NISKVORA

Kelangkaan oleh Kode. Privasi atas Pilihan.

Ledger Zero-Knowledge Dua State untuk Nilai Konfidensial dan Pengungkapan Selektif

Aset Protokol · NKVR

Whitepaper Protokol · Versi 1.0

DAFTAR ISI

Pemberitahuan Hukum dan Yurisdiksi yang Penting

Abstrak

1.0 Ringkasan Eksekutif: Kelangkaan Tanpa Pengintaian

2.0 Katalis Pasar: Privasi dalam Ekonomi yang Dapat Dibaca AI

3.0 Silsilah Moneter: Disiplin Bitcoin, Dibangun Ulang untuk Era Otonom

4.0 Arsitektur Protokol: Tumpukan Dua-State Modular Hibrida

5.0 Ledger Dua-State dan Mesin Kriptografis

6.0 Pengungkapan Selektif: Lapisan Kepatuhan yang Dapat Diaudit

7.0 Witness Network: Delegasi yang Mudah Diakses dan Penguncian Pasokan

8.0 Horizon Ekspansi: Niskvora Verify dan Agent Shield

9.0 Ekonomi Token NKVR: Kelangkaan yang Direkayasa dan Deflasi Dua Tahap

10.0 Tata Kelola Dua Lapis dan Kepengurusan Institusional

11.0 Akses Pasar Genesis, Integritas Pasar, dan Peta Jalan

12.0 Pengungkapan Risiko dan Sikap Regulasi

Lampiran A — Glosarium Formal dan Notasi State Protokol

Lampiran B — Penerbitan Moneter, Era Halving, dan Persamaan Pasokan

Lampiran C — Model Ancaman Kriptografis dan Ringkasan Batas Keamanan

Pemberitahuan Hukum dan Yurisdiksi yang Penting

NKVR adalah aset kripto penyimpan nilai dan agunan (kolateral) validasi jaringan dari protokol Niskvora. NKVR bukan alat pembayaran yang sah, bukan pengganti mata uang negara mana pun, bukan stablecoin, dan tidak dirancang atau dipasarkan sebagai instrumen untuk pembayaran ritel harian. Tidak ada bagian dalam dokumen ini yang merupakan penawaran untuk menjual, ajakan atas penawaran untuk membeli, atau rekomendasi mengenai efek, instrumen keuangan, atau skema investasi kolektif mana pun di yurisdiksi mana pun.

Tidak ada pernyataan dalam whitepaper ini yang boleh dibaca sebagai janji keuntungan, jaminan imbal hasil, batas bawah harga, atau jaminan likuiditas. Parameter protokol yang dijelaskan di sini mencerminkan niat desain pada tanggal publikasi dan hanya dapat diubah melalui proses tata kelola yang diatur dalam Bagian 10.0, dengan tunduk pada batasan konstitusional yang diuraikan di sana.

Distribusi dokumen ini dan ketersediaan NKVR dapat dibatasi atau dilarang di yurisdiksi tertentu. Pihak yang mengakses dokumen ini bertanggung jawab untuk memahami dan mematuhi semua pembatasan yang berlaku. Partisipasi dalam distribusi genesis mana pun diatur secara eksklusif oleh dokumentasi hukum terpisah yang diterbitkan oleh The Niskvora Foundation; apabila dokumentasi tersebut bertentangan dengan whitepaper ini, dokumentasi terpisah itulah yang berlaku.

Tidak ada bagian dalam whitepaper ini yang boleh dipahami sebagai nasihat hukum, pajak, akuntansi, atau investasi.

Abstrak

Niskvora adalah ledger zero-knowledge dua state yang aset protokolnya, NKVR, membawa batas maksimum 21.000.000 unit yang ditegakkan oleh bytecode alih-alih oleh kebijakan — dapat diverifikasi publik secara default dan dapat dipindahkan ke vault terlindung zero-knowledge sesuai keputusan pemegang. Saldo terlindung tetap tunduk pada gerbang konservasi pasokan yang mempublikasikan ukuran agregat pool terenkripsi, sehingga plafon tetap berlaku di kedua state dan tidak ada jalur untuk mencetak terhadap cadangan yang tidak diungkapkan. Pengungkapan ditangani melalui viewing key baca-saja yang berlingkup dan atestasi zero-knowledge yang memungkinkan pemegang membuktikan fakta tertentu — solvabilitas, sumber dana, tidak adanya kontak dengan kumpulan alamat yang dikenai sanksi — kepada pihak lawan tertentu untuk periode tertentu, tanpa memberikan wewenang pengeluaran atau mengekspos ledger yang mendasarinya. Jadwal moneter mengikuti disiplin halving

Bitcoin pada irama era dua belas bulan, dengan 40% pasokan dialokasikan kepada Witness Network yang memungkinkan delegasi stake tanpa perangkat keras khusus. Dua lini pendapatan eksternal — atestasi perusahaan dan vault berizin bagi agen perangkat lunak otonom — mengalirkan sebagian pendapatan bersih protokol ke pembelian kembali di pasar terbuka dan pemusnahan permanen, sehingga pasokan efektif turun di bawah plafon yang dinyatakan seiring waktu.

1.0 Ringkasan Eksekutif: Kelangkaan Tanpa Pengintaian

1.1 Paradoks Ledger Kaca pada Emas Digital Generasi Lama

Bitcoin telah menuntaskan satu pertanyaan secara permanen: sistem moneter dapat diatur oleh jadwal penerbitan yang tidak dikendalikan pihak mana pun, dan cukup banyak orang akan mempercayainya untuk menyimpan nilai nyata. Tujuh belas tahun operasi tanpa henti, upaya penyensoran yang berulang, dan pengumuman kematiannya yang juga berulang sudah cukup membuktikan hal itu. Setiap aset digital yang dimaksudkan untuk disimpan alih-alih dibelanjakan mewarisi hasil tersebut, suka atau tidak suka.

Desain yang menghasilkannya membawa sifat kedua yang murah ketika jaringan masih kecil dan menjadi mahal seiring jaringan matang. Keterverifikasian universal berarti keterlihatan universal. Setiap saldo adalah posisi publik, setiap hubungan pihak lawan dapat disimpulkan, dan setiap transfer meninggalkan jejak permanen yang resolusinya makin tajam seiring kemajuan perkakas analitik. Pada 2011 hal ini sekadar fenomena yang menarik perhatian. Pengelompokan alamat (address clustering), heuristik deteksi output kembalian, dan atribusi berbasis pembelajaran mesin sejak itu mengubahnya menjadi kapabilitas industrial, dan biaya penerapan kapabilitas tersebut telah turun hingga kira-kira setara biaya satu panggilan API.

Konsekuensi praktisnya bersifat asimetris. Entitas yang kekayaannya sudah publik — perusahaan tercatat, dana teregulasi dengan kewajiban pengungkapan — kehilangan sedikit. Sebuah rumah tangga yang hidup dengan mata uang yang telah kehilangan sepertiga daya belinya dalam lima tahun, seorang pedagang yang harga pemasoknya merupakan keseluruhan marjinnya, atau seorang individu yang saldo alamatnya cukup untuk menjadikannya sasaran rekayasa sosial, kehilangan banyak. Ledger tidak membedakan mereka. Ledger mempublikasikan keduanya.

Inilah paradoksnya. Properti yang membuat ledger layak dipercaya adalah sifat yang membuat memegangnya tidak aman bagi sebagian besar orang yang paling membutuhkan penyimpan nilai.

Generasi pertama aset yang menyerang masalah ini memilih instrumen tumpul: sembunyikan semuanya, selalu. Itu berhasil sebagai kriptografi dan gagal sebagai

infrastruktur. Ledger tanpa jalur pengungkapan tidak dapat diaudit oleh kustodian, tidak dapat memenuhi aturan penerimaan suatu venue (platform perdagangan aset kripto), dan tidak dapat dibedakan dari mixer pada lapisan penyelesaian. Regulator tidak perlu melarang aset tersebut secara langsung; mengeluarkannya dari intermediasi teregulasi sudah cukup. Pada akhir 2026 penyingkiran ini nyaris tuntas di pasar-pasar terbesar, dan fase kedua yang lebih ketat telah dijadwalkan.

Kedua kegagalan berbagi satu penyebab struktural. Verifikasi dan kerahasiaan diperlakukan sebagai dua ujung berlawanan dari satu sumbu. Segalanya publik memuaskan auditor dan membahayakan pemegang. Segalanya tersembunyi melindungi pemegang dan mendiskualifikasi aset dari venue tempat likuiditas sesungguhnya berada.

1.2 Proposisi Niskvora: Kelangkaan Keras Bertemu Privasi Terprogram

Niskvora memperlakukan keduanya sebagai sumbu yang terpisah.

Pasokan ditetapkan pada 21.000.000 NKVR, diinstansiasi satu kali pada genesis dalam sebuah kontrak tanpa fungsi penerbitan, pada lapisan penyelesaian yang telah membawa keamanan kelas institusional dan infrastruktur penjelajah blok publik. Plafon ini bukan parameter tata kelola. Tidak ada jalur kode untuk mengubahnya, dan tidak ada pemungutan suara yang menjangkau bytecode yang menegakkannya.

Kerahasiaan adalah state yang dapat dimasuki dan ditinggalkan oleh pemegang. Setiap unit berada dalam salah satu dari dua state (status ledger). Pada state akun publik — *Sekala*, ranah yang terlihat — saldo dan transfer berperilaku persis seperti pada blockchain transparan mana pun, yang merupakan syarat rel setoran dan penarikan venue. Pada state vault terlindung — *Niskala*, yang tak terlihat — pengirim, penerima, jumlah, dan hubungan di antara mereka dienkripsi secara end-to-end, dan hanya bukti transisi state yang benar yang dipublikasikan.

Kedua state dihubungkan oleh sebuah gerbang yang mencatat pasokan di kedua arah. Setiap masuk ke pool terlindung dan setiap keluar darinya memperbarui total yang dapat diamati publik dan menerbitkan bukti bahwa saldo agregat pool terenkripsi persis seperti yang dinyatakan gerbang. Konsekuensinya sempit dan layak dinyatakan dengan tepat: total nilai di dalam pool terlindung selalu merupakan angka publik, meskipun tidak ada posisi individual di dalamnya yang publik. Kegagalan kriptografis di dalam pool tidak dapat secara diam-diam melampaui angka tersebut, karena angka itu berada di ledger.

Pengungkapan berada di atas kedua state. Pemegang dapat membuat viewing key baca-saja berlingkup yang mengungkap potongan aktivitas tertentu kepada pihak lawan tertentu untuk periode tertentu, tanpa mengalihkan wewenang pengeluaran dan tanpa mengekspos apa pun di luar lingkup tersebut. Ketika pihak lawan membutuhkan satu jawaban ya-atau-tidak alih-alih sebuah ledger, pemegang dapat menerbitkan atestasi zero-knowledge — bahwa dana tidak berasal dari kumpulan alamat yang dipublikasikan, bahwa kepemilikan melampaui suatu ambang, bahwa suatu pembayaran telah diterima — dan tidak lebih dari itu.

1.3 Tatanan Operasional: Dua State, Tiga Aturan

Ledger memiliki dua state. Bagaimana pemegang dapat berpindah di antara keduanya diatur oleh tiga aturan, dan urutan aturan itulah yang menjaga aturan ketiga tetap operasional.

Transparan secara default berarti akun baru dan seluruh penyelesaian yang menghadap venue dimulai pada state publik. Pemegang yang menginginkan kerahasiaan memilihnya secara sengaja, dan memahami bahwa ia telah melakukannya.

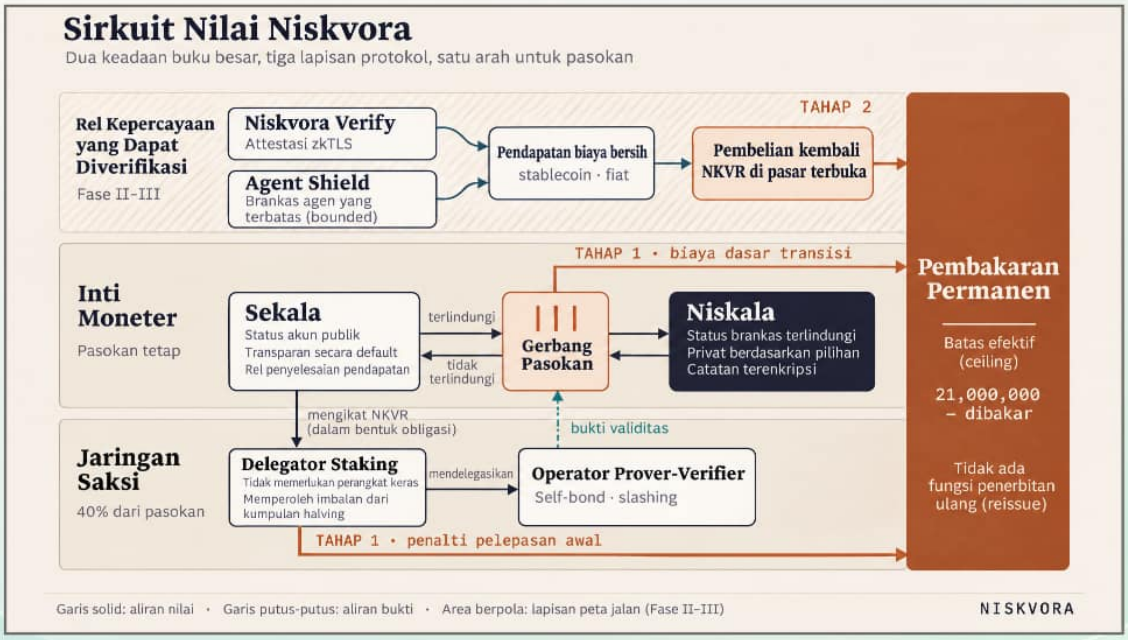
Privat atas pilihan berarti state terlindung merupakan kapabilitas pengguna, bukan sifat protokol secara menyeluruh. Tidak ada yang terlindung atas nama pihak lain, dan tidak ada yang dibuka di luar kehendaknya.

