ISSN: 2962-3545
Prosiding SAINTEK: Sains dan Teknologi Vol.5 No.1 Tahun 2026
Call for papers dan Seminar Nasional Sains dan Teknologi Ke-5 2026
Fakultas Teknik, Universitas Pelita Bangsa, Februari 2026

Analisis Risiko Keamanan pada Mekanisme *Lazy Minting* Berbasis EIP-712 di Ekosistem Ethereum

Security Risk Analysis of the EIP-712-Based Lazy Minting Mechanism in the Ethereum Ecosystem

Abdillah AG1, Ike Ardianti[2], Alhadi Saputra[3]
[1,3]Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa
[2]Pendidikan Guru dan Madrasah Ibtidaiyah, Fakultas Tarbiyah dan Ilmu Keguruan, Institut Ummul Quro Al-Islami Bogor
[1]abdillahag@pelitabangsa.ac.id, [2]ike.ardianti@iuqibogor.ac.id*, [3]alhadi.saputra@pelitabangsa.ac.id*

Abstract

In the current development of web3 technology, especially NFTs, lazy minting has become the dominant mechanism used in NFT marketplaces by eliminating gas fees at the beginning of minting through the creation of off-chain signature-based vouchers. Although this approach is considered to lower barriers to entry for users and increase market participation, the mechanism shifts the security assumption from full on-chain validation to a hybrid off-chain–on-chain authorization model. This research was conducted using a Systematic Literature Review (SLR) approach with the PRISMA framework and synthesized 15 selected literature related to lazy minting policies, EIP-712 standard implementation, replay signature vulnerabilities, meta-transactions, and usability risks that occur in wallets. The synthesis results of this study show that, although the EIP-712 standard improves message clarity through structured signing and domain separation, weak implementation in nonce management and domain separation still opens the door to replay attacks. In addition, the lazy minting mechanism also expands the trust boundary by involving relayers and marketplaces, thereby changing the risk landscape compared to traditional minting models. This research integrates economic, cryptographic, and user experience (UX) perspectives to build an integrated risk model for the EIP-712 standard-based lazy minting process in the NFT ecosystem.

***Keywords**: lazy minting, EIP-712, NFT security, replay attack, Ethereum*

Abstrak

Pada perkembangan teknologi web3 terutama NFT saat ini, *Lazy minting* menjadi mekanisme yang dominan digunakan pada marketplace NFT dengan menghilangkan biaya gas di awal minting melalui pembuatan voucher berbasis tanda tangan *off-chain*. Meskipun pendekatan ini dianggap menurunkan hambatan masuk untuk pengguna dan meningkatkan partisipasi pasar, mekanisme tersebut menggeser asumsi arsitektur melinting dari validasi sepenuhnya yang dilakukan secara on-chain menjadi model otorisasi hibrida *off-chain–on-chain*. Penelitian ini dilakukan menggunakan pendekatan *Systematic Literature Review* (SLR) dengan kerangka PRISMA dan mensintesis 15 literatur terpilih terkait kebijakan lazy minting, implementasi standar EIP-712, kerentanan *replay signature, meta-transaction*, serta risiko *usability* yang terjadi pada *wallet*. Hasil sintesis dari penelitian ini menunjukkan bahwa, meskipun standar EIP-712 meningkatkan kejelasan pesan melalui *structured signing* dan *domain separation*, implementasi yang lemah pada pengelolaan *nonce* dan pemisahan domain tetap membuka celah untuk terjadinya *replay attack*. Selain itu, mekanisme *lazy minting* juga memperluas *trust boundary* dengan melibatkan *relayer* dan *marketplace*, sehingga mengubah lanskap risiko dibandingkan model minting tradisional. Penelitian ini mengintegrasikan perspektif ekonomi, kriptografi, dan pengalaman pengguna (UX) untuk membangun model risiko yang terintegrasi pada proses *lazy minting* berbasis standar EIP-712 pada ekosistem NFT.

Kata kunci: *lazy minting*, EIP-712, keamanan NFT, *replay attack, Ethereum*

Pendahuluan

Perkembangan *web3* dan pertumbuhan dan ekosistem *Non-Fungible Token* (NFT) telah mendorong terjadinya inovasi terutama pada mekanisme *minting* untuk menurunkan hambatan partisipasi pengguna yang terjadi karena proses minting yang mengharuskan pembayaran biaya gas transaksi di awal.. Salah satu mekanisme yang berkembang pesat saat ini adalah *lazy minting*, yakni pendekatan di mana sebuah aset NFT tidak langsung dicetak secara *on-chain*, melainkan direpresentasikan melalui voucher bertanda tangan yang dilakukan secara *off-chain* dan hanya diredeem saat transaksi pembelian terjadi. Studi empiris menunjukkan bahwa kebijakan *lazy minting* tersebut secara signifikan meningkatkan partisipasi pasar dan market thickness karena telah menghilangkan biaya gas transaksi di awal saat aset NFT dibuat [1], [2].

