik keperdataan. Salah satu fenomena yang paling menarik dalam dua dekade terakhir adalah munculnya kontrak digital atau smart contract yang beroperasi melalui teknologi blockchain, serta penggunaan aset kripto (crypto assets) sebagai objek dan instrumen transaksi digital. Kombinasi antara kontrak digital dan aset kripto tersebut menghadirkan bentuk baru hubungan hukum yang bersifat otonom, terdesentralisasi, dan lintas yurisdiksi. Namun, di balik kemajuan teknologi ini, muncul persoalan penting mengenai bagaimana tanggung jawab hukum dapat diterapkan ketika terjadi *force majeure*—keadaan memaksa yang menghalangi pelaksanaan kontrak dalam konteks sistem digital yang otomatis dan tak terpusat [1].

Dalam hukum perdata klasik, kontrak merupakan perjanjian antara dua atau lebih pihak yang menimbulkan akibat hukum berupa hak dan kewajiban. Hubungan kontraktual ini didasarkan pada asas kebebasan berkontrak sebagaimana diatur dalam Pasal 1338 Kitab Undang-Undang Hukum Perdata (KUHPerdata), yang menegaskan bahwa “semua perjanjian yang dibuat secara sah berlaku sebagai undang-undang bagi mereka yang membuatnya. Prinsip ini mengandung makna bahwa kontrak lahir dari kesepakatan rasional para pihak yang bebas menentukan isi dan bentuknya, sepanjang tidak bertentangan dengan undang-undang, kesusilaan, dan ketertiban umum[2].

Namun, kehadiran smart contract mengubah wajah kontraktual tersebut. Smart contract merupakan perjanjian digital yang dieksekusi secara otomatis oleh sistem komputer melalui algoritma tertentu ketika syarat yang disepakati terpenuhi. Teknologi blockchain memungkinkan transaksi direkam secara permanen, transparan, dan tidak dapat diubah (*immutable*). Dengan demikian, pelaksanaan kontrak tidak lagi membutuhkan campur tangan manusia, melainkan dilakukan oleh kode yang telah ditanam dalam sistem. Kondisi ini memunculkan konsekuensi hukum baru: bagaimana hukum memandang “kesepakatan” dalam sistem otomatis dan siapa yang bertanggung jawab apabila terjadi kegagalan sistem.

Menurut penelitian Siregar [3], smart contract tetap memenuhi unsur sahnya perjanjian sebagaimana diatur dalam Pasal 1320 KUHPerdata—yakni adanya kesepakatan, kecakapan, suatu hal tertentu, dan sebab yang halal—meskipun bentuknya digital. Namun, bentuk digital tersebut menimbulkan problem baru karena tidak ada lagi “tanda tangan” atau “kehendak eksplisit” manusia setelah kontrak berjalan. Artinya, pelaksanaan kewajiban terjadi bukan atas dasar kehendak aktual, melainkan kehendak yang terprogram sebelumnya.

Perkembangan *smart contract* tidak dapat dilepaskan dari munculnya aset kripto sebagai objek transaksi digital. Aset kripto merupakan bentuk nilai digital yang menggunakan kriptografi untuk mengamankan transaksi, dikendalikan oleh jaringan *blockchain*, dan tidak bergantung pada otoritas pusat.⁵ Di Indonesia, aset kripto diakui sebagai komoditas yang dapat diperdagangkan di bursa berjangka berdasarkan Peraturan Bappebti No. 8 Tahun 2021. Namun, pengaturan mengenai aset kripto sebagai objek kontrak perdata masih belum spesifik, terutama dalam konteks tanggung jawab hukum[4].

Aset kripto memiliki sifat unik: desentralisasi, volatilitas tinggi, dan ketergantungan pada infrastruktur digital global. Dalam kontrak digital, aset kripto dapat menjadi alat tukar, jaminan, atau instrumen investasi. Misalnya, kontrak *staking* atau *decentralized finance (DeFi)* menggunakan mekanisme otomatis di mana pengguna mengunci aset kripto untuk mendapatkan imbal hasil. Sistem ini bergantung pada kode algoritma, dan kegagalan sistem dapat menyebabkan kerugian besar bagi pengguna tanpa mekanisme tanggung jawab yang jelas. Dalam situasi seperti itu, apabila terjadi gangguan teknologi seperti *network failure*, *hacking*, atau *smart contract bug*, maka pelaksanaan kontrak tidak dapat berjalan sebagaimana mestinya.