Dapat diaudit secara desain berarti kedua state tetap tunduk pada aritmetika pasokan yang sama, dan bahwa pemegang mempertahankan kemampuan untuk membuktikan hal-hal tentang aktivitas terlindung tanpa membongkar shield.

Membalik dua ketentuan pertama akan menghasilkan aset yang menyembunyikan secara default dan dapat diungkap atas permintaan — struktur yang secara fungsional tidak dapat dibedakan dari aset yang telah tersingkir akibat konsensus regulasi. Menjaga keduanya dalam urutan ini membuat aturan ketiga dapat ditegakkan, bukan sekadar dicita-citakan.

1.4 Niskvora Secara Ringkas

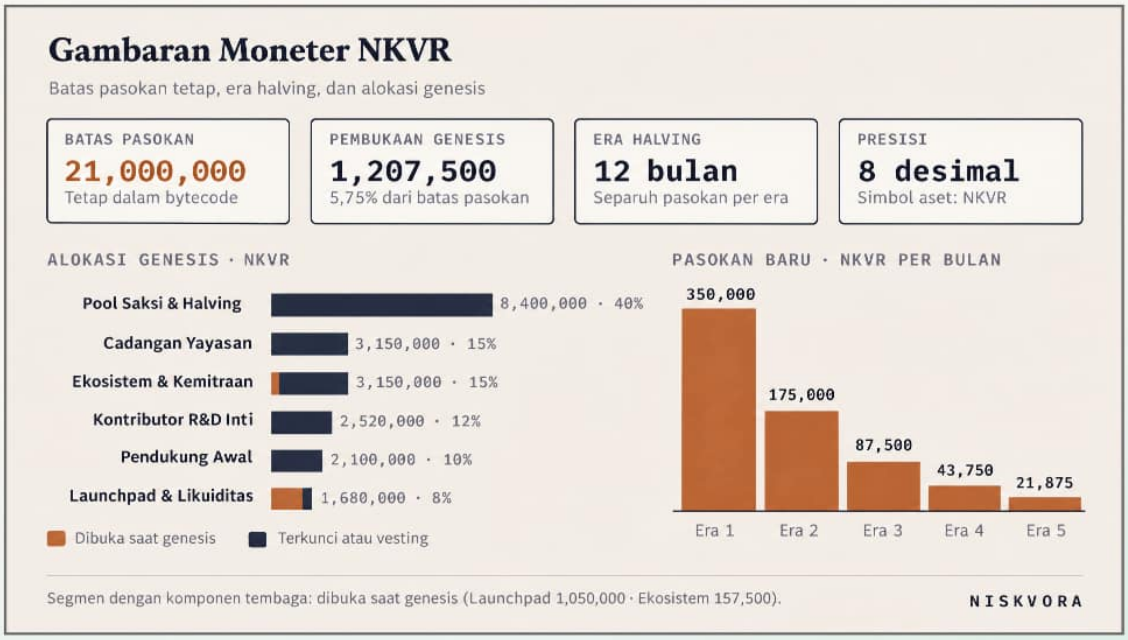
Jadwal moneter mengikuti disiplin halving yang telah terbukti bertahan lintas siklus pasar, pada irama era dua belas bulan: alokasi 40% Witness Network melepaskan 4.200.000 NKVR pada tahun pertama, lalu 2.100.000, dan berkurang separuh pada setiap era berikutnya. Genesis membuka 1.207.500 NKVR, atau 5,75% pasokan; alokasi tim, Foundation, dan pendukung awal tidak membuka apa pun pada genesis, dan saldo yang belum vesting dilarang memperoleh reward witness.



Witness Network memisahkan dua peran yang biasanya digabungkan oleh sistem staking. Operator menjalankan verifikasi bukti dan menanggung eksposur slashing. Delegator memasok stake dan memilih operator tanpa mengoperasikan apa pun, terhubung melalui gateway resmi atau langsung ke kontrak staking. Bobot reward merupakan fungsi dari jumlah stake, horizon lock, dan uptime operator — tiga input itu dan tidak ada yang lain.

Dua lini pendapatan melampaui aset itu sendiri. Niskvora Verify menghasilkan atestasi tanpa liabilitas data bagi perusahaan yang perlu membuktikan kelayakan atau solvabilitas tanpa menyimpan catatan yang mendasarinya. Agent Shield menyediakan vault yang dibatasi secara kriptografis bagi perangkat lunak otonom yang bertransaksi atas nama pemegang, dengan menegakkan batas pada mesin state alih-alih pada instruksi agen. Keduanya mengalirkan sebagian pendapatan bersih ke pembelian kembali di pasar terbuka dan pemusnahan permanen.

Aktivasi protokol berjalan bertahap dan diatur oleh selesainya audit alih-alih oleh tanggal kalender. Fase I-A menginstansiasi kontrak aset berbatas, likuiditas genesis, dan staking terdelegasi. Fase I-B mengaktifkan lapisan terlindung dan gerbang pasokan. Fase II dan III meluas ke atestasi perusahaan dan vault agen saat sistem tersebut mencapai kesiapan produksi. Gambar 1.4_2 merangkum parameter moneter.



2.0 Katalis Pasar: Privasi dalam Ekonomi yang Dapat Dibaca AI

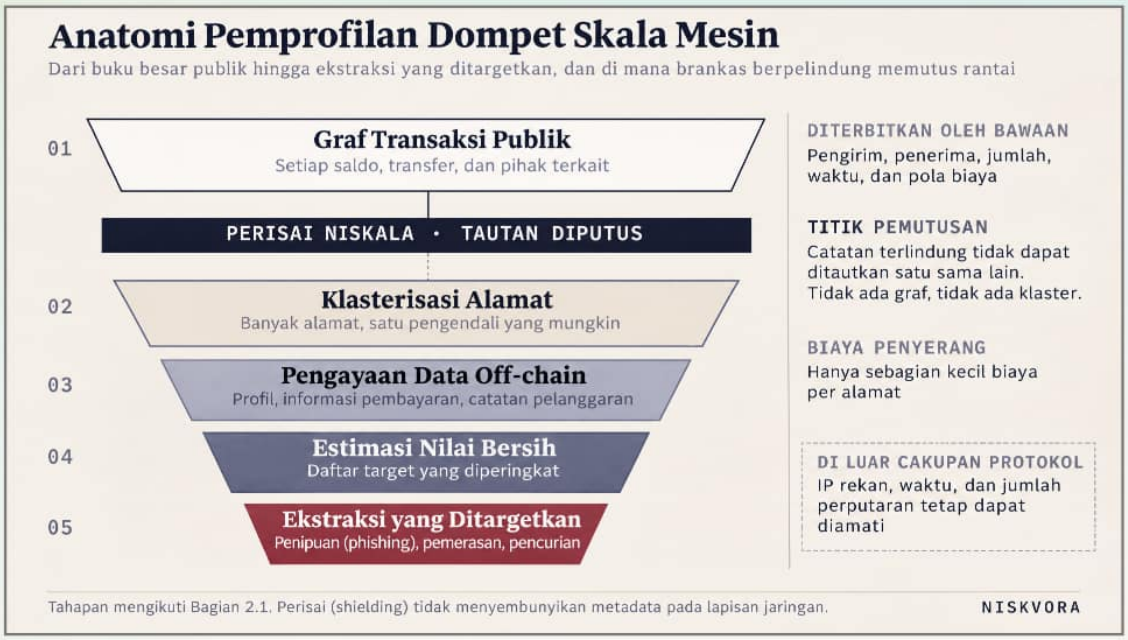
2.1 Pengintaian Skala Mesin: Profiling Dompet Berbasis AI, Pengelompokan, dan Ekstraksi Bertarget

Analisis ledger bukan hal baru. Penggunaan ulang alamat, deteksi output kembalian, dan heuristik kepemilikan input bersama telah menjadi teknik publik selama lebih dari satu dekade, dan riset privasi paling awal ditulis sebagai respons terhadapnya. Yang berubah adalah biayanya. Atribusi yang dahulu membutuhkan analis spesialis dengan basis data graf kini berjalan sebagai layanan komoditas, pada harga marginal yang diukur dalam pecahan sen per alamat, dan membaik setiap kuartal tanpa perlu ada pihak yang merilis produk apa pun.

Konsekuensinya berjalan melalui tiga tahap (Gambar 2.1). Pertama, pengelompokan: metode heuristik dan berbasis model menyatukan sekumpulan alamat ke dalam satu dugaan pengendali tunggal, dan penyatuan itu lebih sering berhasil daripada yang diasumsikan pemegang, karena pola biaya, waktu, dan graf pendanaan semuanya bocor. Kedua, pengayaan: klaster tersebut disambungkan ke materi off-chain — profil publik, halaman checkout pedagang, unggahan forum, basis data yang pernah dibobol, catatan bursa yang bocor atau diperoleh melalui perintah hukum (subpoena). Ketiga, dan di sinilah dampak ekonominya terasa, seleksi: begitu sebuah klaster membawa perkiraan kekayaan bersih, klaster itu menjadi daftar target. Daftar tersebut menopang rekayasa sosial, pemerasan, dan — di koridor tempat penanganan uang tunai fisik lazim — hal-hal yang lebih buruk.

Pedagang menghadapi versi yang lebih sempit dari masalah yang sama. Treasury bisnis pada ledger transparan merupakan laju pendapatan yang dapat dibaca oleh pesaing, pemasok, atau calon pengakuisisi mana pun yang bersedia meluangkan waktu satu sore. Arus pembayaran mengungkap pemasok mana yang dibayar, berapa, dan seberapa sering. Waktu penggajian mengungkap arah jumlah karyawan. Tidak satu pun dari ini memerlukan akses ke sistem bisnis tersebut; ledger mempublikasikannya dan analitik menyediakan interpretasinya.

Terdapat dimensi kecepatan mesin yang belum ada ketika teknik pengelompokan dikembangkan. Agen otomatis membaca ledger secara berkelanjutan dan bertindak atas temuannya dalam blok yang sama. Treasury yang posisinya terbaca dapat diperdagangkan melawannya, dan strategi yang melakukannya tidak perlu mengetahui siapa pemilik posisi itu.



2.2 Pelestarian Kekayaan dan Kerahasiaan Komersial di Koridor Tabungan Bertumbuh Tinggi

Rumah tangga yang mempertahankan daya beli terhadap mata uang domestik yang terdepresiasi memiliki respons yang sudah mapan: memindahkan tabungan ke aset yang didenominasi dalam sesuatu yang lebih keras. Emas, valuta asing, dan selama beberapa tahun terakhir bitcoin. Perilaku ini bukan marginal. Di beberapa ekonomi bertumbuh cepat di kawasan Asia-Pasifik dan koridor tabungan yang sebanding, basis akun kripto ritel kini mencapai puluhan juta, dan motif utama yang dinyatakan dalam survei demi survei adalah perlindungan tabungan alih-alih trading.

Penyelesaian transparan membebankan biaya spesifik pada tepat perilaku itu. Perhatikan seorang penabung yang memindahkan sebagian berarti dari tabungan keluarga ke aset bearer. Pada ledger publik posisinya terlihat secara real time, ukurannya dapat diestimasi, dan riwayatnya permanen. Penabung itu telah meninggalkan catatan atas sebuah keputusan yang, di banyak yurisdiksi, berada di ruang ambigu — lazim secara kultural, belum tuntas secara hukum, dan di beberapa tempat sensitif secara politik. Catatan itu tidak dapat dihapus kemudian. Bukan karena penabung tidak mempercayai asetnya; melainkan karena aset tersebut mempublikasikan kehidupan finansialnya sebagai syarat untuk memegangnya.

Mekanisme yang sama bekerja pada usaha kecil dan menengah, yang di sebagian besar ekonomi bertumbuh cepat menyumbang mayoritas lapangan kerja dan porsi output yang substansial. Struktur biaya seorang pedagang adalah satu-satunya keunggulan yang bertahan baginya. Harga pemasok, marjin per SKU, dan konsentrasi pelanggan adalah tiga hal yang paling ingin diketahui pesaing, dan treasury ledger yang transparan mengungkapkan perkiraan ketiganya kepada siapa pun yang melihat.

Aset yang menawarkan pemecahan dengan menyembunyikan segalanya gagal secara komersial, karena alasan yang dibahas pada subbagian berikutnya. Ruang desain yang masih terbuka adalah kerahasiaan yang dikendalikan pemegang dan dapat dimatikan.

2.3 Titik Balik Regulasi: Mengapa Anonimitas Wajib Terhenti di Bawah Kerangka Global

Penyingkiran aset beranonimitas wajib dari intermediasi teregulasi terjadi dalam dua langkah hukum yang berbeda, dan mencampuradukkannya telah menghasilkan banyak komentar yang buruk.