Meskipun cara ini efektif secara ekonomi, namun penghilangan biaya minting di awal proses, turut menggeser arsitektur keamanan sistem yang awalnya minting dilakukan sepenuhnya *on-chain* sehingga validasi sepenuhnya bergantung pada mekanisme *blockchain* (model tradisional). Sebaliknya, proses *lazy minting* bergantung pada *structured* data *signing*, yang umumnya menggunakan standar EIP-712 untuk menghasilkan otorisasi yang ditandatangani oleh kreator sebelum dicatat ke dalam *blockchain* pada saat pembelian terjadi.

Standar EIP-712 dirancang untuk mengatasi ambiguitas ***message signing*** melalui ***typed structured* data** dan ***domain separation***. Namun, sejumlah penelitian lain menunjukkan bahwa, penggunaan *off-chain message signing* tetap rentan terhadap *signature replay vulnerabilities* dan kesalahan implementasi [3], [4]. Pada Penelitian lebih lanjut menunjukkan bahwa pengelolaan *nonce* dan pemisahan domain yang tidak tepat dapat menyebabkan *reuse signature* lintas konteks [7], [9].

Selain aspek kriptografi, faktor lain seperti *usability* juga memainkan peran yang sangat penting. Studi mengenai *wallet cryptocurrency* menemukan bahwa pengguna sering kali tidak memahami struktur data yang ditandatangani, termasuk dalam skema EIP-712 [5], [6]. Kerentanan akibat penyalahgunaan tanda tangan juga telah menyebabkan kerugian ekonomi yang signifikan dalam ekosistem Ethereum [10], menunjukkan bahwa masalah signature misuse bukan sekadar isu teoretis.

Di sisi lain, implementasi *lazy minting* juga sering kali melibatkan relayer atau model *meta-transaction* yang digunakan untuk memproses *voucher* dan membayar biaya gas transaksi. Studi mengenai arsitektur *meta-transaction* dan *threshold signature* menunjukkan bahwa komponen *off-chain* telah memperluas *trust boundary* serta berpotensi menciptakan titik kegagalan baru [11], [12]. Konsep *verifiable off-chain computation* bahkan telah diusulkan untuk menjaga integritas proses yang dieksekusi di luar blockchain [13]. Pendekatan gas *abstraction* seperti Gas *Station Network (*GSN) juga menunjukkan bahwa adanya pergeseran tanggung jawab biaya transaksi dari pengguna ke *relayer* [14], dan implementasi *gasless* NFT pada aplikasi tertentu menunjukkan peningkatan pengalaman pengguna [15].

Meskipun beberapa literatur telah membahas dampak ekonomi *lazy minting*, kerentanan *replay signature*, serta risiko *usability* secara terpisah, namun belum terdapat kajian yang menganalisis terkait integrasi mekanisme *lazy minting* berbasis EIP-712 dalam perspektif keamanan, model kepercayaan, dan pengalaman pengguna. Dengan begitu, penelitian ini bertujuan untuk mengisi kesenjangan tersebut melalui pendekatan *Systematic Literature Review* berbasis PRISMA.

Metode Penelitian

Penelitian ini dilakukan dengan menggunakan pendekatan *Systematic Literature Review* (SLR) untuk mengkaji mekanisme *lazy minting* berbasis EIP-712 dalam ekosistem Ethereum secara dalam serta implikasinya terhadap keamanan, model kepercayaan, dan pengalaman pengguna pada ekosistem Ethereum. Pendekatan SLR dipilih karena memungkinkan untuk menganalisis literatur secara sistematis dan terstruktur pada berbagai penelitian yang telah dipublikasikan sebelumnya. *Proses review* dilakukan dengan mengacu pada

kerangka PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*) guna untuk memastikan transparansi, konsistensi, serta replikasi dalam proses seleksi literatur.