Dalam doktrin hukum perdata Indonesia, *force majeure* atau keadaan memaksa merupakan keadaan di luar kemampuan manusia yang menyebabkan suatu prestasi tidak dapat dilaksanakan.⁸ Meskipun istilah “*force majeure*” tidak secara eksplisit disebut dalam KUHPerdata, prinsipnya dapat ditemukan dalam Pasal 1244 dan Pasal 1245. Pasal 1244 menyatakan bahwa debitur harus mengganti biaya, kerugian, dan bunga jika tidak dapat membuktikan bahwa keterlambatan atau kegagalan prestasi disebabkan oleh hal yang tidak terduga. Sedangkan Pasal 1245 memberikan pengecualian: debitur tidak perlu mengganti kerugian jika tidak dapat melaksanakan kewajiban karena kejadian di luar kesalahannya[5]. Dalam praktik, *force majeure* sering diartikan sebagai peristiwa alam, perang, kebakaran, atau kebijakan pemerintah yang menghalangi pelaksanaan kontrak. Namun, dalam konteks digital, *force majeure* dapat berupa kegagalan sistem, gangguan server global, kerentanan algoritma, atau serangan siber. Hal ini menimbulkan perdebatan: apakah kerusakan sistem yang masih dalam kendali teknologi dapat dianggap sebagai keadaan memaksa, atau merupakan bagian dari risiko kontraktual?

Sebagai contoh, penelitian oleh Mulyana [6] menjelaskan bahwa definisi *force majeure* harus disesuaikan dengan perkembangan teknologi, karena hukum yang kaku akan sulit menjawab persoalan modern seperti kegagalan algoritma atau serangan *ransomware* terhadap sistem digital. Kontrak digital dan *smart contract* bersifat deterministik—yakni dijalankan secara otomatis tanpa ruang interpretasi. Kelebihan ini memberikan kepastian pelaksanaan, namun sekaligus menghilangkan fleksibilitas hukum. Ketika *force majeure* terjadi, sistem tidak dapat menyesuaikan diri, karena kode akan tetap mengeksekusi perintah sesuai program. Hal ini menimbulkan pertanyaan filosofis: dapatkah tanggung jawab hukum diterapkan kepada sistem non-manusia yang hanya menjalankan instruksi?

Di satu sisi, pengembang atau operator sistem dapat berargumen bahwa kerusakan akibat *bug* atau *cyber attack* merupakan *force majeure* karena berada di luar kendali mereka. Di sisi lain, pengguna mungkin beranggapan bahwa penyelenggara seharusnya memprediksi risiko tersebut dengan menyediakan sistem keamanan memadai. Ketegangan antara prinsip *strict liability* dan *fault-based liability* menjadi semakin kabur dalam konteks kontrak digital[7].

Dalam sistem hukum Indonesia, tanggung jawab kontraktual menuntut adanya unsur kesalahan (*culpa*). Namun, bagaimana menentukan kesalahan jika pelaksanaan dilakukan oleh sistem otomatis? Filosofisnya, konsep kesalahan lahir dari kehendak dan rasionalitas manusia. Ketika kontrak dijalankan oleh kode, maka “kehendak” itu telah dihilangkan, sementara tanggung jawabnya masih dibebankan pada manusia yang merancang sistem tersebut.

Rasionalitas hukum tradisional berpijak pada logika manusia: hukum dianggap sebagai produk dari rasio, kehendak, dan nilai-nilai moral manusia. Menurut Lon L. Fuller, hukum merupakan sistem norma yang berorientasi pada tujuan moral dan rasional, sehingga kepastian dan keadilan harus berjalan seimbang. Namun, perkembangan digital menghadirkan rasionalitas baru—rasionalitas algoritmik—di mana keputusan dan pelaksanaan kontrak tidak lagi melalui proses penalaran manusia, melainkan proses komputasi otomatis.

Fenomena ini menantang eksistensi hukum sebagai sistem normatif. Apakah hukum masih bisa mengontrol sistem otomatis yang bekerja tanpa interpretasi manusia? Menurut Lawrence Lessig, dalam dunia digital “*code is law*”, artinya kode komputer memiliki kekuatan regulatif seperti hukum[8].

Dengan demikian, jika kontrak dijalankan oleh algoritma, maka hukum formal dapat kehilangan otonominya. Rasionalitas hukum klasik—yang didasarkan pada kehendak manusia dan moralitas—menghadapi krisis dalam era digital. Hal ini menimbulkan persoalan mendalam: ketika *force majeure* terjadi dalam *smart contract*, bagaimana hukum harus bertindak? Apakah hukum cukup dengan menafsirkan ulang doktrin *force majeure*, atau perlu membangun paradigma baru tentang tanggung jawab digital?