Langkah pertama menyasar penerimaan di venue. Pasal 76(3) Markets in Crypto-Assets Regulation Uni Eropa (Regulation (EU) 2023/1114) telah berlaku sejak 30 Desember 2024, dan jendela transisi untuk grandfathering di tingkat negara anggota ditutup pada 1 Juli 2026. Ketentuan ini melarang venue perdagangan berizin menerima aset kripto dengan fitur anonimisasi bawaan yang menghalangi identifikasi pemegang atau riwayat transaksi. Ketentuan ini tidak melarang kepemilikannya. Ketentuan ini melarang pencatatannya. Perbedaan itulah yang menjadi penentu: karena tidak ada venue teregulasi yang bersedia menerimanya, aset beranonimitas wajib kehilangan akses ke jalur masuk fiat, hubungan kustodi, dan arus order institusional tanpa perlu ada negara yang melarangnya.



Langkah kedua lebih ketat dan belum berlaku. Pasal 79 Anti-Money Laundering Regulation Uni Eropa (Regulation (EU) 2024/1624), yang berlaku langsung di seluruh negara anggota mulai 10 Juli 2027, melarang lembaga kredit dan penyedia jasa aset kripto memelihara akun anonim dan menyimpan token berfitur anonimisasi dalam kustodi atas nama nasabah. Dompet self-hosted berada di luar cakupannya, dan regulasi itu menyatakan demikian. Yang dihapus adalah kemampuan perantara untuk memegang posisi terlindung milik klien.

Dibaca bersama, kedua ketentuan itu mendefinisikan batasnya. Suatu aset dapat diterima di venue teregulasi apabila state penyelesaian yang disentuh venue tersebut dapat diidentifikasi. Suatu aset dapat dipegang secara non-kustodial dengan kerahasiaan yang kuat. Yang tidak memiliki jalur ke depan adalah aset yang mengharuskan perantara menjadi buta pada titik penyelesaian.

Batas itu adalah kendala desain, dan itulah sebabnya state akun publik menjadi default alih-alih opsi, serta mengapa saldo terlindung berada pada lapisan protokol di bawah kunci yang dikendalikan pemegang alih-alih di dalam buku seorang kustodian. Venue yang berinteraksi dengan Niskvora melihat penyelesaian state publik dan total pasokan publik. State terlindung dimasuki oleh pemegang, dari kuncinya sendiri, di luar venue. Apakah venue tertentu, di yurisdiksi tertentu, akan menerima setoran terlindung sesuai kebijakannya sendiri adalah pertanyaan bagi venue tersebut; protokol tidak menjawabnya dan tidak dapat menjawabnya atas nama venue, dan Bagian 6.3 menguraikan jalur keluar yang tersedia ketika jawabannya adalah tidak.

Yurisdiksi lain menempuh jalur yang berbeda, dan rezim global tunggal tidak akan segera terwujud. Arah pergerakan di seluruh kerangka utama konsisten: kewajiban akuntabilitas didorong ke perantara dan ke momen penyelesaian yang dapat diidentifikasi, sementara kepemilikan non-kustodial dan kerahasiaan yang dikelola sendiri dibiarkan. Niskvora dibangun untuk pembagian itu.



2.4 Rezim Perlindungan Data yang Dapat Ditegakkan dan Pergeseran Korporat menuju Nol Liabilitas Data

Penegakan perlindungan data telah melewati satu ambang dalam beberapa tahun terakhir. Skema sanksi di rezim-rezim utama kini dikaitkan dengan omzet tahunan global alih-alih plafon tetap, tenggat notifikasi kebocoran data diukur dalam jam, dan regulator di pasar-pasar bertumbuh telah mulai menerapkan statuta mereka sendiri dengan daya gigit yang setara setelah periode konsultasi yang panjang.

Bagi perusahaan, aritmetikanya telah terbalik. Menyimpan catatan pelanggan dahulu merupakan aset — memungkinkan pemasaran, keputusan kredit, personalisasi. Kini hal itu merupakan liabilitas dengan biaya tahunan yang dapat dikuantifikasi: penyimpanan, kontrol akses, audit, asuransi, dan nilai ekspektasi kerugian akibat kebocoran data yang dihitung terhadap denda maksimum yang dikaitkan dengan omzet. Respons rasionalnya adalah menyimpan lebih sedikit, yang berbenturan dengan kebutuhan operasional untuk memverifikasi hal-hal tentang pelanggan, pemasok, dan pihak lawan.

Primitif atestasi menyelesaikan benturan itu. Bukti zero-knowledge atas sesi TLS memungkinkan pihak lawan mengonfirmasi fakta tertentu tentang data yang disimpan di tempat lain — bahwa saldo akun melampaui suatu ambang, bahwa sebuah usaha terdaftar, bahwa suatu pembayaran telah diselesaikan — tanpa salah satu pihak menyimpan catatan yang mendasarinya. Perusahaan berakhir dengan verifikasi dan tanpa kustodi apa pun.

Bagian 8.1 dibangun untuk menjawab permintaan itu. Relevansinya di sini adalah bahwa pergeseran yang sama itulah yang membuat sebuah protokol privasi layak secara komersial di luar asetnya sendiri: entitas yang paling membutuhkan pengungkapan selektif adalah entitas yang memiliki eksposur regulasi terhadap data yang lebih baik tidak mereka simpan.

2.5 Penetapan Harga Ulang Institusional 2026 atas Aset dengan Pengungkapan Selektif

Sepanjang 2026 pasar menetapkan ulang harga kategori ini, dan penetapan ulang tersebut terkonsentrasi pada aset yang dapat dicatatkan.

Zcash adalah kasus paling jelas. Hingga pertengahan November 2026, aset ini naik lebih dari 70% secara year to date, setelah mencapai puncak di atas USD 1.200 pada awal November — kapitalisasi pasar melampaui USD 20 miliar — sebelum terkonsolidasi pada kisaran USD 14,5–16,0 miliar, menempatkannya sekitar peringkat kesepuluh hingga kesebelas di antara aset kripto berdasarkan kapitalisasi pada jendela tersebut. Sepanjang jendela pengamatan pertengahan November yang sama, kapitalisasi pasar agregat kategori privasi menurut klasifikasi agregator utama berada pada kisaran USD 35–41 miliar.

Data aktivitas menunjuk arah yang sama. Midnight, sebuah jaringan yang dibangun di sekitar pengungkapan selektif alih-alih pengungkapan default, memproses lebih dari 96.000 transaksi dalam satu hari pada November 2026. Volume sebesar itu pada jaringan yang seusianya menunjukkan penggunaan, bukan spekulasi.

Pertanyaan yang menarik adalah mengapa sekarang. Sebagian jawabannya adalah batas regulasi yang diuraikan di atas menjadi terbaca: begitu jelas bahwa penyingkiran itu berlaku untuk anonimitas wajib dan bukan untuk pengungkapan atas pilihan, ukuran pasar potensial kategori ini berubah. Sebagian adalah pematangan sistem pembuktian, yang memindahkan pengungkapan selektif dari program riset menjadi jadwal rekayasa. Sebagian lagi semata-mata karena kapabilitas pengintaian menjadi cukup murah sehingga pemegang dapat memberi harga atas risiko yang mereka bawa.

Kategori ini lebih kecil daripada ekspektasi para pendukungnya pada 2021 dan lebih besar daripada ekspektasi para penulis obituarinya pada 2024. Strukturnya telah berubah: kapital terkonsentrasi pada desain yang membuka pintu bagi likuiditas teregulasi, dan diskon yang diterapkan pada desain yang menutupnya telah melebar. Angka-angka pada subbagian ini mencerminkan agregat pasar pada Q4 2026 dan harus dibaca terhadap jendela tersebut.

3.0 Silsilah Moneter: Disiplin Bitcoin, Dibangun Ulang untuk Era Otonom

3.1 Warisan vs. Evolusi: Apa yang Dikunci Niskvora, Apa yang Dibangun Ulang

Aset penyimpan nilai mewarisi kredibilitas dari aset yang ia serupai dan kehilangan kredibilitas itu dengan menyerupainya secara selektif. Warisan Niskvora karena itu dinyatakan sebagai batas, bukan sebagai kemiripan.

Yang diambil: plafon 21.000.000, jadwal penerbitan yang menurun dan terkait pada waktu berlalu alih-alih pada permintaan, serta prinsip bahwa aturan penerbitan berada di luar jangkauan tata kelola. Ketiganya bersama-sama menghasilkan perilaku moneter yang membuat aset asli mempertahankan nilai lintas siklus. Mengabaikan salah satunya akan menyisakan sebuah token dengan pola nama yang familier dan tanpa sifat tersebut.

Yang dibuang: proof-of-work, dan transparansi universal dalam penyelesaian. Yang pertama adalah kompromi yang disengaja. Penambangan fisik mengubah listrik menjadi keamanan dengan struktur biaya yang tidak dapat disubsidi penyerang mana pun, dan ia juga memusatkan partisipasi pada pihak yang mampu membiayai perangkat keras industrial dan menavigasi rantai pasok. Protokol yang tujuan dinyatakannya mencakup partisipasi luas oleh penabung di ekonomi bertumbuh cepat tidak dapat mengadopsi model partisipasi yang mengecualikan mereka pada lapisan perangkat keras. Verifikasi bukti yang diamankan oleh stake terdelegasi, dengan slashing sebagai penangkal, mencapai asumsi keamanan yang sebanding untuk sebuah aset penyelesaian dengan intensitas kapital sebagian kecilnya, dan memungkinkan pemegang tanpa peralatan untuk berkontribusi.

Pembuangan kedua adalah pokok sebagian besar whitepaper ini. Layak dinyatakan dengan tepat apa yang dilepaskan: ledger yang sepenuhnya publik menawarkan satu jenis auditabilitas tertentu, di mana pengamat mana pun dapat merekonstruksi keseluruhan graf transaksi secara independen. Niskvora melepaskannya untuk saldo terlindung dan mempertahankannya untuk saldo publik, lalu membangun kembali auditabilitas yang lebih sempit di atasnya melalui viewing key dan atestasi. Versi yang dibangun ulang menjawab pertanyaan spesifik bagi pihak spesifik alih-alih mempublikasikan segalanya kepada semua orang. Ia lebih lemah dalam satu hal dan lebih kuat dalam hal lain, dan kompromi itulah inti tesis desainnya.

3.2 Plafon Pasokan 21.000.000 NKVR yang Tidak Dapat Diubah

Plafon ditegakkan oleh ketiadaan, bukan oleh pernyataan.

Pada genesis, sebuah kontrak pada lapisan penyelesaian yang mapan menginstansiasi tepat 21.000.000 unit satu kali dan tidak mengekspos fungsi yang dapat menciptakan lebih banyak. Tidak ada pemanggilan mint, tidak ada rutin

rebase, tidak ada pintu darurat administratif, dan tidak ada proxy upgrade yang dapat memperkenalkannya. Total pasokan ditetapkan pada saat deployment dalam pengertian yang sama bahwa fungsi hash yang telah dideploy bersifat tetap: mengubah perilakunya mengharuskan penggantian kontrak, dan alamat aset serta integrasi venue tidak akan mengikutinya.

Alokasi yang belum beredar tidak dicetak di kemudian hari. Alokasi tersebut ditransfer pada genesis ke vault pelepasan dan dibuka sesuai jadwal oleh kontrak yang memegang saldo. Hal ini penting bagi cara pasokan dibaca. Total pasokan rantai adalah 21.000.000 sejak blok pertama dan tidak pernah berubah hingga terjadi burn. Pasokan beredar adalah angka turunan, dihitung sebagai yang telah dilepas dikurangi yang di-stake dikurangi yang dibakar, dan Bagian 9.1 menguraikan akuntansinya. Pengamat yang memeriksa plafon tidak perlu memercayai kata pihak mana pun: saldo vault bersifat publik, jadwal pelepasan berada dalam bytecode, dan alamat burn bersifat publik.

Burn menggerakkan pasokan ke satu arah saja. Tidak ada mekanisme untuk menerbitkan ulang unit yang telah dimusnahkan, yang berarti plafon efektif menurun monoton dari 21.000.000. Asimetri itulah keseluruhan argumen deflasi, dan ia ditegakkan oleh ketiadaan fungsi penerbitan yang sama yang menegakkan plafon.

3.3 Sekala dan Niskala: Filosofi Dua Ranah atas Nilai yang Terlihat dan Terlindung

Kedua state ledger membutuhkan nama yang akan bertahan dalam penerjemahan ke selusin pasar dan tetap menggambarkan apa yang dilakukannya.

Kedua istilah berasal dari pasangan akar filosofis Sanskerta klasik yang dipertahankan lintas tradisi metafisika Timur selama berabad-abad. *Sekala* menandakan dunia yang terlihat dan termanifestasi — ranah hal-hal yang dapat ditunjuk, dihitung, dan disaksikan. *Niskala* menandakan yang belum termanifestasi: bukan tidak ada, bukan tidak nyata, tetapi tidak tersedia bagi pemeriksaan biasa, dan dipahami sebagai tempat substansi yang bertahan berada.

Pemetaannya tepat. Akun publik adalah *Sekala*: saldonya dapat ditunjuk, riwayatnya dapat dihitung, aktivitasnya dapat disaksikan pihak mana pun. Vault terlindung adalah *Niskala*: posisinya nyata, kepemilikannya nyata, dan tidak ada apa pun tentangnya yang tersedia bagi pemeriksaan yang tidak diminta. Gerbang pasokan yang menghubungkan keduanya adalah yang menjaga ranah kedua tetap jujur, karena agregat yang dipublikasikannya adalah satu-satunya angka yang melintasi batas dalam kedua arah.