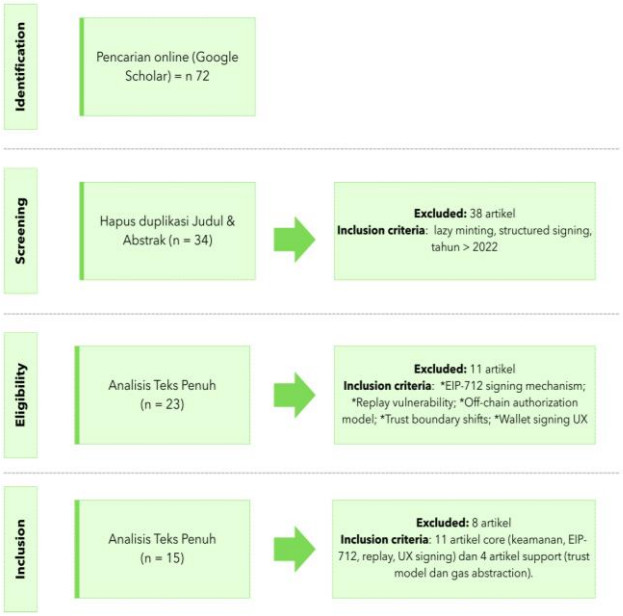
Proses pencarian literatur pada penelitian ini dilakukan melalui platform *Google Scholar* untuk menemukan berbagai sumber publikasi ilmiah yang relevan dengan bidang blockchain itu sendiri dan keamanan sistem terdistribusi. Pencarian dilakukan dengan menggunakan kombinasi kata kunci yang berkaitan dengan topik penelitian yang dimaksud, seperti *"lazy minting AND NFT"*, *"EIP-712 AND Ethereum"*, *"off-chain signing AND Ethereum"*, serta *"meta-transaction AND Ethereum"*. Fokus utama pencarian diarahkan pada publikasi artikel ilmiah yang diterbitkan selama rentang waktu 2022–2026 guna untuk memastikan bahwa literatur yang dianalisis mencerminkan perkembangan terbaru terkait ekosistem NFT dan teknologi Ethereum. Melalui proses identifikasi awal ini, sehingga diperoleh 72 artikel ilmiah yang diharapkan berpotensi serta relevan dengan topik penelitian.

Selanjutnya dilakukan proses penyaringan berdasarkan kriteria inklusi dan eksklusi yang telah ditentukan. Artikel yang berpotensi dimasukkan kedalam kajian adalah apabila membahas mekanisme lazy minting atau model voucher berbasis signature, mengkaji implementasi maupun analisis keamanan EIP-712 dan structured data signing, menganalisis risiko *replay attack*, *misuse signature*, atau *domain separation*, serta membahas implikasi penggunaan *off-chain* signing terhadap model kepercayaan maupun pengalaman pengguna. Sebaliknya, artikel akan dieliminasi apabila hanya membahas blockchain secara umum tanpa relevansi terhadap mekanisme signing, berfokus pada *post-quantum cryptography* tanpa kaitan dengan EIP-712, membahas pemodelan risiko DeFi yang tidak melibatkan structured signing, atau tidak mengkaji mekanisme *off-chain authorization*.

Proses seleksi literatur dilakukan melalui beberapa tahap sesuai dengan kerangka PRISMA. Pada tahap awal atau identification, diperoleh sebanyak 72 artikel dari hasil pencarian pada Google Scholar. Kemudian masuk pada tahap berikutnya yakni proses *screening*, dimana proses penyaringan dilakukan berdasarkan judul dan abstrak dari artikel yang ditemukan untuk mengeliminasi artikel yang tidak relevan dengan mekanisme *lazy minting* atau *structured signing*. Pada tahap ini sebanyak 38 artikel dieliminasi, sehingga tersisa 34 artikel untuk kemudian dianalisis lebih lanjut.

Tahap berikutnya adalah *eligibility*, di mana ke-34 artikel yang telah di screening tersebut dianalisis secara menyeluruh melalui pembacaan teks lengkap untuk memastikan kesesuaian metodologis serta relevansi langsung dengan topik penelitian yang dilakukan, khususnya terkait standar EIP-712 signing mechanism, kerentanan *signature replay*, model *off-chain authorization*, pergeseran *trust boundary*, serta *aspek wallet signing usability*. Dari proses evaluasi pada tahap ketiga ini, sebanyak 11 artikel dieliminasi karena tidak membahas lebih spesifik mengenai EIP-712, dan tidak mengkaji mekanisme otorisasi berbasis *signature*, atau terlalu jauh dari konteks NFT dan *lazy minting*.

Selanjutnya masuk pada tahapan terakhir yakni *inclusion*, di mana dari 23 artikel yang tersisa, dilakukan seleksi akhir berdasarkan kesesuaian terhadap tujuan penelitian dan kedalaman analisis terhadap mekanisme *lazy minting* berbasis standar EIP-712. Dari proses tersebut diperoleh 15 artikel yang dipertahankan sebagai korpus utama dalam studi SLR ini. Artikel-artikel tersebut terdiri dari 11 artikel inti yang secara langsung membahas mengenai aspek keamanan, implementasi standar EIP-712, kerentanan replay, serta *usability* pada proses *signing user*, dan 4 artikel pendukung lainnya yang memberikan konteks tambahan terkait model kepercayaan dan mekanisme gas abstraction dalam ekosistem Ethereum.