Dari sudut pandang filsafat hukum, pergeseran dari kontrak manual ke kontrak otomatis menuntut rekonstruksi rasionalitas hukum. Hans Kelsen dalam *Pure Theory of Law* menegaskan bahwa hukum adalah sistem normatif yang terlepas dari moralitas dan faktualitas sosial. Namun, teori ini tidak memadai untuk menjelaskan kompleksitas hubungan manusia-teknologi. Sebaliknya, H.L.A. Hart menekankan bahwa hukum bukan hanya perintah, tetapi juga sistem aturan yang diinterpretasikan secara sosial. Dalam kontrak digital, interpretasi sosial hampir hilang, karena pelaksanaan bersifat otomatis[9].

Oleh karena itu, rasionalitas hukum di era digital harus bergeser dari “rasionalitas positif” menuju “rasionalitas reflektif”—yakni hukum yang tidak hanya menilai kepastian norma, tetapi juga mempertimbangkan dimensi keadilan dan kemanusiaan dalam ruang digital. Kajian filosofis terhadap tanggung jawab hukum dalam *force majeure* digital menjadi penting agar hukum tetap relevan terhadap perubahan teknologi.

Kajian ini menjadi penting karena realitas hukum Indonesia belum memiliki regulasi yang spesifik terkait tanggung jawab dalam kontrak digital berbasis *blockchain*. UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) memang mengakui validitas dokumen dan tanda tangan elektronik, tetapi belum menjawab persoalan tanggung jawab dalam sistem otomatis. Begitu pula, regulasi aset kripto oleh Bappebti lebih menekankan aspek perdagangan, bukan tanggung jawab kontraktual. Akibatnya, terjadi kekosongan hukum (*legal vacuum*) ketika *force majeure* muncul dalam kontrak digital.

Secara praktis, hal ini berpotensi merugikan pengguna yang tidak memahami aspek teknis kontrak digital. Secara filosofis, hukum menghadapi tantangan eksistensial: bagaimana menegakkan keadilan dalam sistem yang dikendalikan algoritma. Maka, penelitian ini bertujuan untuk menganalisis tanggung jawab hukum atas *force majeure* dalam kontrak digital aset kripto serta merefleksikan rasionalitas hukum di era digital agar tetap menjamin kepastian, keadilan, dan kemanfaatan hukum.

Metode

Penelitian ini merupakan penelitian hukum normatif (*normative legal research*) dengan pendekatan filosofis dan konseptual. Penelitian hukum normatif dilakukan dengan mengkaji norma-norma hukum positif, asas-asas hukum, serta doktrin yang berkaitan dengan tanggung jawab hukum dalam keadaan *force majeure* pada kontrak digital aset kripto. Pendekatan filosofis digunakan untuk memahami dan merefleksikan rasionalitas hukum dalam merespons perkembangan teknologi digital, khususnya dalam konteks otomatisasi kontrak (*smart contract*) dan penggunaan aset kripto. Pendekatan ini membantu mengungkap dimensi nilai dan rasionalitas di balik norma hukum, serta menjawab pertanyaan apakah konsep tanggung jawab hukum tradisional masih relevan dalam dunia digital yang dikendalikan algoritma. Selain itu, digunakan juga pendekatan konseptual (*conceptual approach*) untuk menganalisis konsep-konsep kunci seperti *force majeure*, kontrak digital, tanggung jawab hukum, dan rasionalitas hukum. Pendekatan ini bertujuan untuk membangun pemahaman teoretis yang utuh dan menemukan kemungkinan rekonstruksi konsep hukum dalam konteks era digital.

Bahan hukum primer meliputi peraturan perundang-undangan yang relevan, antara lain:

1. Kitab Undang-Undang Hukum Perdata (KUHPerdata), khususnya Pasal 1320, 1338, 1244, dan 1245.
2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).
3. Peraturan Bappebti Nomor 8 Tahun 2021 tentang Pedoman Penyelenggaraan Pasar Fisik Aset Kripto.
4. Konvensi internasional dan prinsip hukum perdata modern yang relevan dengan *force majeure* dan kontrak digital, seperti *UNIDROIT Principles of International Commercial Contracts* (2016)

Bahan hukum sekunder mencakup literatur hukum dan filsafat hukum seperti buku, jurnal, artikel ilmiah, serta hasil penelitian yang membahas kontrak digital, aset kripto, tanggung jawab hukum, dan rasionalitas hukum. Sumber utama meliputi karya dari Hans Kelsen, Lon L. Fuller, Lawrence Lessig, H.L.A. Hart, serta literatur kontemporer tentang *smart contract* dan hukum siber.