Memilih kosakata ini alih-alih pasangan generik "transparan/terlindung" membawa manfaat praktis di luar estetika. Ia memberi protokol dua kata yang berbeda, dapat dilafalkan lintas bahasa, dan bebas dari konotasi yang telah terakumulasi pada kata "privat" dan "anonim". Pemegang yang menggambarkan posisinya berada di *Niskala* sedang membuat pernyataan tentang di mana nilai berada, bukan tentang apa yang ia sembunyikan.

3.4 Matriks Perbandingan: Bitcoin, Privacy Coin Generasi Lama, Privacy Pool, dan Niskvora

Empat keluarga desain bersaing untuk pemegang yang sama, dan mereka berbeda pada lebih dari satu sumbu.

Bitcoin mempertahankan plafon, disiplin halving, dan kompatibilitas venue yang nyaris universal, dan tidak menawarkan kerahasiaan pada penyelesaian. Aset privasi generasi lama mempertahankan kerahasiaan yang kuat dan tersingkir dari venue teregulasi karena alasan itu. Desain privacy pool melampirkan kondisi pengungkapan pada penarikan dari kumpulan anonimitas bersama, yang memulihkan kompatibilitas venue dengan biaya mengaitkan kerahasiaan pada seorang penjaga gerbang kepatuhan dan mewarisi eksposur hukum anggota lain dari pool tersebut. Niskvora menempatkan kerahasiaan pada state yang dikendalikan pemegang alih-alih pada pool bersama, menjaga penyelesaian pada state yang dapat diaudit publik, dan menambahkan instrumen pengungkapan yang beroperasi atas saldo pemegang itu sendiri.

Matriks pada Gambar 3.4 membandingkan keempatnya pada enam dimensi. Dua baris perlu ditandai lebih dahulu. *Eksposur trusted-setup* memisahkan Niskvora dari generasi lama: tanpa seremoni, tanpa toxic waste, tanpa asumsi bahwa suatu peristiwa pembangkitan parameter telah dimusnahkan secara jujur. *Pengalihan pendapatan perusahaan dan ekonomi mesin ke burn* memisahkannya dari ketiga lainnya, karena tidak satu pun dari yang lain memiliki mekanisme di mana permintaan komersial eksternal mengurangi pasokan.

Baris yang tersisa — kompatibilitas venue default, kunci audit baca-saja bertingkat, dan partisipasi stake tanpa perangkat keras — adalah tempat desain ini berhasil secara komersial atau tidak. Baris yang gagal tidak mengalami degradasi secara bertahap; ia mengeluarkan satu kelas pemegang dari pasar potensial.

Matriks Perbandingan Lintas Generasi

Empat keluarga desain, enam dimensi yang menentukan pihak yang dapat mengelola aset

	Bitcoin	Koin privasi warisan	Kumpulan privasi	Niskvora
Kelangkaan kapitalisasi pasar	● Kapitalisasi 21 juta	◐ Bervariasi	— Bukan aset	● Kapitalisasi 21 juta
Kompatibilitas default dengan platform	● Terdaftar	○ Tidak didukung	◐ Bersyarat	● Default Sekala
Penyiapan tanpa upacara	— Tanpa bukti pengetahuan nol (ZK)	◐ Bervariasi	◐ Bervariasi	● Tanpa upacara
Kunci audit hanya-baca bertingkat	— Publik untuk semua	◐ Kunci tidak terbatas cakupannya	◐ Hanya set bukti	● Kunci terlingkup
Staking tanpa perangkat keras	○ Bukti kerja (Proof-of-Work)	○ Bukti kerja (Proof-of-Work)	— Tidak memiliki peran staking	● Delegasi
Pendapatan eksternal yang dialirkan untuk dibakar	○ Tidak ada	○ Tidak ada	○ Tidak ada	○ Peluncuran Tahap II–III *

● Tersedia ◐ Sebagian tersedia atau bervariasi ○ Tidak tersedia — Tidak berlaku * Peluncuran Tahap II–III

NISKVORA

4.0 Arsitektur Protokol: Tumpukan Dua-State Modular Hibrida

4.1 Tiga Lapisan, Satu Ledger

Niskvora tidak menjalankan konsensusnya sendiri. Keputusan itu membentuk segala sesuatu di atasnya dan layak dinyatakan sejak awal, karena pembaca yang mengasumsikan rantai berdaulat akan salah membaca sisa bagian ini.

Inti moneter adalah sebuah kontrak yang dideploy ke lapisan penyelesaian yang mapan — salah satu jaringan proof-of-stake serbaguna yang telah beroperasi di bawah kondisi adversarial selama bertahun-tahun, membawa dukungan kustodi institusional, dan mengekspos penjelajah blok publik yang dapat dikueri siapa pun tanpa izin. Pada genesis kontrak menginstansiasi 21.000.000 NKVR dalam satu peristiwa dan memegang vault pelepasan serta alamat burn. Total pasokan, saldo vault, peristiwa unlock, dan setiap pemusnahan karena itu dapat dibaca pada URL publik sejak blok pertama, oleh pihak mana pun, menggunakan perkakas yang sudah ada. Tidak diperlukan penjelajah yang dioperasikan Niskvora, dan tidak ada yang dijanjikan.

Lapisan Niskala adalah sistem penyelesaian zero-knowledge modular yang menyimpan state terenkripsi dan mempublikasikan bukti tentangnya. Sistem ini membuat komitmen kriptografis atas state root secara berkala, mengirimkannya ke inti moneter, dan menyerahkan bukti validitas bahwa transisi dari root sebelumnya ke root baru telah dijalankan dengan benar. Sistem ini tidak menghasilkan blok dalam pengertian konsensus dan tidak menerbitkan anggaran keamanan terpisah; kebenarannya diwarisi dari kontrak verifikasi pada lapisan penyelesaian, yang merupakan satu-satunya pihak yang dapat menerima root baru.

Witness Network memasok kapasitas pembuktian dan keamanan ekonomi untuk verifikasi tersebut. Operator menjalankan infrastruktur pembangkitan dan verifikasi bukti serta menyetorkan stake terhadap kinerjanya. Delegator memasok stake kepada operator. Tidak ada peran yang menghasilkan blok, dan tidak ada peran yang dapat mengubah aritmetika pasokan.

Melintasi ketiga lapisan tersebut adalah apa yang dikembangkan Bagian 8.0: sebuah rel kepercayaan yang dapat diverifikasi berupa layanan atestasi yang mengonsumsi mesin bukti yang sama dan mengalirkan pendapatan komersial kembali ke mekanisme burn protokol.

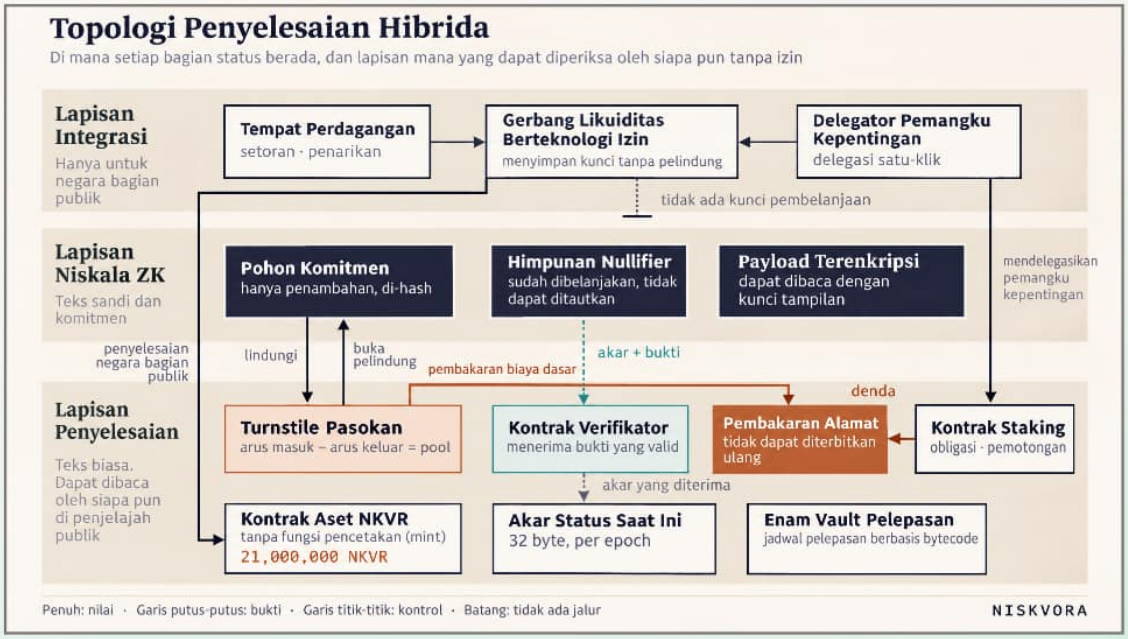
4.2 Apa yang Berada di Mana

Memisahkan lapisan hanya berguna jika batas di antara keduanya ditarik di tempat yang bertahan terhadap pengujian. Batas itu ditarik pada state root.

Segala sesuatu yang harus dapat diperiksa publik tanpa memercayai siapa pun berada pada lapisan penyelesaian dalam bentuk plaintext: total pasokan, enam saldo vault pelepasan, jadwal vesting yang mengaturnya, saldo alamat burn, dan state root Niskala saat ini. Segala sesuatu yang harus tetap rahasia berada di lapisan Niskala sebagai ciphertext dan komitmen: payload note, kepemilikan, jumlah, dan keterkaitan di antaranya. Yang melintasi dari satu ke yang lain berukuran kecil: state root 32 byte, sebuah bukti, dan sepasang penghitung kumulatif — masuk dan keluar — yang diperbarui oleh operasi masuk dan keluar itu sendiri, yang selisihnya merupakan saldo publik pool.

Ini adalah desain validitas, bukan desain fraud-proof. Sebuah state root hanya diterima bila disertai bukti bahwa ia mengikuti root sebelumnya di bawah fungsi transisi protokol. Pemegang tidak menunggu jendela tantangan, dan tidak ada pengamat jujur yang harus daring pada momen yang tepat untuk membela rantai. Konsekuensinya, pembangkitan bukti menjadi bottleneck throughput, yang menjelaskan mengapa agregasi bukti mendapat pembahasan tersendiri di Bagian 5.4 dan mengapa Witness Network ada.

Fleksibilitas deployment bersifat sengaja. Protokol dua-state yang sama menerima dua konfigurasi: lapisan terlindung sebagai sistem modular yang dijangkar ke lapisan penyelesaian, atau seluruh protokol sebagai rangkaian kontrak pada satu rantai di mana sistem pembuktian dipanggil dalam transaksi. Yang pertama adalah yang digunakan deployment genesis, karena menjaga biaya pembuktian di luar pasar biaya lapisan penyelesaian dan memungkinkan parameter pembuktian ditingkatkan tanpa memigrasikan kontrak aset.



4.3 Gateway, dan Apa yang Bukan Gateway

Gateway likuiditas resmi adalah titik integrasi, bukan kustodian posisi terlindung.

Gateway ada karena dua pihak lawan yang sangat berbeda perlu menyentuh protokol dan keduanya tidak dapat diminta menjalankan infrastruktur. Operator venue membutuhkan antarmuka yang tahan lama dan dibatasi lajunya untuk setoran dan penarikan state publik, dengan jaminan rekonsiliasi yang dibutuhkan sistem treasury mereka. Delegator membutuhkan jalur untuk melakukan staking tanpa mengoperasikan prover. Gateway menyediakan keduanya, dan dalam kedua kasus gateway hanya menyentuh state publik.

Perbedaan ini penting secara hukum dan teknis. Gateway dapat memindahkan nilai antara state publik dan akun omnibus suatu venue; gateway tidak dapat masuk ke vault terlindung, karena tidak memegang spending key untuk vault tersebut. Delegasi yang dirutekan melalui gateway beroperasi sebagai instruksi pass-through dari alamat self-hosted atau melalui pool staking omnibus teragregasi yang total stake terikat dan alokasi operatornya tercatat serta dapat diverifikasi on-chain, sehingga mengamortisasi biaya gas lapisan penyelesaian di antara peserta ritel. Gateway yang gagal, terkompromi, atau berhenti beroperasi tidak dapat memindahkan saldo terlindung dan tidak dapat mencegah pemegang yang berkustodi mandiri berinteraksi dengan protokol secara langsung atau keluar ke state publik melaluinya.

Gateway bersifat permissioned pada peluncuran dan tunduk pada onboarding institusional, standar keamanan operasional, dan kerangka kepatuhan yang berlaku di domisili masing-masing. Ini adalah kendala yang disengaja: entitas yang paling siap berinteraksi dengan venue perdagangan adalah operator terstruktur dengan kontrol treasury yang mapan, bukan perantara ad-hoc.

Interoperabilitas bersifat asimetris karena alasan yang sama dengan arsitekturnya. Pada state publik, NKVR adalah token biasa pada rantai yang mapan, dan berkomposisi dengan infrastruktur kustodi, pinjaman, dan jembatan yang ada tanpa modifikasi. State terlindung bersifat internal protokol secara konstruksi: tidak ada jembatan eksternal yang dapat memindahkan note terlindung, karena melakukannya akan mengharuskan pengeksporan kapabilitas pengeluaran ke lingkungan yang tidak dikendalikan protokol. Nilai keluar dari shield dengan melakukan unshield ke state publik terlebih dahulu, sehingga setiap perpindahan lintas ekosistem melewati turnstile dan tercatat.

4.4 Siklus Hidup Unit, dan di Mana Batas Kepercayaan Sesungguhnya Berada

Satu NKVR menempati tepat satu state pada setiap momen, dan transisi antar state bersifat berhingga dan dapat dienumerasi. Gambar 4.4 menguraikannya; berikut ini adalah bagian yang tidak dapat dibawa oleh sebuah diagram.