Gambar 1. Diagram Alur Metode Prisma

Analisis terhadap literatur terpilih dilakukan menggunakan pendekatan *thematic synthesis*. Melalui pendekatan ini, artikel-artikel yang dianalisis diklasifikasikan ke dalam beberapa tema utama yang merepresentasikan aspek penting dari mekanisme *lazy minting* berbasis **EIP-712**. Tema pertama berkaitan dengan mekanisme lazy minting dan gas abstraction, yang menjelaskan bagaimana model voucher dan meta-transaction digunakan untuk menghilangkan biaya minting awal. Tema kedua berkaitan dengan kerentanan structured signing dan replay risk, yang mengkaji potensi penyalahgunaan signature akibat implementasi EIP-712 yang tidak tepat. Tema ketiga berkaitan dengan model kepercayaan dan implikasinya terhadap pengguna, yang membahas pergeseran trust boundary akibat integrasi komponen off-chain seperti marketplace dan relayer.

Melalui sintesis tematik ini, penelitian dapat mengidentifikasi hubungan antara penerapan EIP-712 dalam mekanisme *lazy minting* dengan potensi risiko keamanan serta perubahan model kepercayaan dalam ekosistem NFT.

Hasil dan Pembahasan

Berdasarkan sintesis terhadap 15 artikel yang telah dipilih melalui proses *Systematic Literature Review,* temuan literatur yang diperoleh dapat diklasifikasikan ke dalam tiga tema utama yang saling berkaitan, yaitu 1) mekanisme lazy minting dan pergeseran biaya transaksi; 2) kerentanan structured signing berbasis EIP-712; serta 3) implikasi terhadap model kepercayaan dan pengalaman pengguna dalam ekosistem NFT.

Mekanisme *Lazy Minting* dan Pergeseran Biaya Transaksi:

Banyak studi menunjukkan bahwa kebijakan *lazy minting* secara signifikan telah meningkatkan partisipasi pengguna dan volume transaksi NFT karena telah menghilangkan kebutuhan pembayaran biaya gas pada tahap awal aset NFT di-minting [1], [2]. Pada model minting tradisional, gas *fee* atau biaya transaksi minting sebuah aset berfungsi sebagai semacam filter kualitas (*quality signal*) yang membatasi jumlah aset yang akan dicetak karena kreator harus mengeluarkan biaya sejak awal. Namun sebaliknya, pada mekanisme *lazy minting* hambatan biaya yang dimaksud tersebut dihilangkan, sehingga entry barrier menjadi lebih rendah. Hal ini memungkinkan lebih banyak kreator yang tertarik berpartisipasi pada *marketplace* NFT.

Meskipun demikian, penghilangan biaya gas pada tahap awal sebuah aset dicetak tidak hanya berdampak pada dinamika ekonomi pasar NFT saja, tetapi juga mengubah arsitektur teknis bagaimana sebuah aset NFT

dicetak (*minting*). Dalam mekanisme lazy minting, kreator tidak langsung mencetak NFT secara *on-chain* pada jaringan blockchain tertentu, namun sebagai gantinya, mereka menghasilkan *voucher* yang ditandatangani secara kriptografis melalui proses *signing* yang dilakukan secara *off-chain*. Voucher yang dihasilkan tersebut kemudian digunakan sebagai bukti otorisasi yang akan ditukar (*redeem*) pada smart-contract marketplace ketika transaksi pembelian terjadi. Proses ini secara implisit sangat bergantung pada mekanisme *structured data signing* seperti yang didefinisikan dalam standar EIP-712.

Dengan demikian, efisiensi biaya yang diperoleh melalui mekanisme lazy minting ternyata berbanding lurus dengan meningkatnya ketergantungan terhadap keamanan sistem signature yang digunakan dalam proses otorisasi transaksi tersebut.

Kerentanan *Structured Signing* dan *Replay Risk*:

Beberapa Literatur menunjukkan bahwa penggunaan *off-chain message signing* dalam ekosistem Ethereum sangat luas dan rentan terhadap berbagai bentuk penyalahgunaan [4]. *Signature replay vulnerability* (SRV) teridentifikasi pada persentase signifikan *smart contract Ethereum* [3], yang menunjukkan bahwa reuse signature menjadi ancaman nyata.