Pengumpulan bahan hukum dilakukan melalui metode studi kepustakaan (library research). Metode ini mencakup kegiatan penelusuran terhadap:

- a. Dokumen hukum positif yang berlaku di Indonesia dan internasional.
- b. Literatur ilmiah dari jurnal nasional dan internasional yang berkaitan dengan *blockchain*, *smart contract*, dan *force majeure*.
- c. Sumber primer klasik dari filsafat hukum untuk memahami kerangka rasionalitas hukum.

Seluruh bahan hukum dikumpulkan secara sistematis untuk kemudian diklasifikasi berdasarkan relevansinya terhadap tiga aspek utama penelitian: (1) *force majeure* dalam kontrak digital, (2) tanggung jawab hukum para pihak, dan (3) refleksi filosofis atas rasionalitas hukum di era digital.

Bahan hukum yang telah dikumpulkan dianalisis menggunakan metode analisis kualitatif deskriptif dan reflektif.

1. Analisis deskriptif digunakan untuk menggambarkan secara sistematis pengaturan hukum positif mengenai *force majeure*, kontrak digital, dan aset kripto, serta praktik penerapannya di berbagai yurisdiksi.
2. Analisis reflektif-filosofis digunakan untuk mengkaji dasar rasionalitas hukum di balik norma-norma tersebut. Pendekatan ini bertujuan menemukan makna substantif dari tanggung jawab hukum dalam konteks digital, serta menggali kemungkinan rekonstruksi hukum agar tetap relevan dengan perubahan teknologi.

Dalam analisis ini, peneliti juga menerapkan pendekatan hermeneutik hukum, yaitu penafsiran terhadap teks hukum dan doktrin untuk menemukan makna filosofis dan nilai rasional di baliknya. Hermeneutik hukum digunakan agar interpretasi tidak berhenti pada tataran formal-normatif, tetapi juga mempertimbangkan konteks sosial dan teknologi yang melatarbelakanginya. Untuk memperkaya analisis, penelitian ini juga menggunakan pendekatan perbandingan hukum (comparative approach) secara terbatas, dengan membandingkan pengaturan dan praktik hukum di beberapa yurisdiksi seperti Uni Eropa dan Amerika Serikat. Misalnya, *European Union Blockchain Observatory and Forum* (2020) telah mengatur prinsip *force majeure* dalam konteks *smart contract*, dan beberapa yurisdiksi AS telah menerapkan doktrin “impossibility” atau “frustration of purpose” terhadap kontrak digital [10].

Hasil dan Pembahasan

A. Konsep dan Kedudukan Force Majeure dalam hukum Kontrak, khususnya dalam konteks Transaksi digital Aset Kripto

Perkembangan teknologi digital telah membawa perubahan signifikan dalam cara manusia melakukan transaksi ekonomi. Salah satu inovasi yang paling menonjol adalah munculnya aset kripto sebagai instrumen digital yang dapat diperdagangkan secara global. Aset kripto, seperti Bitcoin, Ethereum, dan berbagai token digital lainnya, beroperasi melalui teknologi blockchain yang terdesentralisasi, memungkinkan transaksi berlangsung tanpa memerlukan lembaga keuangan tradisional sebagai perantara. [11]

Seiring dengan meningkatnya volume dan kompleksitas transaksi kripto, muncul pula berbagai risiko yang bersifat unik, termasuk risiko teknis, risiko keamanan siber, dan risiko regulasi.

Dalam konteks hukum kontrak, salah satu aspek penting yang perlu diperhatikan adalah *force majeure*, yaitu keadaan di luar kendali para pihak yang dapat memengaruhi pelaksanaan kewajiban kontraktual. Dengan kata lain, bagaimana hukum memandang dan menempatkan konsep *force majeure* dalam transaksi digital aset kripto menjadi sangat relevan untuk menjamin kepastian hukum, keadilan, dan efisiensi kontrak. [12]

Force majeure (keadaan memaksa) merupakan suatu keadaan luar biasa yang menyebabkan pihak dalam kontrak tidak dapat memenuhi prestasinya karena hal di luar kendali dan tidak dapat diprediksi. Dalam konteks hukum Indonesia, dasar hukumnya dapat ditemukan dalam Pasal 1244 dan 1245 KUH Perdata, yang pada intinya menyatakan bahwa debitur tidak wajib mengganti kerugian apabila ia tidak dapat melaksanakan kewajibannya karena suatu hal yang tidak dapat dipertanggungjawabkan kepadanya. Umumnya, keadaan *force majeure* harus memenuhi unsur: [13]

- a. Terjadi peristiwa di luar kekuasaan para pihak (misalnya bencana alam, peperangan, gangguan sistem global).
- b. Tidak dapat diperkirakan sebelumnya saat kontrak dibuat.
- c. Tidak dapat dihindari meskipun pihak telah beritikad baik.

d. Menimbulkan ketidakmungkinan objektif untuk melaksanakan kewajiban kontraktual.

