BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi digital pada era modern saat ini telah memberikan dampak yang sangat besar terhadap hampir seluruh aspek kehidupan manusia, termasuk dalam bidang hukum yang dituntut untuk beradaptasi dengan berbagai inovasi teknologi. Salah satu bentuk inovasi yang menarik perhatian dalam ranah hukum perdata adalah munculnya *smart contracts* atau kontrak pintar. *Smart contract* yaitu suatu bentuk perjanjian yang dijalankan secara otomatis melalui kode komputer dengan menggunakan teknologi *blockchain* sebagai sistem pencatatannya. Konsep ini pertama kali digagas oleh Nick Szabo pada tahun 1994 sebagai solusi untuk menjamin pelaksanaan kontrak secara otomatis dan aman.[1] Sedangkan *blockchain* adalah sistem pencatatan data yang terdesentralisasi, di mana setiap transaksi disimpan dalam blok yang terhubung secara kronologis dan tidak bisa diubah tanpa persetujuan dari semua pihak yang terlibat. Berbeda dengan basis data tradisional yang terpusat dan bisa dimodifikasi oleh administrator, *blockchain* menawarkan tingkat transparansi dan keamanan yang lebih tinggi. [2]

Keberadaan *smart contracts* dinilai mampu memberikan berbagai manfaat seperti peningkatan efisiensi pelaksanaan kontrak, transparansi dalam setiap transaksi, serta meminimalisasi risiko terjadinya kesalahan manusia (*human error)* dalam proses eksekusi perjanjian. Meskipun demikian, penerapan *smart contracts*

[1] Hesti Ayu Wahyuni, "*Penggunaan Smart Contract pada Transaksi E-Commerce dalam Perspektif Hukum Perdata di Indonesia*", Jurnal Hukum In Certo, Vol. 2 No. 1, 2023, hlm. 3
[2] Joosten, dkk, "*Mengupas Tuntas Teknologi Blockchain: Panduan Memahami Revolusi Di Balik Mata Uang Kripto Modern*", Nusantara Journal of Multidisciplinary Science, Vol. 2 No. 4, 2024, hlm. 898

di Indonesia masih menghadapi sejumlah persoalan yuridis, terutama yang berkaitan dengan keabsahan dan kekuatan mengikatnya dalam perspektif hukum perdata nasional. Hal ini disebabkan karena sistem hukum Indonesia yang berakar pada asas-asas tradisional dalam Kitab Undang-Undang Hukum Perdata (KUHPerdata) belum sepenuhnya mengakomodasi bentuk kontrak yang berbasis teknologi digital.

*Smart contract*s memiliki kemampuan untuk menjalankan berbagai fungsi kompleks dalam dunia bisnis dan keuangan, seperti pengelolaan keuangan terdesentralisasi (DeFi), tokenisasi aset, serta otomatisasi proses hukum dalam perjanjian sewa, asuransi, dan perdagangan internasional.[3] Dengan meningkatnya adopsi teknologi *blockchain* di berbagai sektor, penggunaan *smart contract*s semakin berkembang untuk menggantikan kontrak konvensional yang masih bergantung pada perantara hukum atau lembaga keuangan tradisional.

Keamanan *smart contract*s sangat bergantung pada karakteristik *blockchain* yang bersifat *immutable*, artinya data yang telah dicatat dalam *blockchain* tidak dapat diubah atau dimanipulasi oleh pihak manapun setelah transaksi diverifikasi oleh jaringan.[4] Hal ini membuat *smart contract*s lebih sulit untuk disalahgunakan dibandingkan kontrak digital yang disimpan dalam sistem terpusat, karena tidak ada satu entitas pun yang memiliki kendali penuh atas kontrak tersebut. Namun, karena sifatnya yang tidak dapat diubah, kesalahan dalam kode pemrograman *smart contract*s dapat menimbulkan dampak yang besar.[5]

---

[3] Kasih Maharani, Recu Campus. 2024. "*Apa itu DeFi dan Bagaimana Cara Kerjanya?*", https://reku.id/en/campus/apa-itu-defi-dan-bagaimana-cara-kerjanya , diakses pada tanggal 14 November 2025 pukul 20.00 Wita

[4] Michael Tanley, dkk, "*Analisis Potensi Dan Tantangan Teknologi Blockchain Dalam Mendukung Digitalisasi Ekonomi Di Indonesia*", Indonesian Journal of Education And Computer Science, Vol. 2 No. 3, 2024, hlm. 162