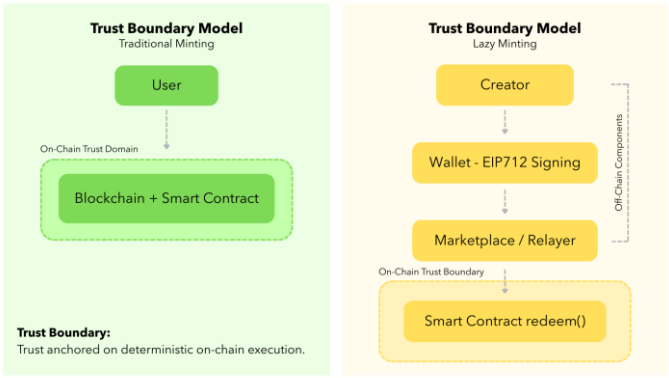
Standar EIP-712 dirancang untuk mengatasi ambiguitas *message signing* dengan *domain separation dan typed structured* data. Namun, beberapa studi lain menunjukkan bahwa kesalahan implementasi, seperti domain separator yang tidak unik atau pengelolaan nonce yang lemah, dapat membuka celah serangan *replay attack* [7].

Dalam konteks penggunaan *lazy minting*, *voucher* yang ditandatangani secara *off-chain* memiliki kemungkinan menjadi celah *replay* lintas konteks atau platform apabila *nonce* tidak dikelola dengan sangat ketat, *expiry time* yang tidak ditetapkan, serta *domain separation* yang tidak spesifik pada *contract* dan chain ID tertentu. Dengan demikian, keamanan terkait **lazy minting** bukan hanya bergantung pada kriptografi ECDSA, tetapi juga pada disiplin implementasi standar EIP-712 yang ketat.

Implikasi terhadap Model Kepercayaan:

Beberapa penelitian menunjukkan bahwa penggunaan meta-transaction dan relayer memperkenalkan pergeseran model kepercayaan [11], [14]. Dalam arsitektur gasless atau *lazy minting*, relayer atau *marketplace* sering kali berperan dalam memproses *voucher* dan membayar gas.

Hal ini menggeser *trust boundary* dari sistem sepenuhnya on-chain menjadi kombinasi *off-chain–on-chain*. Studi mengenai *threshold signature* dan *verifiable off-chain computation* menunjukkan bahwa arsitektur *off-chain* yang tidak terverifikasi dapat meningkatkan risiko single *point of failure* [12], [13]. Dengan demikian, *lazy minting* memperkenalkan model *trust hybrid* yang harus dianalisis secara eksplisit.

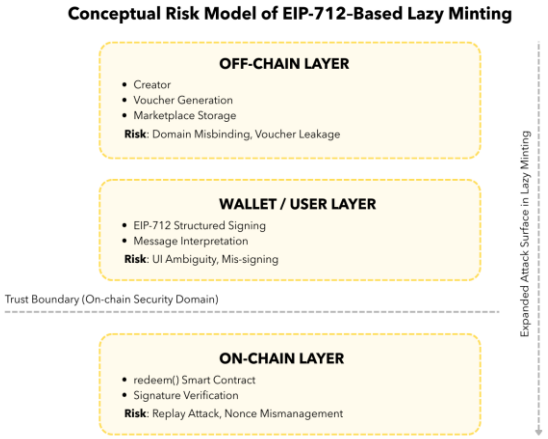


Gambar 2. Model Pergeseran *Trust Boundary*

Dampak terhadap Pengalaman Pengguna:

Penelitian sebelumnya menunjukkan bahwa pengguna seringkali tidak sepenuhnya memahami pesan yang ditandatangani dalam *structured signing* [6]. Bahkan pada *wallet* populer, sering ditemukan berbagai vektor serangan berbasis ambiguitas antarmuka pengguna [5].

Dalam konteks *lazy minting*, pengguna mungkin menandatangani *voucher* atau otorisasi tanpa memahami implikasi pada ekonominya secara penuh. Risiko ini paralel dengan fenomena misuse pada token *approval scam* yang menyebabkan kerugian besar secara finansial [10]. Dengan demikian, pengurangan gas *fee* tidak selalu berarti merupakan peningkatan keamanan atau transparansi bagi pengguna akhir.



Gambar 3 Model Risiko Konseptual Lazy Minting

Research Gap

Meskipun telah terdapat berbagai penelitian sebelumnya yang telah membahas mengenai aspek tertentu dari mekanisme lazy minting dan teknologi pendukungnya, namun kajian yang dilakukan umumnya masih terfragmentasi pada domain yang berbeda. Beberapa studi tersebut berfokus pada dampak ekonomi dari kebijakan lazy minting terhadap dinamika pasar NFT dan partisipasi kreator [1], [2]. Penelitian lain juga mengkaji kerentanan replay pada smart contract Ethereum serta potensi penyalahgunaan signature dalam transaksi berbasis kriptografi [3].