Konsep *force majeure* berfungsi untuk melindungi pihak yang tidak bersalah dari tanggung jawab akibat kegagalan pelaksanaan kontrak karena keadaan di luar kendalinya. Dengan demikian, prinsip keadilan dan keseimbangan kontraktual tetap terjaga dalam sistem hukum perdata Indonesia: [14]

1. *Force majeure* merupakan alasan peniadaan tanggung jawab (*exoneration clause*).

2. Para pihak diperbolehkan mengatur secara eksplisit dalam kontrak bentuk-bentuk keadaan yang dikategorikan sebagai *force majeure*.

3. Dalam praktiknya, banyak kontrak bisnis (termasuk kontrak digital) mencantumkan klausula *force majeure* dengan rinci, seperti: “kerusakan sistem elektronik, serangan siber, gangguan jaringan global, atau kegagalan sistem blockchain.”

Force Majeure dalam Konteks Transaksi Digital Aset Kripto memiliki Karakteristik Khusus Transaksi Kripto dilakukan secara terdesentralisasi melalui teknologi blockchain, tanpa perantara sentral, serta bergantung pada infrastruktur digital (internet, server, node, dan jaringan global). Oleh karena itu, risiko *force majeure*-nya bersifat teknologis, bukan hanya fisik.

Bentuk *Force Majeure* dalam Transaksi Kripto antara lain: [15]

a. Kegagalan sistem blockchain atau *network crash* global.

b. Serangan siber (*cyber attack*), seperti *51% attack*, *hacking*, atau *smart contract exploit*.

c. Gangguan infrastruktur digital, seperti *server down*, *power outage*, atau *internet blackout*.

d. Perubahan regulasi secara tiba-tiba (misalnya larangan perdagangan kripto oleh pemerintah) yang membuat pelaksanaan kontrak menjadi tidak mungkin.

Hingga saat ini, Indonesia belum memiliki regulasi khusus yang mengatur *force majeure* dalam transaksi aset kripto. Namun, prinsip umum hukum kontrak tetap berlaku, sehingga: [16]

1. Pihak yang tidak dapat melaksanakan kewajiban karena sebab di luar kendalinya dapat menggunakan dasar *force majeure* sesuai Pasal 1244–1245 KUH Perdata.

2. Dalam kontrak digital (misalnya *smart contract* atau perjanjian pengguna bursa kripto), klausula *force majeure* biasanya diatur secara eksplisit untuk mencakup risiko teknologi.

Adapun beberapa Tantangan Penerapan dalam penerapan *force majeure* pada transaksi kripto: [17]

a. Sulitnya pembuktian apakah gangguan sistem benar-benar di luar kendali pengguna.

b. Ketidadaan pihak sentral dalam blockchain menyebabkan tidak jelas siapa yang bertanggung jawab.

c. Klausula otomatis dalam smart contract sering kali tidak memiliki mekanisme pembatalan akibat *force majeure*.

B. Bentuk Tanggung Jawab Hukum Para Pihak dalam Kontrak Digital Aset Kripto Jika Terjadi Force Majeure

Force majeure merupakan istilah hukum yang secara tradisional digunakan untuk merujuk pada peristiwa di luar kendali manusia, yang menyebabkan pelaksanaan suatu kewajiban kontraktual menjadi tidak mungkin atau secara signifikan terganggu. Dalam Kitab Undang-Undang Hukum Perdata (KUHPerdata), meskipun istilah *force majeure* tidak disebutkan secara eksplisit, prinsip serupa tercermin dalam Pasal 1244–1245 KUHPerdata yang mengatur tentang perikatan dan pengecualian tanggung jawab apabila terjadi keadaan yang tidak dapat diperkirakan. Dalam konteks kontrak digital aset kripto, *force majeure* bisa terjadi dalam beberapa bentuk, antara lain: [18] kegagalan jaringan blockchain, serangan siber (*cyberattack*), kerusakan sistem otomatisasi kontrak (*smart contract malfunction*), atau regulasi pemerintah yang tiba-tiba melarang transaksi tertentu. Bentuk-bentuk ini menunjukkan bahwa *force majeure* di dunia digital tidak selalu identik dengan bencana alam atau perang, tetapi juga mencakup gangguan teknologis dan hukum [19].