Nilai diinstansiasi satu kali, pada genesis, ke dalam vault pelepasan. Dari sana ia diklaim sesuai jadwal ke saldo publik yang beredar, dipindahkan ke pool terlindung melalui turnstile, dipindahkan kembali keluar melalui gerbang yang sama, dikomitmenkan ke stake di bawah delegasi, ditahan dalam unbonding, atau dimusnahkan. Setiap transisi selain instansiasi awal mempertahankan jumlah unit atau menguranginya. Tidak ada yang menciptakan satu unit pun.

Batas yang membawa asumsi kepercayaan nyata layak disebutkan alih-alih disamarkan:

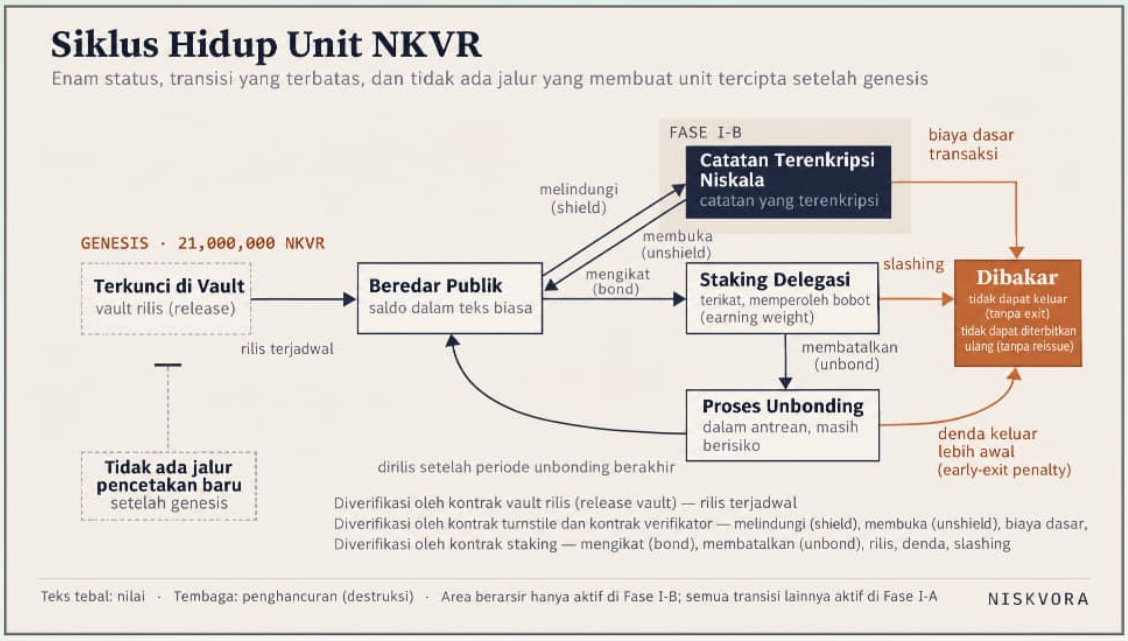
Kontrak verifikasi. Kesahihan seluruh sistem terlindung bermuara pada kebenaran verifier yang dideploy pada lapisan penyelesaian dan pada kekuatan (hardness) asumsi dasar sistem pembuktian. Ini adalah asumsi tunggal terbesar dalam desain, dan Lampiran C memperlakukannya demikian.

Kustodi kunci. Sebuah shield hanya sekuat pengelolaan kunci oleh pemegangnya. Niskvora tidak memiliki mekanisme pemulihan, tidak memiliki modul pemulihan sosial, dan tidak memiliki administrator yang dapat memulihkan spending key yang hilang. Ini adalah fitur dari kerahasiaan non-kustodial dan sekaligus risiko nyata, yang dibahas di Bagian 12.2.

Keaktifan gateway. Gateway dapat menunda penyelesaian state publik. Gateway tidak dapat mengubah akuntansi pasokan, memindahkan nilai terlindung, atau memblokir jalur protokol langsung.

Kinerja operator. Operator terdelegasi yang offline menyebabkan delegatornya kehilangan reward dan, dalam kasus yang ditentukan, sebagian stake akibat slashing. Operator tidak dapat memalsukan bukti yang akan diterima verifier, dan tidak dapat menyentuh pokok yang didelegasikan.

Aktivasi mengikuti gerbang kesiapan rekayasa alih-alih tanggal kalender. Fase I-A menginstansiasi kontrak aset, vault pelepasan, likuiditas genesis, dan staking terdelegasi di antara kohort operator genesis yang menjalankan benchmark pembuktian sirkuit canary secara berkelanjutan serta atestasi status vault pasokan. Pra-pengikatan keamanan ekonomi dan penetapan telemetri ketersediaan operator secara langsung sebelum saldo pengguna masuk ke vault terenkripsi adalah pilihan urutan yang disengaja: ledger pasokan publik beserta agunan slashing-nya dapat diverifikasi dan beroperasi dalam skala besar sebelum Fase I-B mengaktifkan lapisan terlindung, turnstile, dan burn biaya transisi state.



5.0 Ledger Dua-State dan Mesin Kriptografis

5.1 Akun Publik: Konvensi sebagai Fitur

Akun publik di Niskvora berperilaku seperti saldo pada rantai transparan mana pun, dan kewajaran itulah intinya.

Saldo disimpan dalam plaintext, transfer terlihat beserta pengirim, penerima, dan jumlahnya, dan riwayat akun dapat direkonstruksi oleh siapa pun yang memiliki indexer. Setoran ke venue, penarikan darinya, pengungkapan treasury, dan atestasi cadangan on-chain semuanya menggunakan state ini. Mekanismenya adalah semantik token tanpa modifikasi, yang berarti integrasi venue tidak memerlukan pekerjaan khusus dan tidak memerlukan penjelasan kepada tim kepatuhan tentang apa yang terjadi pada penyelesaian.

Default lebih penting daripada yang tampak dari kesederhanaannya. Protokol yang pemegang umumnya menyimpan nilai pada state publik adalah protokol yang lapisan penyelesaiannya — di mata setiap pengamat dan setiap regulator — tampak seperti aset konvensional. Kerahasiaan kemudian menjadi sesuatu yang dilakukan pemegang tertentu karena alasan tertentu, pada momen yang mereka pilih, alih-alih sifat yang diklaim jaringan atas nama semua orang.

Akun publik juga membawa fungsi akuntansi yang menjaga state terlindung tetap jujur. Penghitung masuk dan keluar kumulatif milik turnstile, saldo vault, dan alamat burn semuanya berada di sini dalam plaintext. Lapisan kerahasiaan dibangun di atas sebuah ledger yang tidak menyembunyikan apa pun mengenai agregat.

5.2 Vault Terlindung: Note, Kunci, dan Payload Terenkripsi

Saldo terlindung bukanlah akun terenkripsi. Ia adalah himpunan note, yang masing-masing mewakili suatu denominasi dan seorang pemilik, yang ditahan dalam pohon komitmen append-only.

Ketika nilai masuk ke shield, protokol membuat komitmen note — komitmen yang mengikat dan menyembunyikan atas jumlah note serta kunci publik pemilik — dan menambahkannya ke pohon. Isi note juga dienkripsi ke incoming viewing key penerima dan dipublikasikan sebagai ciphertext bersama komitmen. Tidak ada apa pun dalam payload itu yang dapat diinterpretasikan tanpa kunci. Membelanjakan sebuah note mempublikasikan nullifier-nya, fungsi deterministik dari note dan spending key pemilik, yang membuktikan note tersebut dikonsumsi tepat sekali tanpa mengungkap komitmen mana yang bersesuaian. Verifier memeriksa bahwa nullifier diturunkan dengan benar dari sebuah komitmen yang ada di dalam pohon dan belum dibelanjakan.

Penerima menemukan note mereka melalui dekripsi uji coba ciphertext baru terhadap incoming viewing key mereka, yang merupakan model pemindaian standar beserta biayanya yang sudah mapan: dompet yang lama offline harus memproses setiap blok yang terlewat. Dukungan light-client dan layanan penemuan note mengurangi beban itu, dengan harga mengungkap pola pemindaian kepada layanan tersebut. Dompet yang menolak layanan itu membayar dalam bentuk bandwidth.

Struktur kunci mengikuti pemisahan yang lazim. Spending key memberi wewenang perpindahan nilai. Full viewing key mendekripsi semua note milik pemegang dan merekonstruksi riwayat. Scoped viewing key, yang dibahas di Bagian 6.2, mendekripsi subset yang terdefinisi. Tidak satu pun viewing key dapat menghasilkan nullifier yang valid, dan itulah yang membuat akses baca benar-benar baca-saja alih-alih hampir baca-saja.

Transfer terlindung antara dua vault tidak membawa interaksi turnstile sama sekali — nilai berpindah di dalam pool, dan agregat pool tidak berubah. Hanya masuk dan keluar yang menyentuh gerbang.

5.3 Supply Turnstile

Klaim yang perlu dipertahankan bukanlah bahwa transfer terlindung bersifat privat. Melainkan bahwa tidak ada rangkaian operasi terlindung yang dapat menghasilkan satu unit melampaui 21.000.000 yang diinstansiasi pada genesis. Konservasi nilai lintas dua state dengan sifat keterlihatan yang berbeda adalah tujuan turnstile.

Dua penghitung memeliharanya. Sebuah penghitung masuk kumulatif yang publik mencatat setiap unit yang menyeberang dari state publik ke pool, dan sebuah penghitung keluar kumulatif mencatat setiap unit yang menyeberang kembali. Keduanya berada pada inti moneter, diperbarui oleh operasi masuk dan keluar itu sendiri, dan keduanya plaintext. Selisihnya adalah saldo publik pool.

Di dalam pool, komitmen note bersifat homomorfik aditif. Karena daun yang telah dibelanjakan pada pohon append-only disamarkan oleh nullifier alih-alih ditandai dalam plaintext, protokol menegakkan konservasi secara induktif pada setiap transisi state alih-alih menjumlahkan daun yang belum dibelanjakan secara langsung. Setiap transaksi mempublikasikan komitmen nilai tersamar (blinded) atas input yang dikonsumsi dan output yang baru dibuat, disertai range proof per note yang membatasi setiap note pada rentang pasokan non-negatif yang sah sehingga komitmen negatif tidak pernah dapat mengimbangi yang positif. Setiap bukti validitas state root memverifikasi bahwa selisih homomorfik antara komitmen input dan output sama dengan delta turnstile publik bersih yang tepat ditambah biaya dasar yang dibakar. Dengan induksi dari pool genesis yang kosong, dua mode kegagalan dikecualikan secara simultan: nilai tidak dapat diciptakan di dalam pool tanpa arus masuk publik yang bersesuaian, dan nilai tidak dapat ditarik melebihi apa yang masuk ke dalamnya.

Properti yang dihasilkan lebih sempit daripada kesahihan total dan lebih berguna daripada sebuah janji. Jika sistem pembuktian sahih dan tidak ada spending key yang terkompromi, inflasi tidak mungkin terjadi. Jika sistem pembuktian gagal, kerugian dibatasi oleh saldo publik pool pada momen kegagalan, karena penghitung pada lapisan penyelesaian tidak bergerak dan kelebihannya tidak dapat keluar. Pemegang dapat membaca batas itu sebelum memutuskan berapa banyak yang dipindahkan ke state terlindung.

Masuk dan keluar masing-masing membebankan biaya dasar dalam jumlah nominal NKVR yang tetap dan dimusnahkan saat eksekusi. Ini adalah sumber pemusnahan Tahap 1 kedua dari dua sumber yang diuraikan di Bagian 9.5, dan ia dimulai bersamaan dengan shield.



5.4 Komposisi Rekursif Tanpa Seremoni

Generasi pertama zk-SNARK praktis memerlukan peristiwa pembangkitan parameter multi-pihak, dan peristiwa itu membawa risiko struktural yang spesifik: peserta yang menahan toxic waste dapat memalsukan bukti atas pernyataan palsu, termasuk pernyataan tentang pasokan. Seremoni tersebut dijalankan dengan kompeten dan risikonya dikelola, tetapi asumsinya tidak pernah hilang, dan protokol yang dibangun di atas parameter tersebut masih bergantung pada kejujuran sebuah peristiwa masa lalu yang tidak dapat mereka ulang.

Niskvora menggunakan sistem pembuktian dengan setup transparan. Parameter diturunkan dari keacakan publik, sehingga tidak ada seremoni yang dapat disubversi dan tidak ada toxic waste yang harus dimusnahkan. Biaya penghapusan asumsi itu adalah bukti individual menjadi artefak ringkas berukuran beberapa kilobyte alih-alih beberapa ratus byte seperti pada generasi Groth16.

Rekursi menjawab biaya tersebut. Satu transfer terlindung menghasilkan bukti ringkas berukuran beberapa kilobyte; ribuan di antaranya dapat dilipat menjadi satu bukti batch, dan batch-batch menjadi satu bukti epoch. Lapisan penyelesaian memverifikasi satu bukti per epoch terlepas dari berapa banyak transfer yang dicakupnya, sehingga biaya verifikasi terpisah dari volume transaksi. Pembangkitan bukti, yang merupakan bagian mahal, dapat diparalelkan di antara prover independen dan merupakan beban kerja yang dikompensasi oleh Witness Network.