Selain itu, terdapat pula studi yang membahas mengenai berbagai bentuk vulnerabilitas pada mekanisme off-chain message signing dalam sistem terdesentralisasi [4], serta penelitian mengenai implementasi dan strategi mitigasi keamanan pada standar structured signing EIP-712 [7]. Di sisi lain, sejumlah penelitian juga menyoroti aspek seperti pengalaman pengguna, khususnya terkait risiko ambiguitas dalam proses wallet signing yang dapat memicu kesalahan interpretasi atau penyalahgunaan otorisasi oleh pengguna [5], [6].

Berdasarkan kesenjangan tersebut, penelitian ini bertujuan untuk mengintegrasikan berbagai perspektif yang sebelumnya terpisah dalam literatur, yaitu 1) perspektif ekonomi NFT; 2) keamanan kriptografi pada structured signing; serta 3) faktor pengalaman pengguna pada proses wallet signing. Melalui pendekatan *Systematic Literature Review*. Penelitian ini juga mensintesis literatur lintas domain untuk memberikan analisis terintegrasi mengenai risiko keamanan dan implikasi sistemik yang kemungkinan terjadi dari mekanisme lazy minting berbasis EIP-712 dalam ekosistem Ethereum.

Design Recommendations

Dengan didasarkan pada sintesis dari 15 literatur yang terpilih, beberapa rekomendasi desain dapat dirumuskan untuk meningkatkan keamanan dan keandalan mekanisme lazy minting berbasis EIP-712 tersebut. Berikut adalah beberapa rekomendasi yang dimaksud:

Strict Domain Isolation: Implementasi standar EIP-712 harus mempertimbangkan domain separator yang secara eksplisit mengikat seperti *contract address*, chain ID, *contract name* dan version, serta *marketplace context*. *Domain* binding yang lemah

dapat berpotensi memungkinkan *reuse signature* lintas kontrak atau lintas jaringan.

Time-Bound dan Nonce-Based Signature: Pada voucher lazy mint sebaiknya menyertakan parameter expiry time (timestamp) untuk memberi batasan waktu, menggunakan nonce unik per kreator serta mengimplementasikan nonce invalidation setelah redeem atau setelah sebuah aset terjual. Pendekatan ini secara signifikan dapat mengurangi risiko *replay attack* lintas konteks atau *reuse signature* di waktu yang berbeda.

Explicit Replay Protection Logic: Fungsi redeem pada smart contract harus dapat memverifikasi bahwa sebuah voucher atau signature belum pernah digunakan sebelumnya, menyimpan *hash voucher* sebagai consumed sera menghindari reliance pada ecrecover tanpa state check tambahan. Selain itu, *Replay* mitigation tidak boleh hanya bergantung pada keabsahan kriptografis, tetapi juga pada kontrol status.

Wallet Interpretability Enhancement: Marketplace NFT disarankan untuk, menampilkan ringkasan *human-readable pada structured signing*, memberikan *preview* risiko dan informasi yang jelas (misalnya: "*Authorize mint voucher for tokenId X")* dan menghindari JSON ambigu tanpa konteks. Studi terkait pengalaman pengguna menunjukkan bahwa interpretabilitas pesan secara langsung dapat mempengaruhi kemampuan pengguna mendeteksi risiko.

Trust Boundary Minimization: Jika menggunakan relayer atau model meta-transaction disarankan untuk mempertimbangkan *threshold signature*. Gunakan *enclave-based relayer* untuk melindungi *key custody* dan dokumentasikan secara transparan terkait komponen *off-chain*. *Lazy minting* adalah *hybrid trust* model, sehingga desain yang dirancang harus benar-benar meminimalkan *single point of failure*.

Comparative Insight

Untuk memperjelas perbedaan arsitektur dan implikasi keamanan dari proses *lazy minting* dan *minting* tradisional, tabel berikut menyajikan perbandingan antara kedua model minting yang dimaksud.