Dalam perspektif filsafat hukum, *force majeure* menggambarkan ketegangan antara prinsip kepastian hukum (*legal certainty*) dan keadilan (*justice*). Kepastian hukum menuntut kontrak dilaksanakan sesuai ketentuan, sedangkan keadilan menuntut agar pihak tidak dirugikan akibat peristiwa yang berada di luar kendalinya. Dalam kontrak digital, ketegangan ini semakin kompleks karena kontrak bersifat otomatis dan berjalan tanpa intervensi manusia langsung.

Secara umum, tanggung jawab hukum dalam kontrak tradisional terbagi menjadi dua bentuk: [20]

1. Tanggung jawab wanprestasi (*breach of contract*), yaitu kewajiban untuk mengganti kerugian akibat pelanggaran kontrak yang disengaja atau kelalaian.

2. Pengecualian tanggung jawab, yaitu situasi di mana pihak yang seharusnya bertanggung jawab dibebaskan karena peristiwa di luar kendali (*force majeure*). Dalam KUHPdata, Pasal 1245 menyatakan bahwa debitur dibebaskan dari tanggung jawab bila perikatan tidak dilaksanakan akibat sebab yang tidak dapat dipertanggungjawabkan.

Dalam praktik kontrak tradisional, pihak yang mengklaim *force majeure* harus membuktikan bahwa: [21]

- a. Peristiwa tersebut benar-benar berada di luar kontrolnya,
- b. Tidak dapat diperkirakan sebelumnya, dan
- c. Menjadi penyebab utama ketidakmungkinan pelaksanaan kewajiban

Kontrak digital aset kripto sering diwujudkan dalam bentuk smart contract, yaitu kode program yang berjalan otomatis di blockchain dan mengeksekusi perjanjian berdasarkan kondisi yang telah ditentukan.⁸ Beberapa karakteristik unik kontrak digital ini yang memengaruhi tanggung jawab hukum adalah: [22]

1. Otomatisasi Eksekusi – Kontrak berjalan tanpa perlu intervensi manusia; pelanggaran atau ketidakmampuan untuk melaksanakan kewajiban dapat terjadi akibat bug atau kesalahan teknis.
2. Transparansi dan Immutabilitas – Semua transaksi terekam secara permanen di blockchain, sehingga klaim tanggung jawab lebih mudah diverifikasi, tetapi koreksi kesalahan teknis menjadi sulit.
3. Globalitas – Aset kripto dapat diperdagangkan lintas yurisdiksi, sehingga menimbulkan ketidakpastian hukum mengenai forum dan hukum yang berlaku.

Akibat karakteristik tersebut, tanggung jawab hukum dalam kontrak digital tidak bisa hanya mengandalkan prinsip tradisional. Misalnya, jika terjadi kegagalan kontrak akibat serangan siber, tidak selalu jelas siapa pihak yang bertanggung jawab karena kerusakan bersifat teknologi, bukan perilaku manusia langsung.

Dalam konteks digital tanggung jawab hukum para pihak dapat dianalisis melalui tiga perspektif yaitu :

Debitur adalah pihak yang berkewajiban untuk melaksanakan kontrak. Dalam *force majeure*, debitur dapat dibebaskan dari kewajiban jika memenuhi kriteria berikut: [23]

- a. Menunjukkan bahwa peristiwa berada di luar kendali. Misalnya, *smart contract* gagal karena bug yang tidak diketahui sebelumnya.
- b. Memberikan pemberitahuan tepat waktu kepada kreditur mengenai keadaan tersebut.
- c. Tidak ada unsur kelalaian atau kesengajaan dalam pemeliharaan sistem.

Namun, kebebasan ini tidak absolut. Dalam beberapa yurisdiksi, debitur tetap dapat dimintai tanggung jawab jika kegagalan teknis dapat diprediksi dan diantisipasi dengan langkah mitigasi yang wajar. Dalam hal aset kripto, mitigasi ini bisa berupa audit kontrak, penggunaan protokol cadangan (*fallback protocol*), atau asuransi siber.

Kreditur atau penerima manfaat kontrak juga memiliki tanggung jawab dalam kontrak digital. Misalnya, jika kontrak gagal akibat kesalahan pihak penerima (seperti salah alamat dompet kripto atau kegagalan menyetorkan dana yang diperlukan), maka kreditur dapat dianggap turut bertanggung jawab.