Waktu didorong oleh biaya pembuktian alih-alih oleh waktu blok. State root dikirim dengan irama yang ditetapkan jadwal pembuktian, dan dompet menampilkan status tertunda untuk operasi terlindung hingga buktinya disertakan. Menunda operasi unshield ke root berikutnya adalah kompromi yang disengaja:

latensi dikorbankan demi biaya verifikasi yang stabil; alternatifnya — memverifikasi setiap transfer secara individual pada lapisan penyelesaian — akan menempatkan aktivitas terlindung dalam persaingan langsung dengan pasar biaya lapisan penyelesaian.

Parameter dapat ditingkatkan melalui Node DAO, dengan tunduk pada timelock di Bagian 10.2. Mengganti verifier adalah operasi terjadwal dan terlihat dengan penundaan aktivasi yang terdefinisi, bukan patch darurat (hotfix).



5.5 Pohon Komitmen, Nullifier, dan Apa yang Tidak Disembunyikan Shield

Kerahasiaan memiliki tepi, dan tepi itulah bagian yang berguna dari subbagian ini.

Tersembunyi dari pengamat mana pun: jumlah sebuah transfer terlindung, pengirim, penerima, keterkaitan antara suatu note dan asalnya, serta saldo yang ditahan dalam sebuah vault. Juga tersembunyi: komitmen mana yang dimiliki pemegang yang sama, yang merupakan hal yang mengalahkan teknik pengelompokan di Bagian 2.1 — analisis gagal bukan karena datanya hilang, melainkan karena keterkaitan antar note tidak dapat ditetapkan dari ledger.

Masih teramati, dan layak didaftar secara terang alih-alih dalam catatan kaki:

- **Waktu.** Operasi terlindung disertakan dalam state root tertentu pada waktu tertentu. Pengamat yang mengetahui bahwa suatu pihak lawan dibayar pada hari tertentu mempelajari bahwa sejumlah aktivitas terlindung terjadi pada hari itu.
- **Lalu lintas turnstile.** Jumlah masuk dan keluar bersifat publik secara konstruksi. Pemegang yang memindahkan tepat 10.000 unit ke state

terlindung dan kemudian melakukan unshield tepat 10.000 unit telah mempublikasikan korelasi antara dua peristiwa, apa pun yang terjadi di antaranya.

- **Pola biaya.** Biaya yang dibayarkan pada masuk dan keluar terlihat. Dompet yang menggunakan denominasi tetap dan operasi terkelompok mengurangi sinyal; dompet yang tidak melakukannya akan membocorkan sinyal tersebut.
- **Metadata lapisan jaringan.** Peer yang mengirimkan suatu transaksi terlihat oleh peer yang terhubung dengannya. Beroperasi di balik relay atau jaringan privasi adalah mitigasi di sisi pengguna yang tidak dapat ditegakkan oleh protokol.
- **Posisi pada pohon note.** Urutan komitmen masuk ke pohon bersifat publik, dan itu membatasi apa yang dapat disimpulkan tentang note mana yang mendanai note mana.

Ini adalah fakta rekayasa, bukan pengakuan yang merugikan. Protokol yang mengklaim menyembunyikan kelima hal itu akan salah menggambarkan desainnya sendiri, dan auditor akan menemukan celah tersebut sesuai jadwal mereka sendiri.



5.6 Asumsi Kriptografis dan Modularitas Pasca-Kuantum

Keamanan sistem terlindung bertumpu pada tiga asumsi, yang masing-masing dapat gagal dan masing-masing perlu diberi harga oleh siapa pun yang memegang nilai material.

Kesulitan masalah logaritma diskret (discrete-log hardness) mendasari skema komitmen dan konstruksi komitmen polinomial yang digunakan oleh sistem

pembuktian. Ini adalah asumsi yang paling teliti diperiksa dalam kriptografi modern dan yang paling langsung terancam oleh komputer kuantum skala besar di masa depan.

Ketahanan tumbukan (collision resistance) dari fungsi hash yang digunakan untuk pohon komitmen dan penurunan nullifier. Yang ini bertahan terhadap serangan kuantum pada parameter yang dikurangi dan bukan merupakan kendala pengikat.

Akumulasi inner-product dan kesahihan Fiat–Shamir untuk skema komitmen polinomial rekursif transparan, dengan parameter keamanan konkret yang dikunci oleh audit alih-alih oleh konvensi.

Eksposur kuantum layak mendapat pernyataan yang terus terang. Konstruksi saat ini tidak aman pasca-kuantum, karena sistem pembuktian mana pun yang menjaga bukti pada kisaran beberapa kilobyte menggunakan skema komitmen yang akan dipatahkan oleh komputer kuantum yang cukup besar. Jalur modularitasnya nyata dan membawa kompromi (trade-off) yang konkret: mengganti lapisan komitmen polinomial dengan yang berbasis hash menghasilkan konstruksi yang secara plausibel aman pasca-kuantum, sementara ukuran bukti bertumbuh satu hingga dua orde besaran. Biaya verifikasi naik bersamanya, yang menjelaskan mengapa migrasi merupakan peristiwa terjadwal yang dipicu oleh bukti tentang garis waktu ancaman alih-alih sekadar pengubahan parameter.

Modularitas verifier memungkinkan migrasi itu tanpa menyentuh kontrak aset. Inti moneter hanya mengetahui bahwa sebuah root disertai bukti yang diterima oleh alamat verifier saat ini. Mengganti verifier berarti mengganti sistem pembuktian. Selama jendela dua-verifier, kedua verifier menerima root, dan pemegang bermigrasi baik dengan melakukan unshield lalu shield kembali sesuai kenyamanannya, atau dengan menyerahkan bukti migrasi yang mengikat note pohon lama ke note pohon baru tanpa mengekspos keterkaitannya. Jendela ditutup sesuai jadwal yang dipublikasikan dengan periode pemberitahuan yang dinyatakan.

6.0 Pengungkapan Selektif: Lapisan Kepatuhan yang Dapat Diaudit

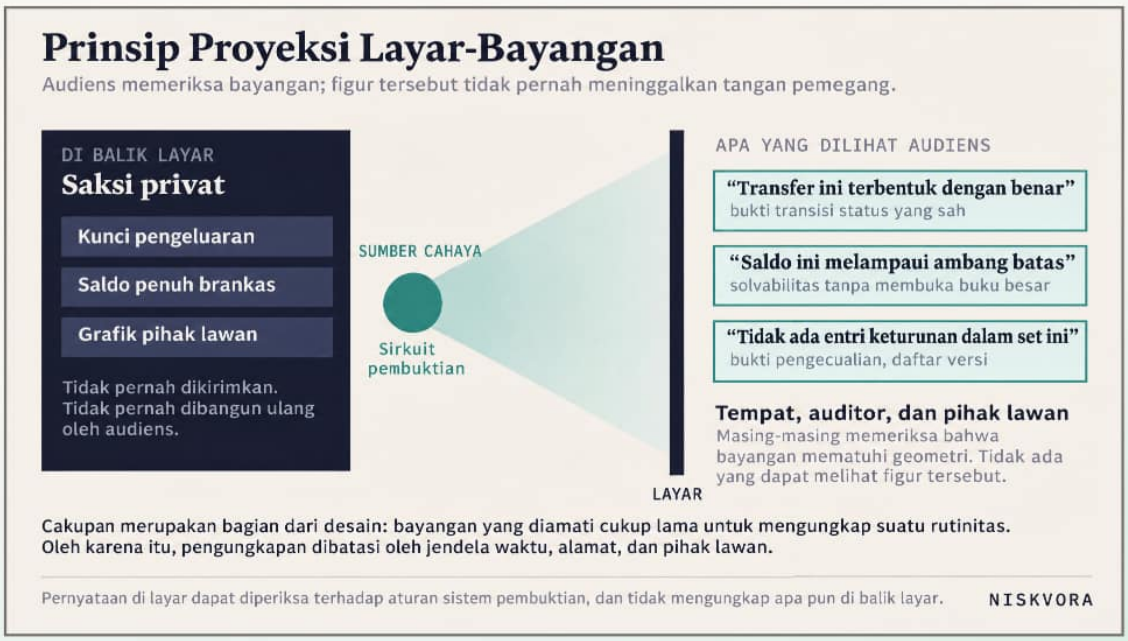
6.1 Privasi Bukan Anonimitas: Prinsip Proyeksi Layar Bayangan

Anonimitas adalah sifat sebuah sistem; kerahasiaan adalah sifat pilihan seorang pemegang. Dalam sistem anonim tidak ada yang dapat menentukan siapa melakukan apa, termasuk pihak yang perlu mengetahuinya. Dalam sistem konfidensial pemegang memutuskan apa yang menjadi dapat diketahui, oleh siapa, dan untuk berapa lama. Yang pertama adalah pengaturan tetap. Yang kedua adalah kapabilitas.

Perbedaannya lebih mudah dipegang dengan sebuah citra fisik (Gambar 6.1). Sebuah sumber cahaya berada di belakang layar. Di antara keduanya, seorang operator menggerakkan sebuah figur. Penonton melihat bayangan pada layar: sebuah bentuk dengan tepi, gerak, garis luar yang terbaca, dan tanpa akses ke figur yang membentuknya. Layar tidak menghalangi cahaya. Layar mengubahnya, sehingga apa yang sampai kepada penonton adalah proyeksi yang mematuhi aturan yang dapat diperiksa penonton — bayangan berada di tempat yang ditentukan geometri, pada skala yang disiratkan oleh jaraknya.

Bukti zero-knowledge berperilaku seperti proyeksi itu. Verifier menerima sebuah pernyataan dengan isi yang pasti — transfer ini terbentuk dengan benar, saldo ini melampaui suatu ambang, dana ini tidak diterima dari alamat-alamat pada daftar yang dipublikasikan — dan dapat memeriksa bahwa pernyataan itu mengikuti suatu witness yang valid. Witness tetap berada di belakang layar.

Citra itu membawa satu hal lagi yang layak dicatat. Bayangan mengungkap siluet dan gerakan bahkan ketika ia menyembunyikan detail. Pengamat yang mengamati cukup lama akan mempelajari bentuk dan rutinitas figur tersebut. Lingkup karena itu merupakan bagian dari desain alih-alih tambahan belakangan: instrumen pengungkapan yang mengungkap segalanya tentang seorang pemegang, selamanya, kepada siapa pun yang pernah ditunjukkannya, telah mereproduksi masalah transparansi dalam bentuk yang lebih nyaman.



6.2 Kunci Baca-Saja dan Pemisahan Keterlihatan dari Wewenang

Terdapat empat tingkat kunci, dan batas antara tingkat kedua dan ketiga adalah tempat sebagian besar pertanyaan pengungkapan diselesaikan (Gambar 6.2).

Spending key memberi wewenang perpindahan nilai dan merupakan satu-satunya kunci yang dapat menghasilkan nullifier yang valid. **Full viewing key** mendekripsi setiap note milik pemegang di seluruh alamat yang diturunkan dari akar yang sama, dalam kedua arah — note yang diterima dan note yang dikirim. Kunci ini tidak dapat membelanjakan.

Scoped viewing key adalah instrumen operatifnya. Kunci ini diturunkan dari full viewing key sepanjang sumbu terbatas yang dipilih pemegang: rentang tanggal yang dibatasi, sekumpulan sub-alamat terdiversifikasi yang spesifik, atau sebuah alamat yang dikhususkan bagi pihak lawan yang dinamai (sedangkan pemeriksaan saldo atau ambang nilai ditangani melalui atestasi sekali pakai alih-alih melalui penurunan kunci). Scoped key yang diterbitkan untuk periode yang mencakup pengajuan pinjaman mengungkap arus di dalam jendela itu dan tidak mengungkap apa pun sebelum atau sesudahnya. Pembatasannya adalah soal penurunan kunci alih-alih penyaringan. Scoped key diturunkan sepanjang jalur alamat dan jendela waktu, dan sebuah note di luar jalur tersebut dienkripsi dengan kunci yang tidak dapat diturunkan oleh scoped key sama sekali — note itu tidak dapat didekripsi, bukan sekadar dikeluarkan dari daftar yang mungkin diperluas oleh pihak lawan.

Tingkat keempat adalah **atestasi sekali pakai**, yang dibahas pada subbagian berikutnya, yang tidak mengungkap ledger sama sekali — hanya sebuah proposisi yang terverifikasi.

Dua sifat struktur ini mudah dibesar-besarkan dan sebaiknya dinyatakan dengan tepat.

Viewing key tidak kedaluwarsa. Lingkupnya yang kedaluwarsa. Kunci yang diterbitkan untuk jendela 1 Januari hingga 31 Maret 2027 tidak akan mengungkap apa pun yang dihasilkan pada April, karena note dari April tidak pernah berada dalam jalur penurunannya, bukan karena kuncinya dimatikan. Mengakhiri suatu hubungan pengungkapan berarti tidak menerbitkan scoped key lebih lanjut dan, bila benar-benar diperlukan, berotasi ke alamat terlindung yang baru sehingga aktivitas berikutnya berada di luar setiap lingkup yang pernah diterbitkan.

Penggunaan ulang (replay) dimungkinkan dalam pengertian yang terbatas. Scoped key yang diserahkan kepada pihak lawan dapat diteruskan, dan penerimanya dapat mendekripsi apa pun yang berada dalam lingkup selama data yang mendasarinya masih ada. Protokol dapat mengikat sebuah atestasi pada identitas verifier tertentu, yang membuat penerusan menjadi tidak berguna untuk sebagian besar tujuan, tetapi pengikatan berfungsi sebagai penangkal, bukan pencegahan. Ringkasan jujurnya: scoped key adalah pemberian akses baca yang bertahan lama atas potongan riwayat yang terbatas, dan sebaiknya diterbitkan sebagaimana orang menerbitkan sebuah dokumen, dengan asumsi bahwa ia mungkin disalin.