[5] Ibid

Dengan demikian, meskipun *smart contract*s menawarkan tingkat keamanan yang lebih tinggi dibandingkan kontrak konvensional, terdapat tantangan signifikan dalam memastikan kode yang digunakan telah diuji secara menyeluruh sebelum diterapkan dalam transaksi bernilai tinggi. Audit keamanan terhadap *smart contract*s menjadi sangat penting untuk menghindari eksploitasi kode oleh pihak yang tidak bertanggung jawab. Seiring dengan meningkatnya regulasi di berbagai negara, perlu adanya standar keamanan global yang lebih ketat untuk memastikan *smart contract*s dapat digunakan secara aman dan efisien di berbagai sektor industri. Kontrak ini diprogram menggunakan bahasa pemrograman khusus dan dijalankan di atas teknologi *blockchain*, sehingga semua ketentuan yang disepakati akan dilakukan secara otomatis ketika kondisi tertentu terpenuhi. Keamanan *smart contract*s bergantung pada karakteristik *blockchain* yang bersifat *immutable*, artinya data yang telah dicatat dalam *blockchain* tidak dapat diubah atau dimanipulasi.[6]

Dalam konteks *smart contracts*, *blockchain* berperan sebagai infrastruktur utama yang memastikan pelaksanaan otomatis kontrak digital tanpa memerlukan perantara. Beberapa jenis *blockchain* yang sering digunakan untuk *smart contracts* adalah *Ethereum*, *Binance Smart Chain*, dan *Solana*. *Ethereum* menjadi pelopor dalam penerapan *smart contracts* dengan memperkenalkan *Ethereum Virtual Machine* (EVM) dan penggunaan bahasa pemrograman *Solidity*, yang memungkinkan pengembang untuk membuat *smart contract* yang dapat berjalan secara otomatis berdasarkan kode yang telah ditentukan. *Binance Smart Chain* (BSC) menawarkan biaya transaksi yang lebih rendah dibandingkan *Ethereum*,

[6] Joosten, dkk, hlm. 899

sementara *Solana* dikenal dengan kecepatan transaksinya yang tinggi, mencapai hingga 65.000 transaksi per detik (TPS). Dengan berbagai keunggulan ini, *blockchain* telah menjadi fondasi bagi ekosistem keuangan terdesentralisasi (DeFi), *Non-Fungible* Tokens (NFT), serta berbagai aplikasi berbasis Web yang terus berkembang pesat.[7]

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Nomor 11 Tahun 2008, yang telah diubah melalui UU Nomor 1 Tahun 2024, mengatur secara umum transaksi dan informasi elektronik termasuk kontrak elektronik, Namun, regulasi ini belum secara eksplisit mengatur *smart contract* sebagai bentuk lanjutan kontrak elektronik berbasis kode program otomatis di *blockchain* (seperti *Solidity*), yang menimbulkan tantangan pada pelaksanaan otomatis tanpa intervensi manusia.

Ketiadaan regulasi khusus mengenai *smart contract* dapat menghambat inovasi dan investasi di sektor digital, padahal regulasi sejatinya berfungsi sebagai pedoman untuk mengatur masyarakat, termasuk dalam penggunaan teknologi seperti *smart contract*, untuk menjamin kepastian hukum. Jika risiko hukum *smart contract* tidak diimbangi perkembangan kepastian hukum yang eksplisit, kelemahan yuridis akan menjadi celah bagi wanprestasi akibat kelalaian, baik disengaja maupun karena ketidaktahuan para pihak terhadap fondasi sistem *blockchain*, aturan teknis, hingga pengaturan perundang-undangan di Indonesia.

Ketidaan regulasi khusus ini semakin diperumit dengan perbedaan pendekatan hukum di berbagai negara. Misalnya, Uni Eropa cenderung mengadopsi regulasi yang lebih proaktif terkait teknologi *blockchain* dan *smart contracts*, dengan adanya *Markets in Crypto-Assets Regulation* (MiCA) yang bertujuan untuk

[7] Imran Bashir, 2017, "*Mastering Blockhain: Deeper insights into decentralization, cryptography, bitcoin and popular blockchain frameworks*", Packt, Birmingham, hlm. 25

menciptakan ekosistem yang lebih stabil. Sebaliknya, di beberapa negara berkembang, *smart contract*s masih berada dalam area abu-abu hukum, sehingga menyulitkan pihak yang terlibat dalam penyelesaian sengketa lintas negara.[8]