Dalam filosofi hukum, hal ini menunjukkan distribusi tanggung jawab berbasis rasionalitas: kontrak digital tidak hanya menuntut kewajiban hukum unilateral, tetapi juga tanggung jawab bersama untuk memastikan keberhasilan eksekusi otomatis. Beberapa peristiwa *force majeure* digital melibatkan pihak ketiga, misalnya penyedia infrastruktur blockchain atau penyedia layanan dompet kripto. Pertanggungjawaban pihak ketiga ini masih menjadi area abu-abu hukum, karena regulasi atas *service provider* digital di Indonesia dan internasional belum jelas. Dalam konteks ini, prinsip filosofi hukum modern mengusulkan adanya konsep tanggung jawab bersama (*shared responsibility*), yang memperluas paradigma tradisional debitur–kreditur. Dengan demikian, jika *force majeure* terjadi akibat serangan pada jaringan blockchain, tanggung jawab dapat dibagi antara debitur, kreditur, dan penyedia infrastruktur. [24]

Selain tanggung jawab kontraktual, *force majeure* digital dapat menimbulkan tanggung jawab non-kontraktual, seperti:

1. Tanggung jawab pidana, jika terjadi peretasan atau manipulasi transaksi.
2. Tanggung jawab perdata, jika pihak yang mengalami kerugian mengajukan tuntutan ganti rugi karena kelalaian atau wanprestasi yang tidak dapat dikategorikan sebagai *force majeure*.

Fenomena ini memperlihatkan bahwa *force majeure* di dunia digital menuntut redefinisi tanggung jawab hukum yang lebih fleksibel. Konsep tradisional “tidak dapat dipertanggungjawabkan” harus diperluas untuk mencakup:

- a. Kegagalan teknis yang tidak dapat diprediksi,

b. Risiko siber,

c. Faktor eksternal regulatif dan geopolitik

Untuk mengurangi ketidakpastian hukum, kontrak digital aset kripto harus menyertakan klausul *force majeure* secara eksplisit. Klausul ini biasanya memuat:

1. Definisi peristiwa *force majeure*, termasuk bencana alam, kegagalan jaringan, serangan siber, atau perubahan regulasi.
2. Mekanisme pemberitahuan kepada pihak lain.
3. Batas tanggung jawab pihak dalam situasi darurat.
4. Mekanisme mitigasi dan penyelesaian sengketa.

Dengan klausul ini, tanggung jawab hukum menjadi lebih jelas, dan risiko hukum dapat dialihkan atau diminimalkan sesuai kesepakatan para pihak. Filosofinya, klausul ini adalah manifestasi prinsip rasionalitas hukum, yang menyeimbangkan kepastian hukum dan keadilan

Tanggung jawab hukum dalam *force majeure* digital menghadapi beberapa tantangan filosofis:

- a. Ketidakpastian Algoritmik – Sistem otomatis mungkin gagal tanpa kesalahan manusia. Dalam filsafat hukum, hal ini menimbulkan pertanyaan: siapa yang menjadi subjek hukum?
- b. Globalitas Transaksi – Aset kripto bersifat lintas yurisdiksi, sehingga hukum nasional tidak selalu bisa diterapkan secara konsisten.
- c. Asimetri Informasi – Pihak yang memahami teknologi lebih baik memiliki keunggulan, yang dapat menimbulkan ketidakadilan jika tidak ada regulasi yang jelas.

Oleh karena itu, kajian filosofi hukum menyarankan adanya rekonstruksi rasionalitas hukum, yaitu: hukum harus adaptif terhadap teknologi, mampu mengidentifikasi tanggung jawab non-tradisional, dan tetap menjaga prinsip keadilan serta kepastian hukum.

Simpanan

1. Konsep dan Kedudukan Force Majeure dalam Kontrak Digital Aset KriptoForce majeure merupakan prinsip hukum kontrak yang memberikan perlindungan kepada pihak yang tidak dapat melaksanakan kewajibannya akibat peristiwa di luar kendali dan tidak dapat diprediksi. Dalam konteks transaksi digital aset kripto, force majeure memiliki karakteristik khusus karena menyangkut risiko teknologi, seperti kegagalan sistem blockchain, serangan siber, gangguan infrastruktur digital, atau perubahan regulasi mendadak. Secara hukum, force majeure tetap berlandaskan pada prinsip umum KUH Perdata (Pasal 1244–1245), namun penerapannya perlu disesuaikan dengan sifat terdesentralisasi dan otomatisasi kontrak digital.
2. Bentuk Tanggung Jawab Hukum dalam Keadaan Force MajeureKetika force majeure terjadi, tanggung jawab hukum para pihak dalam kontrak digital aset kripto dapat dikurangi atau dibebaskan, selama peristiwa tersebut memenuhi unsur-unsur force majeure: tidak dapat diperkirakan, di luar kendali, dan tidak dapat dihindari. Namun, dalam praktiknya, penerapan tanggung jawab hukum menghadapi tantangan khusus, seperti pembuktian kejadian force majeure, tidak adanya pihak sentral yang bertanggung jawab, serta keterbatasan smart contract dalam menanggapi peristiwa luar biasa. Oleh karena itu, klausula force majeure dalam kontrak digital perlu dirumuskan secara eksplisit untuk memberikan kepastian hukum bagi para pihak.
3. Implikasi Filosofis dan Rasionalitas Hukum di Era DigitalKajian ini menunjukkan bahwa rasionalitas hukum harus menyesuaikan diri dengan perkembangan teknologi digital. Konsep force majeure yang awalnya bersifat umum dalam hukum kontrak tradisional perlu diperluas dan diadaptasi agar relevan dengan risiko digital. Pendekatan filosofis ini menekankan keseimbangan antara perlindungan hukum bagi pihak yang terdampak dan kepastian pelaksanaan kontrak di era digital.