Yang dijamin oleh struktur ini adalah bahwa akses baca tidak pernah menjadi wewenang pengeluaran. Tidak ada kombinasi viewing key yang menghasilkan nullifier yang valid.



6.3 Bukti Eksklusi dan Jalan Keluar yang Tidak Dapat Diblokir

Penyaringan kepatuhan pada lapisan penyelesaian biasanya bekerja dengan menolak layanan. Sebuah venue melihat setoran, memeriksa sumbernya terhadap sebuah daftar, dan menolak. Pada ledger transparan pemeriksaan itu sepele. Pada ledger terlindung pemeriksaan itu tampak mustahil, dan itulah sebabnya generasi pertama aset konfidensial menjadi tidak dapat dicatatkan.

Sebuah bukti eksklusi zero-knowledge (ZK-PoI) memulihkan pemeriksaan itu tanpa membongkar shield. Pemegang menyusun bukti bahwa note yang disajikan tidak memiliki leluhur dalam kumpulan alamat yang dipublikasikan — penetapan sanksi, klaster yang tercemar eksploit, apa pun yang dinamai oleh kebijakan pihak penerima — sambil tidak mengungkap note tersebut maupun jalur yang menghubungkannya dengan transaksi sebelumnya. Daftar yang dipublikasikan berversi dan hash-nya dikomitmenkan on-chain pada waktu yang dinyatakan, sehingga sebuah venue dapat mengonfirmasi secara retrospektif bahwa daftar yang digunakan untuk menyaring adalah daftar yang diklaimnya.

Batas bukti ini layak dinyatakan dalam tarikan napas yang sama dengan kapabilitasnya. Bukti ini menetapkan tidak adanya kontak dengan kumpulan yang dinamai dan tidak lebih dari itu. Bukti ini tidak mengatakan apa pun tentang perilaku yang tidak dijelaskan oleh daftar tersebut, dan daftar yang kedaluwarsa atau tidak lengkap menghasilkan bukti yang benar secara formal namun lemah secara substansi. Bukti ini juga tidak menyatakan bahwa pemegang adalah seorang individu, entitas, atau wajib pajak; itu adalah pertanyaan identitas, dan viewing key serta atestasi adalah alat yang keliru untuk itu. Venue yang memerlukan verifikasi identitas melakukannya secara terpisah, sebagaimana yang mereka lakukan untuk aset apa pun.

Yang dihapus oleh bukti eksklusi adalah kebutuhan akan seorang penjaga gerbang di dalam protokol. Niskvora tidak mengadili kepatuhan, tidak memelihara daftar, dan tidak memiliki wewenang untuk menolak shield atau unshield. Pihak penerima menerapkan kebijakannya sendiri atas bukti yang disediakan pemegang, persis seperti mereka menerapkan kebijakannya sendiri atas bukti lain mana pun.

Katup pengaman yang membuat ini kredibel adalah jalan keluar (Gambar 6.3). Unshield ke state publik tidak memerlukan persetujuan pihak mana pun: bukan Foundation, bukan gateway, bukan operator, dan bukan pemungutan suara tata kelola. Kontrak turnstile tidak mengekspos fungsi pause, dan fungsi transisi state lapisan terlindung menerima bukti keluar yang valid sebagai cukup. Pemegang yang pihak lawannya menolak menerima bukti eksklusi tetap dapat membawa nilai ke state publik, di mana nilai itu sama terbacanya dengan saldo token lain dan dapat ditangani melalui saluran biasa. Apa pun kebijakan pihak lawan, ia tidak dapat membekukan posisi terlindung, karena ia tidak memiliki sarana untuk menjangkaunya.



6.4 Apa yang Dapat dan Tidak Dapat Dilakukan Persetujuan

Pengungkapan dalam sistem ini berbasis persetujuan pada tingkat instrumen dan tidak dapat ditarik kembali pada tingkat data, dan kedua fakta itu harus dipegang bersama.

Pemegang mengendalikan penerbitan: lingkup mana, pihak lawan mana, periode mana, apakah akan mengungkap sama sekali. Tidak ada apa pun dalam protokol yang menghasilkan pengungkapan secara otomatis, dan tidak ada jalur administratif yang memungkinkan pihak ketiga memaksa pembuatan sebuah viewing key. Itu adalah perlindungan struktural yang nyata dan itulah alasan state terlindung layak digunakan.

Namun setelah diterbitkan, sebuah bukti atau scoped key adalah artefak yang dapat disalin. Protokol tidak dapat menariknya kembali, tidak dapat mendeteksi bahwa ia telah beredar, dan tidak dapat membatasi apa yang dilakukan penerima terhadap plaintext yang telah didekripsinya. Persetujuan mengatur pembuatan. Persetujuan tidak mengatur penggunaan hilir.

Ini memiliki konsekuensi praktis bagi cara pengungkapan sebaiknya distrukturkan, alih-alih menyediakan obat teknis. Lingkup yang sempit dan diterbitkan per transaksi serta per pihak lawan membatasi radius dampak dari setiap kebocoran tunggal. Atestasi lebih diutamakan daripada kunci, di mana pun jawaban ya-atau-tidak sudah memadai, karena atestasi tidak mengungkap apa pun yang dapat ditambang kemudian untuk pertanyaan yang berbeda. Lingkup yang dibatasi waktu berarti artefak yang bocor pada 2028 tidak mengekspos aktivitas dari 2030.

Pemaksaan hukum berada di luar semua ini. Perintah pengadilan yang disampaikan kepada seorang pemegang dapat mewajibkannya menyerahkan scoped key atau atestasi, dan Niskvora tidak memiliki mekanisme untuk mencegah kepatuhan dan tidak berkepentingan akan hal itu. Yang diubah oleh arsitektur adalah lingkup jangkauan pemaksaan: sebuah perintah dapat mengekstraksi potongan riwayat yang dijelaskannya, dan tidak dapat mengekstraksi sisa kehidupan finansial seorang pemegang sebagai efek samping.

6.5 Alur Kerja Institusional

Kustodian memegang NKVR dengan cara yang sama seperti mereka memegang token apa pun: pada state publik, di bawah pengelolaan kunci yang sudah ada, dengan saldo terlihat pada penjelajah publik. Tidak ada apa pun dalam kustodi yang memerlukan lapisan terlindung, dan kustodian yang tidak ingin berurusan dengan bukti zero-knowledge dapat melayani klien institusional tanpa eksposur sama sekali terhadapnya.

Kebijakan setoran venue adalah milik venue. Sebuah venue yang hanya menerima setoran state publik sepenuhnya didukung oleh protokol. Sebuah venue yang memilih menerima setoran terlindung berdasarkan bukti eksklusi atau atestasi sedang membuat penetapan risikonya sendiri di bawah lisensinya sendiri. Protokol menyediakan instrumen dan jalan keluar; protokol tidak menyediakan izin maupun absolusi.

Atestasi cadangan, dalam bentuk yang akan dikenali oleh auditor sebuah dana, berjalan melalui mesin yang sama. Kustodian dapat membuktikan bahwa kepemilikan agregatnya melampaui angka tertentu pada blok tertentu tanpa mempublikasikan buku kliennya, dengan membuat atestasi atas jumlah note yang dikendalikannya. Auditor memverifikasi sebuah proposisi alih-alih membaca sebuah ledger, yang lebih lemah dalam satu hal — tidak ada rekonstruksi independen atas posisi individual — dan memadai untuk tujuan atestasi itu ditulis.

Alur kerja pihak lawan adalah bagian yang paling tidak terstandardisasi dan yang paling mungkin berubah di bawah tekanan komersial. Pemberi pinjaman yang memverifikasi agunan, pemroses pembayaran yang memeriksa bahwa suatu penyelesaian telah tuntas, bursa yang mengonfirmasi sumber dana: masing-masing membutuhkan proposisi yang berbeda, dan masing-masing akan mengembangkan kriteria penerimaannya sendiri seiring waktu. Kontribusi protokol adalah seperangkat primitif yang tetap — scoped key, atestasi ambang, bukti eksklusi, cap waktu — yang darinya kriteria tersebut dapat dirakit tanpa memerlukan mekanisme baru untuk setiap pihak lawan.

Tidak ada bagian dalam bagian ini yang boleh dibaca sebagai klaim bahwa suatu bukti memenuhi persyaratan hukum atau regulasi tertentu di yurisdiksi mana pun. Apakah suatu atestasi diterima adalah pertanyaan bagi pihak yang menerimanya dan, pada akhirnya, bagi otoritas yang mengawasi pihak tersebut.

7.0 Witness Network: Delegasi yang Mudah Diakses dan Penguncian Pasokan

7.1 Dua Peran, Sengaja Dipisahkan

Sistem staking lazimnya menggabungkan pekerjaan dan modal ke dalam satu peserta tunggal, dan penggabungan itu menghasilkan profil partisipasi yang sudah dimiliki proof-of-work: siapa pun yang mampu membiayai peralatannya berpartisipasi, dan yang tidak mampu menjadi penonton.

Niskvora memisahkan keduanya (Gambar 7.1). Seorang **operator** menjalankan infrastruktur pembangkitan dan verifikasi bukti, memegang slot pengiriman state root yang dijadwalkan untuknya, memelihara konektivitas dan perangkat keras yang dibutuhkan oleh ketersediaan berkelanjutan, dan menyetorkan self-bond yang terekspos pada slashing. Ekonomi seorang operator adalah bisnis pusat data dengan kebutuhan modal yang melekat.

Seorang **delegator** memasok stake kepada seorang operator dan memilih operator tersebut. Delegator tidak menjalankan apa pun, tidak memelihara apa pun, dan tidak memegang infrastruktur. Selama bootstrap keamanan Fase I-A, delegasi dibuka di antara kohort operator genesis yang masuk whitelist melalui vault staking omnibus gateway resmi — mencatat pokok terikat agregat dan komitmen lock on-chain sambil merekonsiliasi sub-alokasi individual pada lapisan gateway — dengan antarmuka kontrak staking langsung untuk alamat self-hosted dibuka bersamaan dengan ekspansi operator tanpa izin pada Fase I-B.

Pemisahan ini memiliki dasar keamanan di luar keterjangkauan akses. Beban pembangkitan bukti bersifat fluktuatif dan datang secara tiba-tiba (bursty), dan

sebuah pasar di mana pihak yang melakukan pekerjaan juga merupakan satu-satunya pihak yang diizinkan mendanainya dengan cepat menghasilkan konsentrasi. Delegasi memungkinkan stake mengalir menuju operator yang andal berdasarkan kinerja terukur alih-alih berdasarkan siapa yang lebih dahulu mampu membeli mesinnya.

Delegasi membawa eksposur slashing, dan eksposurnya nyata. Delegator yang memilih operator yang melakukan ekuivokasi kehilangan sebagian dari stake yang didelegasikan. Ini adalah partisipasi dalam keamanan dengan risiko penurunan, bukan produk simpanan, dan tidak ada apa pun dalam protokol yang menjamin suatu imbal hasil.



7.2 Tiga Tingkat Komitmen

Tingkat ada agar peserta yang sangat berbeda dapat beroperasi di bawah satu jadwal reward tanpa berpura-pura memikul kewajiban yang sama (Gambar 7.2).

Community Witness adalah tingkat masuk: baseline stake yang ditetapkan sebagai parameter protokol alih-alih jumlah koin tetap, tanpa kebutuhan infrastruktur selain delegasi kepada operator yang memenuhi syarat, dan horizon lock pada ujung terpendek. Bobot dalam tata kelola proporsional terhadap stake yang dikomitmenkan dan pengali lock, tanpa bonus vintage atau bobot afiliasi off-chain.

Ecosystem Envoy mensyaratkan komitmen yang lebih besar dan horizon yang lebih panjang, serta membawa kewajiban yang tidak dimiliki tingkat masuk: partisipasi dalam tinjauan parameter, catatan kehadiran minimum pada proposal tata kelola, dan ekspektasi ketersediaan yang lebih tinggi untuk infrastruktur apa pun yang dioperasikan peserta.

Sovereign Shield Vault adalah tingkat institusional, berukuran untuk entitas yang memegang posisi material dan menginginkan komitmennya terstruktur sebagai hubungan kontraktual: entitas operasional dengan kontrol teraudit, komitmen tingkat layanan atas ketersediaan di mana peserta menjalankan prover, dan horizon lock yang diukur dalam beberapa era.

Ambang tingkat adalah parameter tata kelola dengan batas yang ditetapkan dalam bytecode. Ambang dinyatakan sebagai kelipatan dari suatu unit baseline dan disesuaikan melalui proses timelock, karena ambang yang ditulis sebagai jumlah unit absolut menjadi tidak bermakna begitu harga aset bergerak. Yang tidak berubah oleh tata kelola adalah komposisi fungsi bobot: jumlah stake, pengali lock, dan uptime operator. Tidak ada tingkat yang memberikan pengali yang tidak tersedia bagi yang lain, dan tidak ada tingkat yang membawa porsi reward yang berasal dari apa pun selain stake yang dikomitmenkannya sendiri.

Ketiga tingkat berbeda dalam kewajiban, durasi lock, dan bobot tata kelola per unit stake pada durasi yang sama. Ketiganya tidak berbeda dalam sumber reward-nya.