Di samping itu, perkembangan *smart contracts* juga tidak terlepas dari risiko teknis, seperti *bug* dalam kode pemrograman dan serangan siber. Kasus *The DAO Hack* tahun 2016 menjadi contoh nyata bagaimana kelemahan dalam kode *smart contract* dapat dieksploitasi oleh peretas. *The DAO*, atau *Decentralized Autonomous Organization*, adalah sebuah proyek investasi terdesentralisasi yang dibangun di atas *blockchain Ethereum*. *The DAO* bertujuan untuk memberikan cara baru dalam pengelolaan dana investasi dengan memanfaatkan teknologi *smart contracts* untuk menghilangkan perantara tradisional. Dalam waktu singkat, proyek ini berhasil mengumpulkan dana lebih dari USD 150 juta dalam bentuk Ether (ETH), menjadikannya salah satu kampanye penggalangan dana terbesar dalam sejarah blockchain pada saat itu. Namun, celah dalam kode *smart contract* memungkinkan peretas untuk mengeksploitasi fungsi pemisahan dana, sehingga mereka dapat menarik dana berkali-kali sebelum saldo diperbarui. Eksploitasi ini menyebabkan pencurian lebih dari USD 60 juta oleh seorang peretas bernama samaran *Blackhat* dalam bentuk *Ethereum* dari dana yang tersimpan di *The DAO*. Serangan ini memanfaatkan kerentanan yang disebut *reentrancy attack*, di mana kontrak pintar gagal memperbarui saldo pengguna sebelum transaksi selesai diproses, sehingga memungkinkan peretas untuk menarik dana yang sama berulang

[8] Wilda Malika Mulfihah, "*Transformasi Hukum Dagang Internasional Di Era Teknologi Blockchain Dan Cryptocurrency*", Ikraith Ekonomika, Vol. 7 No. 3, 2024, hlm. 386

kali.[9] Serangan ini mengekspos kelemahan mendasar dalam *smart contracts* yang tidak memiliki mekanisme perlindungan terhadap eksekusi ulang fungsi yang tidak diinginkan. Hal ini mengakibatkan kekhawatiran besar dalam komunitas *Ethereum*, karena proyek sebesar *The DAO* tidak memiliki mekanisme pemulihan yang memadai untuk mengembalikan dana kepada investor yang dirugikan.

Pada tahun 2022, terjadi eksploitasi terhadap *Wormhole Bridge*, sebuah jembatan antar-*blockchain* yang memungkinkan transfer aset digital antar jaringan yang berbeda. Serangan ini mengakibatkan kehilangan aset kripto senilai lebih dari USD 320 juta akibat *bug* dalam kode *smart contract* yang mengelola transaksi lintas *blockchain*. Eksploitasi ini terjadi ketika peretas menemukan celah yang memungkinkan mereka mencetak token *Wrapped Ethereum* (wETH) tanpa harus menyetorkan dana asli ke dalam sistem. Setelah berhasil mencetak token palsu, peretas kemudian menukarkannya dengan aset asli di *blockchain* lain, menyebabkan kerugian besar bagi pengguna yang mempercayakan dana mereka pada *Wormhole Bridge*.[10]

Lebih lanjut, dalam konteks Indonesia, penggunaan *smart contract*s juga telah dikaitkan dengan kasus aset kripto yang bermasalah, seperti skandal *Binance* dan FTX yang mengguncang pasar global. FTX, misalnya, mengalami kebangkrutan pada tahun 2022 setelah ditemukan adanya penyalahgunaan dana pelanggan yang disimpan dalam platform berbasis *blockchain*.[11]

---

[9] Zubin Pratap, Chainlink. 2022. "*Reentrancy Attacks and The DAO Hack*", https://blog.chain.link/reentrancy-attacks-and-the-dao-hack/, diakses pada tanggal 12 Desember 2025 pukul 21.36 Wita

[10] Merkle Science. 2022. "*Hack Track: Analysis Of Wormhole Token Bridge Exploit*", https://www.merklescience.com/blog/hack-track-analysis-of-wormhole-token-bridge-exploit , diakses pada tanggal 14 November 2025 pukul 22.11 Wita

[11] CNN Indonesia. 2022. "*Kronologi Kebangkrutan FTX dan Ancaman Penjara untuk Sam Bankman-Fried*", https://www.cnnindonesia.com/ekonomi/20221206151412-92-883548/kronologi-kebangkrutan-ftx-dan-ancaman-penjara-untuk-sam-bankman-fried , diakses pada tanggal 14 November 2025 pukul 22. 25 Wita