Secara keseluruhan, tanggung jawab hukum atas force majeure dalam kontrak digital aset kripto tetap dapat diatur melalui prinsip hukum kontrak tradisional, tetapi memerlukan penyesuaian kontekstual dan teknologis agar tetap rasional, adil, dan efektif di era digital.

References

1. R. Subekti, Hukum Perjanjian. Jakarta, Indonesia: Intermasa, 2008, p. 15.
2. Republic of Indonesia, Civil Code of Indonesia (Kitab Undang-Undang Hukum Perdata), Art. 1338.
3. D. Tapscott and A. Tapscott, Blockchain Revolution. New York, NY, USA: Penguin Random House, 2018, p. 89.
4. M. Siregar, "Kedudukan Smart Contract dalam Perspektif Hukum Perdata," Jurnal Kertha Semaya, vol. 10, no. 4, pp. 670–680, 2022.

5. N. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," White Paper, 2008.
6. Commodity Futures Trading Regulatory Agency (Bappebti), Regulation No. 8 of 2021 on Guidelines for the Implementation of Crypto Asset Physical Markets. Jakarta, Indonesia, 2021.
7. Zubairi, "Legalitas Aset Kripto di Indonesia," *Jurnal Hukum dan Ekonomi Syariah*, vol. 5, no. 2, pp. 110–120, 2021.
8. R. Subekti, *Pokok-Pokok Hukum Perdata*. Jakarta, Indonesia: Intermasa, 2001, p. 45.
9. P. M. Hadjon, *Pengantar Hukum Perdata*. Surabaya, Indonesia: Yuridika, 2010, p. 97.
10. D. Mulyana, "Force Majeure dalam Perspektif Kontrak Elektronik," *Jurnal Hukum dan Bisnis*, vol. 12, no. 1, pp. 45–60, 2021.
11. R. Reijers et al., "Now the Code Runs Itself," *Science and Engineering Ethics*, vol. 27, no. 2, pp. 1–21, 2021.
12. S. Rahardjo, *Ilmu Hukum*. Bandung, Indonesia: Citra Aditya Bakti, 2006.
13. K. R. Popper, *The Logic of Scientific Discovery*. London, UK: Routledge, 1959.
14. L. L. Fuller, *The Morality of Law*. New Haven, CT, USA: Yale University Press, 1964.
15. L. Lessig, *Code and Other Laws of Cyberspace*. New York, NY, USA: Basic Books, 1999.
16. H. Kelsen, *Pure Theory of Law*. Berkeley, CA, USA: University of California Press, 1967.
17. H. L. A. Hart, *The Concept of Law*. Oxford, UK: Clarendon Press, 1994.
18. Republic of Indonesia, Law No. 11 of 2008 on Electronic Information and Transactions. Jakarta, Indonesia, 2008.
19. S. Soekanto and S. Mamudji, *Normative Legal Research: A Brief Overview*. Jakarta, Indonesia: Rajawali Pers, 2014.
20. P. M. Marzuki, *Legal Research*. Jakarta, Indonesia: Kencana Prenada Media Group, 2019.
21. J. Ibrahim, *Theory and Methodology of Normative Legal Research*. Malang, Indonesia: Bayumedia Publishing, 2006.
22. B. A. Sidharta, *Reflections on the Structure of Legal Science*. Bandung, Indonesia: Mandar Maju, 2009.
23. L. Rasjidi and I. B. W. Putra, *Law as a System*. Bandung, Indonesia: Mandar Maju, 2003.
24. EU Blockchain Observatory and Forum, *Legal and Regulatory Framework of Blockchain and Smart Contracts in the European Union*. Brussels, Belgium, 2020.