Tabel 1. Perbandingan Minting Tradisional dan Lazy Minting

Aspek	Traditional Minting	Lazy Minting (EIP-712-based
Waktu Minting	Sebelum listing	Saat pembelian terjadi
Biaya Gas Awal	Dibayar kreator	Tidak ada
Otorisasi	On-chain transaction	Off-chain signed voucher
Ketergantungan Signature	Rendah	Tinggi
Risiko Replay	Rendah (nonce tx native)	Tinggi jika domain/nonce lemah
Model Trust	Fully on-chain	Hybrid (off-chain + on-chain)
UX Barrier	Tinggi (gas upfront)	Rendah
Permukaan Serangan	Smart Contract saja	Smart Contract+ Wallet + Relayer
Replay Protection	Native tx nonce	Harus diimplementasikan eksplisit
Domain Separation	Implisit	Bergantung implementasi EIP-712

Model tradisional minting memiliki biaya gas awal lebih tinggi dari *lazy minting,* tetapi kemungkinan terjadinya serangan sangat terbatas dikarenakan seluruh validasi dilakukan pada lapisan jaringan blockchain. Sementara*, lazy minting* yang diterapkan untuk meningkatkan efisiensi ekonomi dan aksesibilitas, sebaliknya memperluas kemungkinan *attack surface* melalui *voucher signing*, *relayer*, dan *wallet interpretability*.

Dengan demikian*, lazy minting* berbasis EIP-712 menghadirkan *trade-off* sistemik antara efisiensi ekonomi dan kompleksitas keamanan.

Kontribusi Penelitian

Penelitian ini diharapkan dapat memberikan beberapa kontribusi utama terhadap kajian keamanan NFT dan mekanisme lazy minting berbasis EIP-712, meliputi:

Kontribusi Konseptual: Penelitian ini diharapkan dapat mengintegrasikan perspektif ekonomi NFT, keamanan kriptografi *structured signing*, serta faktor *usability wallet* ke dalam satu kerangka analisis terpadu. Pada Literatur sebelumnya yang ditemukan, telah membahas terkait aspek-aspek tersebut namun secara terpisah dan belum mengintegrasikan secara khusus dalam konteks *lazy minting* berbasis *voucher*.

Kontribusi Sintesis Keamanan: Studi ini juga mengidentifikasi bahwa risiko pada lazy minting tidak hanya berasal dari *signature replay*, tetapi juga dari beberapa hal lain seperti kegagalan domain separation, manajemen *nonce* yang lemah, serta ambiguitas interpretasi *structured signing* oleh pengguna.

Kontribusi Model Kepercayaan: Penelitian ini juga menunjukkan bahwa *lazy minting* dapat memperluas *trust boundary* melalui keterlibatan relayer dan *marketplace*, sehingga menghadirkan model kepercayaan hibrida yang berbeda dari minting tradisional berbasis *on-chain*.

Kontribusi Praktis: Studi ini merumuskan rekomendasi implementasi seperti penggunaan *time-bound signature*, *strict domain isolation*, serta peningkatan interpretabilitas pesan pada *wallet* untuk meminimalkan risiko penyalahgunaan *signature* dalam *marketplace* NFT.

Keterbatasan Penelitian

Meskipun penelitian ini memberikan sintesis yang komprehensif, namun penelitian ini juga memiliki beberapa keterbatasan diantaranya adalah: 1) Penelitian ini dilakukan menggunakan pendekatan *Systematic Literature Review* tanpa melakukan eksperimen langsung pada smart contract terkait mekanisme lazy minting di lingkungan produksi; 2) Analisis risiko *replay* dan *misuse signature* didasarkan pada *literatur* yang tersedia dan tidak mencakup pengujian exploit terhadap marketplace NFT tertentu; 3) Studi ini berfokus pada *literatur* yang tersedia di *Google Scholar* dalam rentang waktu tertentu, sehingga kemungkinan masih terdapat banyak publikasi non-terindeks atau whitepaper teknis yang tidak tercakup; 4) Penelitian ini tidak melakukan evaluasi kuantitatif terhadap tingkat kerugian ekonomi yang secara khusus disebabkan oleh replay pada mekanisme lazy minting NFT.

Keterbatasan ini membuka peluang bagi penelitian lanjutan yang melibatkan analisis eksperimen kontrak pintar, studi kasus marketplace spesifik, atau pengembangan model formal verifikasi EIP-712 pada sistem lazy minting.

Kesimpulan

Penelitian ini bertujuan untuk menganalisis mekanisme lazy minting berbasis EIP-712 dalam ekosistem Ethereum melalui pendekatan *Systematic Literature Review* (SLR) berbasis PRISMA dengan 15 literatur terpilih dari Google Scholar. Hasil sintesis dari penelitian ini menunjukkan bahwa lazy minting mampu menurunkan hambatan biaya minting aset NFT diawal dan meningkatkan partisipasi dalam pasar NFT. Namun demikian, mekanisme ini juga secara fundamental menggeser arsitektur minting yang sebelumnya dari model sepenuhnya on-chain menuju model hibrida yang mengandalkan otorisasi berbasis tanda tangan o*ff-chain*.