Selain itu, baru-baru ini terjadi kasus penipuan investasi kripto di Indonesia, di mana sindikat penipuan daring berhasil mengelabui investor dengan janji keuntungan tinggi dari perdagangan kripto. Skema ini menyebabkan kerugian hingga Rp 105 miliar, dengan enam tersangka yang terlibat, tiga di antaranya telah ditahan sementara lainnya masih buron. Modus yang digunakan adalah dengan menawarkan investasi melalui media sosial dan meminta korban mentransfer dana ke rekening perusahaan fiktif. Menurut laporan dari Badan Reserse Kriminal (Bareskrim) Polri, lebih dari 5.000 investor tersebar di berbagai daerah menjadi korban skema ini, dengan nilai investasi individu bervariasi antara Rp 10 juta hingga Rp 500 juta. Polisi juga menemukan bahwa dana hasil kejahatan ini sebagian besar telah dikonversi menjadi aset kripto seperti Bitcoin dan USDT (*Tether*) sebelum ditransfer ke rekening di luar negeri, terutama di Singapura dan Hong Kong. Investigasi lebih lanjut mengungkap bahwa dana hasil penipuan ini telah dipindahkan ke berbagai akun luar negeri melalui transaksi kripto yang sulit dilacak. Chainalysis, sebuah perusahaan analisis *blockchain*, melaporkan bahwa lebih dari Rp 50 miliar dana korban telah dikonversi menjadi Monero (XMR), sebuah mata uang kripto yang dikenal dengan anonimitasnya, sehingga menyulitkan proses pemulihan dana oleh otoritas penegak hukum.[12]

Keabsahan hukum merujuk pada kondisi sahnya suatu perbuatan hukum atau perjanjian yang telah diformalkan melalui instrumen hukum tertulis, baik berupa peraturan perundang-undangan, peraturan pemerintah, surat edaran, maupun

[12] Intan Rakhmayanti, CNBC Indonesia. 2025. "*Polri Bongkar Modus Penipuan Kripto, Warga RI Rugi Rp 105 Miliar*", https://www.cnbcindonesia.com/tech/20250319160849-37-620039/polri-bongkar-modus-penipuan-kripto-warga-ri-rugi-rp-105-miliar , diakses pada tanggal 14 November 2025 pukul 22.40 Wita

bentuk ketentuan hukum lainnya yang memiliki daya ikat secara normatif.[13] Dalam hukum perdata Indonesia, keabsahan suatu perjanjian ditentukan oleh terpenuhinya syarat-syarat sah perjanjian sebagaimana diatur dalam Pasal 1320 Kitab Undang-Undang Hukum Perdata (KUHPerdata). Pasal ini menetapkan empat unsur pokok, yaitu adanya kesepakatan para pihak, kecakapan para pihak untuk membuat perjanjian, adanya suatu objek tertentu, serta sebab yang halal. Dua syarat pertama merupakan syarat subjektif yang berkaitan dengan subjek hukum yang membuat perjanjian, sedangkan dua syarat terakhir merupakan syarat objektif yang berkaitan dengan substansi perjanjian itu sendiri. Apabila syarat subjektif tidak terpenuhi, maka perjanjian tersebut dapat dibatalkan, sedangkan apabila syarat objektif tidak terpenuhi, perjanjian menjadi batal demi hukum.[14] Dalam konteks perkembangan kontrak digital, ketentuan Pasal 1320 KUHPerdata tetap menjadi tolok ukur utama untuk menilai sah atau tidaknya suatu perjanjian, termasuk *smart contract* yang berbasis teknologi *blockchain* dan dieksekusi secara otomatis.

Berdasarkan uraian tersebut, penelitian ini secara khusus difokuskan untuk mengkaji keabsahan (validitas) *smart contract* ditinjau dari pemenuhan syarat-syarat sahnya perjanjian sebagaimana diatur dalam Pasal 1320 KUHPerdata, mengingat karakteristik *smart contract* yang bersifat otomatis, berbasis kode pemrograman, serta minim intervensi manusia setelah kontrak dijalankan. Oleh karena itu, penulis meyakini perlu untuk melakukan kajian secara mendalam terkait

---

[13] Ni Luh Putu Eka Wijayanti, Garuda Kemdikbud. 2021. "*Keabsahan Sebuah Perjanjian Berdasarkan Dari Kitab Undang Undang Hukum Perdata*", https://download.garuda.kemdikbud.go.id/article.php?article=1333941&val=907&title=KEABSAHAN+SEBUAH+PERJANJIAN+BERDASARKAN+DARI+KITAB+UNDANG+UNDANG+HUKUM+PERDATA, diakses pada tanggal 13 November 2025 pukul 19.28 Wita

[14] Vika Nur Senda, dkk, "*Implikasi Hukum Ketidakterpenuhan Syarat Subjektif Dalam Pasal 1320 Kitab Undang-Undang Hukum Perdata Terhadap Keabsahan Perjanjian*", Letterlijk: Jurnal Hukum Perdata, Vol. 1 No. 2, 2024, hlm. 3

dengan persoalan ini yang dirumuskan dalam judul skripsi **"ANALISIS YURIDIS KEABSAHAN DAN KEKUATAN HUKUM *SMART CONTRACT* DALAM HUKUM PERDATA INDONESIA"**