Dalam mekanisme tersebut, standar EIP-712 berperan sangat penting dalam menyediakan *structured* data signing dan domain separation untuk meningkatkan kejelasan pesan serta validitas *signature*. Meskipun demikian, berbagai penelitian menunjukkan bahwa kelemahan dalam pengelolaan nonce, domain separation, dan validitas signature masih berpotensi menimbulkan replay attack dan penyalahgunaan signature.

Selain itu, keterlibatan *relayer* dan *marketplace* dalam mekanisme *meta-transaction* memperluas *trust boundary* sistem dibandingkan model minting tradisional. Dari perspektif pengguna, pengurangan biaya gas transaksi

minting tidak selalu diikuti dengan peningkatan keamanan, karena ambiguitas antarmuka wallet dan keterbatasan pemahaman pengguna terhadap *structured signing* masih membuka peluang untuk memicu kesalahan otorisasi pengguna.

Secara keseluruhan, teknik lazy minting berbasis EIP-712 menghadirkan *trade-off* antara efisiensi biaya dan peningkatan kompleksitas keamanan. Oleh karena itu, implementasi mekanisme ini perlu disertai dengan domain *isolation* yang ketat, pengelolaan nonce yang terstruktur dan konsisten, serta peningkatan interpretabilitas pesan pada *wallet* untuk menjaga keamanan dan kepercayaan dalam ekosistem NFT.

Daftar Rujukan

[1] H. Zhang, C. Gu, and J. Liu, "Chasing Market Growth and Matching Performance in Two-Sided Platforms: Evidence from the Lazy-Minting Policy in an NFT Marketplace," 2022, doi: https://dx.doi.org/10.2139/ssrn.4279215 .

[2] M. Fang, Y. Li, and X. Zhou, "The Impact of Lazy Minting on Seller Performance in NFT Marketplaces: A Transaction Cost Economics Perspective," 2024, doi: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4794907 .

[3] Z. Wang, T. Kim, and X. Zhang, "One Signature, Multiple Payments: Demystifying and Detecting Signature Replay Vulnerabilities in Smart Contracts," in Proc. ICSE, 2026, doi: https://doi.org/10.48550/arXiv.2511.09134 .

[4] S. Meisami, M. Hu, and G. Wang, "SigScope: Detecting and Understanding Off-Chain Message Signing-Related Vulnerabilities in Decentralized Applications," 2025, doi: https://doi.org/10.1145/3696410.3714686 .

[5] X. Hu, Y. Zhou, and F. Long, "WalletProbe: A Testing Framework for Browser-Based Cryptocurrency Wallet Extensions," 2025, doi: https://doi.org/10.48550/arXiv.2504.11735 .

[6] Y. Qin and H. Duan, "What I Sign Is Not What I See: Towards Explainable and Trustworthy Cryptocurrency Wallet Signatures," 2026, doi: https://doi.org/10.48550/arXiv.2601.16751 .

[7] T. H. Romel et al., "A Patient-Centric Blockchain Framework for Secure Electronic Health Record Management: Decoupling Data Storage from Access Control," 2025, doi: https://doi.org/10.48550/arXiv.2511.17464 .

[8] A. Ghosh, M. Rahman, and S. Kim, "Design and Implementation of a Decentralized Token Exchange Platform with EIP-712 Support," 2022.

[9] R. Li et al., "On Tokenizing Securities in Contemporary Decentralized Finance Ecosystems," 2024, doi: https://doi.org/10.1109/BRAINS63024.2024.10732268 .

[10] T. Kim, "An Empirical Study of Token Approval Scams and Signature Misuse in Ethereum," 2024.

[11] E. Onica and C. Amariei, "Using SGX for Meta-Transactions Support in Ethereum DApps," 2022, doi: https://doi.org/10.48550/arXiv.2204.09864 .

[12] A. Bigiotti, L. Mostarda, A. Navarra, P. Shah, and R. Trestian, "Threshold Signature in Off-Chain Components to Manage Inter-Chain Transactions," 2024, doi: https://doi.org/10.1109/BRAINS63024.2024.10732513 .

[13] R. Hartnell and E. Battaglia, "Verifiable Off-Chain Governance for Decentralized Systems," 2024, doi: https://doi.org/10.48550/arXiv.2512.23618 .

[14] M. Naveed Shariff and K. Nachiar, "GSN as a Service: Evaluating Gas Abstraction in Ethereum-Based Systems," 2023.

[15] F. Darmawan and Bakhtiar, "Pembangunan Game Lost Chain Menggunakan Blockchain dan Gasless Transaction," 2023, doi: https://doi.org/10.51211/isbi.v8i1.2459 .