1.2 Rumusan Masalah

Adapun rumusan masalah dalam penelitian ini adalah:

1. Apakah *Smart Contracts* sah menurut ketentuan Pasal 1320 Kitab Undang-Undang Hukum Perdata (KUHPerdata), serta bagaimana mekanisme *smart contract* dalam sistem *blockchain*?
2. Bagaimana karakteristik *smart contract* serta implikasinya terhadap kepastian hukum dan kekuatan hukum perjanjian dalam hukum perdata Indonesia?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah maka tujuan dari penelitian ini adalah:

1. Untuk mengkaji dan menganalisis keabsahan (validitas) *Smart Contract* ditinjau dari syarat-syarat sahnya perjanjian menurut Pasal 1320 Kitab Undang-Undang Hukum Perdata (KUHPerdata), dan mekanisme *smart contract* dalam sistem *blockchain*.
2. Untuk mengkaji dan menganalisis karakteristik *smart contract* serta implikasinya terhadap kepastian hukum dan kekuatan hukum perjanjian dalam hukum perdata Indonesia.

1.4 Manfaat Penelitian

Manfaat yang dapat diambil dari penelitian ini adalah:

1. Manfaat Teoretis

   Penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan ilmu pengetahuan di bidang hukum perdata, khususnya terkait konsep perjanjian digital modern dalam perspektif hukum perdata Indonesia. Kajian ini memperluas pemahaman teoritis mengenai penerapan asas-asas perjanjian dalam Kitab Undang-Undang Hukum Perdata (KUHPerdata), terutama Pasal 1320 dan Pasal 1338 KUHPerdata, terhadap fenomena hukum baru berupa *smart contracts* yang dijalankan melalui teknologi *blockchain*. Dengan demikian, penelitian ini dapat menjadi referensi ilmiah bagi kalangan akademisi dan peneliti dalam mengembangkan doktrin hukum terkait keabsahan perjanjian berbasis digital dan relevansinya terhadap prinsip kebebasan berkontrak serta aspek kepastian hukum dalam era transformasi digital.

2. Manfaat Praktis

   a. Bagi Pembuat Kebijakan dan Regulator

      Penelitian ini memberikan masukan konstruktif bagi pemerintah dan lembaga regulator, seperti DPR, Kementerian Kominfo, Otoritas Jasa Keuangan (OJK), dan Bank Indonesia, dalam merumuskan regulasi yang lebih komprehensif terkait penggunaan *smart contracts*. Hasil penelitian ini dapat menjadi dasar pertimbangan dalam penyusunan kerangka hukum khusus yang bertujuan untuk memberikan kepastian

hukum, perlindungan konsumen, serta mekanisme penyelesaian sengketa dalam transaksi berbasis *blockchain*.

b. Bagi Praktisi Hukum

Penelitian ini memberikan pemahaman yang lebih mendalam bagi advokat, notaris, arbiter, akademisi, dan konsultan hukum tentang posisi *smart contracts* dalam sistem hukum perdata Indonesia. Dengan adanya kajian ini, praktisi hukum dapat memahami potensi penerapan *smart contracts* dalam transaksi bisnis, risiko yuridis yang mungkin timbul, serta strategi penyelesaian sengketa apabila terjadi pelanggaran atau kegagalan kontrak.

c. Bagi Pelaku Usaha dan Industri Digital

Hasil penelitian ini dapat menjadi pedoman bagi pelaku industri teknologi, *start-up* berbasis *blockchain*, dan perusahaan yang menggunakan transaksi digital untuk memastikan pemanfaatan *smart contracts* dilakukan sesuai prinsip legalitas. Dengan demikian, penelitian ini membantu pelaku usaha dalam mengambil keputusan strategis yang aman dan minim risiko hukum, terutama terkait keamanan transaksi dan keabsahan kontrak digital.

d. Bagi Peneliti Selanjutnya

Penelitian ini dapat menjadi bahan referensi dan rujukan ilmiah bagi mahasiswa dan peneliti yang ingin mengembangkan topik serupa, khususnya dalam kajian hukum perdata modern dan transformasi hukum digital. Hasil penelitian ini juga membuka peluang penelitian lanjutan mengenai harmonisasi regulasi, penyelesaian sengketa digital,

serta pembentukan kebijakan *smart contract* yang lebih terstruktur di Indonesia.