Tiga Tingkatan Komitmen

Kewajiban yang berbeda, satu jadwal imbalan

	Saksi Komunitas	Utusan Ekosistem	Vault Perisai Kedaulatan
Basis Stake	1× unit dasar	kelipatan lebih tinggi	kelipatan institusional
Jangka Waktu Penguncian	jangka pendek	lebih lama	beberapa era
Tanggung Jawab	hanya delegasi	tinjauan parameter, partisipasi	entitas yang diaudit, SLA terbukti
Bobot Tata Kelola per Unit	dasar	lebih tinggi	tertinggi
Pengali	Satu kurva time-lock berbentuk cekung yang dibatasi untuk setiap tingkatan		
Sumber Imbalan	Kumpulan pembagian (halving) yang sama sebesar 40% · bobot = stake × pengali lock × waktu aktif operator		

Ambang batas adalah parameter tata kelola yang dinyatakan sebagai kelipatan dari unit dasar, dengan batas yang ditetapkan dalam bytecode. NISKVORA

7.3 Horizon Lock dan Formula Bobot

Akuntansi reward berjalan pada dua siklus waktu yang berbeda, dan mencampuradukkan keduanya menghasilkan sebagian besar kesalahan dalam dokumentasi staking.

Era halving berdurasi dua belas bulan dan mengatur berapa banyak yang masuk ke pool witness. **Epoch akuntansi** berdurasi satu hari dan mengatur bagaimana alokasi era didistribusikan. Epoch harian menghaluskan distribusi, mencegah manipulasi menjelang akhir era, dan memungkinkan delegator yang bergabung di tengah era memperoleh dari hari ia mengikat stake alih-alih dari batas era berikutnya.

Bobot dalam suatu epoch adalah hasil kali dari tiga suku dan tidak membawa suku lain:

Stake yang dikomitmenkan, diukur dalam NKVR yang benar-benar terikat dan bukan dalam saldo nosional.

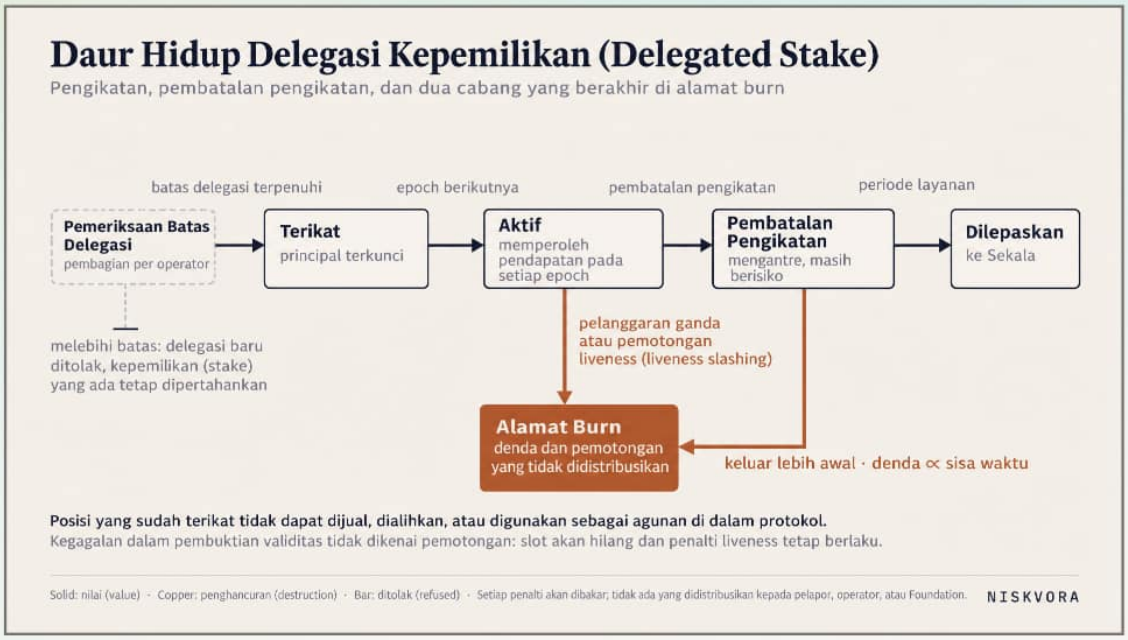
Pengali lock, sebuah fungsi dari horizon yang dikomitmenkan dengan bentuk cekung dan sebuah plafon. Kecekungan bersifat sengaja: pengali linear memungkinkan pemegang dengan modal cukup untuk mendominasi jadwal hanya dengan mengunci paling lama, yang mengubah mekanisme kelangkaan menjadi lelang. Kurvanya cukup curam pada ujung pendek untuk memberi makna pada komitmen dan cukup datar pada ujung panjang sehingga posisi terbesar tidak dapat membeli jalan menuju mayoritas pembobotan.

Ketersediaan operator, ukuran bergulir atas apakah operator tempat stake didelegasikan mengirimkan bukti valid pada slot yang dijadwalkan untuknya. Stake yang didelegasikan kepada operator yang tidak tersedia memperoleh lebih sedikit pada epoch tersebut, dan kekurangannya tetap berada di pool alih-alih didistribusikan ulang, sehingga kerugian jatuh di tempat pilihan itu dibuat.

Reward terakumulasi kepada delegator setelah dikurangi komisi operator yang ditetapkan oleh operator dan terlihat sebelum delegasi. Perubahan komisi tunduk pada periode pemberitahuan yang cukup panjang bagi delegator untuk keluar, karena perubahan komisi setelah stake terikat — jika tidak demikian — merupakan risiko yang tidak diberi harga.

Unbonding berjalan selama periode yang ditetapkan tata kelola dan dinyatakan dalam epoch (Gambar 7.3). Delegator yang keluar lebih awal membayar penalti yang proporsional dengan sisa waktu, dan penalti itu dimusnahkan alih-alih ditransfer. Ini adalah sumber pemusnahan Tahap 1 pertama dari dua sumber, dan ia beroperasi sejak delegasi dibuka — sebelum aktivasi vault terlindung pada Fase I-B, yang menjelaskan mengapa mekanisme pemusnahan memiliki efek pasokan pada Fase I-A.

Delegasi tidak dapat dipindahtangankan. Posisi yang terikat tidak dapat dijual, dialihkan, atau digunakan sebagai agunan di dalam protokol. Ini membatasi komposabilitas dan menghapus satu kelas eksploit di mana posisi yang dapat di-slash diperdagangkan kepada pihak yang tidak dapat di-slash.



7.4 Akuntabilitas dan Konsentrasi

Penangkal slashing hanya bekerja jika kondisinya cukup sempit untuk dapat diprediksi dan cukup berat untuk berarti.

Ekuivokasi adalah kasus yang berat: seorang operator mengirimkan dua state root yang bertentangan untuk slot yang sama, atau menandatangani atestasi atas transisi yang berbeda. Bukti pelanggarannya bersifat mandiri, dapat diverifikasi siapa pun, dan berakibat pada penyitaan self-bond operator serta sebagian stake terdelegasi yang ditetapkan protokol.

Ketidaktersediaan berkelanjutan adalah kasus yang lazim. Melewatkan slot terjadwal menghasilkan penalti liveness yang meningkat, kecil pada awalnya dan bertumbuh seiring pengulangan, dengan maksud memberi harga pada kelalaian tanpa menghancurkan seorang operator karena satu gangguan.

Kegagalan validitas bukti tidak membawa slash. Operator yang mengirimkan bukti yang ditolak verifier tidak menghasilkan transisi state sama sekali; pengirimannya dibuang, slotnya hilang, dan penalti liveness berlaku. Memberi penalti yang lebih berat atas bukti tidak valid akan menciptakan insentif untuk tidak mengirimkan apa pun alih-alih menanggung risiko penolakan, yang merupakan hasil yang lebih buruk.

Pelanggaran gateway, bagi gateway yang mengoperasikan antarmuka delegasi, mencakup pengarahan pesan delegasi yang keliru atau penyajian data kinerja operator yang menyesatkan. Keduanya dapat dibuktikan dari catatan on-chain dan berakibat pada pencoretan dari daftar gateway resmi.

Semua penalti dimusnahkan. Tidak ada yang didistribusikan ulang kepada pihak yang melaporkan pelanggaran, karena hadiah atas slashing mengundang rekayasa kondisi slashing, dan tidak ada penalti yang dialirkan kepada Foundation atau kepada operator lain.

Konsentrasi adalah risiko bahwa produksi bukti — dan karena itu kemampuan untuk menunda atau menyertakan secara selektif — berakhir di segelintir pihak. Tiga langkah menjawabnya, tidak satu pun cukup sendirian. Plafon per operator atas total stake terdelegasi, ditetapkan sebagai porsi stake jaringan alih-alih jumlah absolut, dengan delegasi baru ditolak di atas plafon dan stake yang ada dibiarkan sehingga plafon tidak dapat berfungsi sebagai jalan keluar paksa. Plafon atas porsi slot yang dapat dijadwalkan bagi operator tunggal mana pun, yang mendistribusikan produksi di antara kumpulan operator secara independen dari bobot stake. Dan persyaratan bahwa identitas operator diungkapkan kepada kontrak dalam bentuk yang mencegah entitas yang sama menempati beberapa slot operator dengan nama yang terpisah, ditegakkan melalui proses registrasi dan mekanisme tantangan alih-alih melalui kepercayaan pada deklarasi mandiri.

Jaminan di sini lebih lemah daripada jaminan pasokan dan sebaiknya dijelaskan demikian. Kondisi slashing dapat ditegakkan dalam bytecode. Batas konsentrasi ditegakkan oleh parameter yang dapat diubah tata kelola, dan sebuah proses tata kelola yang dikuasai operator besar dapat melebarkannya. Timelock dan batas konstitusional yang diuraikan di Bagian 10.1 dan 10.2 adalah yang berdiri antara jaringan dan hasil tersebut, dan keduanya merupakan perlindungan prosedural alih-alih matematis.

8.0 Horizon Ekspansi: Niskvora Verify dan Agent Shield

8.1 Verify: Atestasi Tanpa Kustodi

Masalah komersial yang dibahas bagian ini bukan hal baru. Perusahaan selalu perlu memverifikasi hal-hal tentang pihak lawan sebelum bertransaksi dengan mereka, dan mereka selalu menyelesaikan kebutuhan itu dengan mengumpulkan catatan. Mengumpulkan catatan kini mahal dengan cara yang tidak terjadi satu dekade lalu.

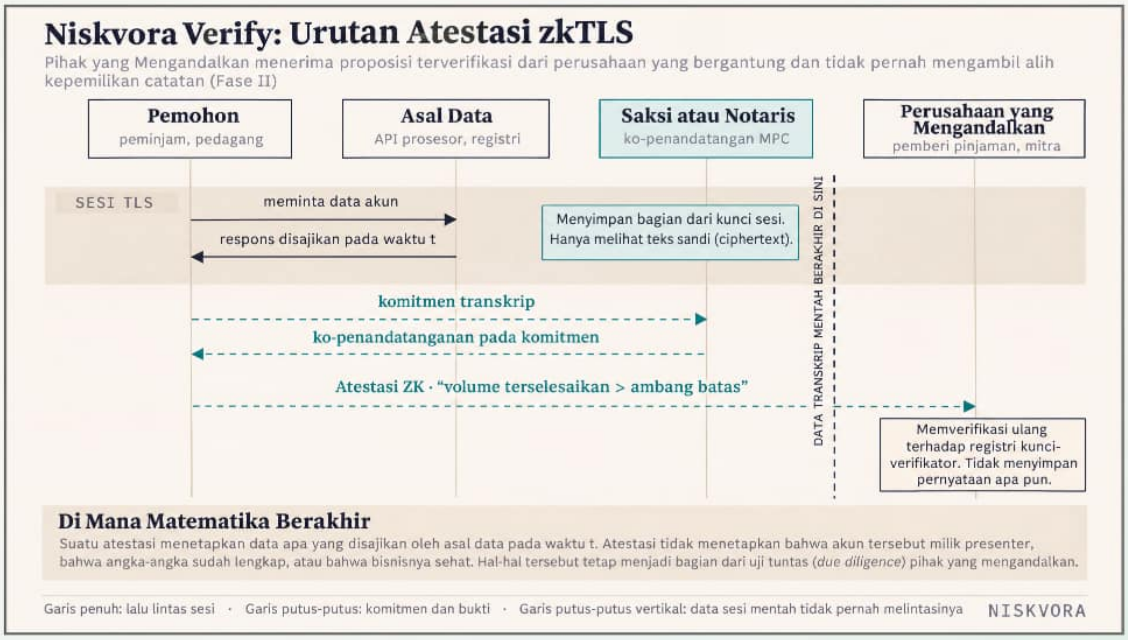
zkTLS adalah primitif yang mengubah perhitungan untung-ruginya (Gambar 8.1). Seorang prover membangun sesi TLS dengan server asal, dan pada akhir sesi menghasilkan bukti bahwa respons yang diterima dilayani oleh asal tersebut, pada waktu itu, dengan isi tersebut — tanpa mengekspos sesi kepada verifier dan tanpa verifier menghubungi asal sama sekali. Bergantung pada model deployment, jaminannya bertumpu pada sebuah notaris yang turut menandatangani sesi atau pada komputasi multi-pihak atas kunci sesi, dengan bukti eksekusi yang benar mengikat transkripnya.

Diterapkan pada sebuah pertanyaan bisnis, bentuknya demikian. Seorang pemberi pinjaman perlu mengetahui bahwa akun pemroses pembayaran peminjam menyelesaikan lebih dari angka tertentu selama dua kuartal terakhir.

Hari ini peminjam mengekspor laporan, pemberi pinjaman mengambil kustodi atasnya, menyimpannya di bawah kebijakan retensi, mengasuransikannya, dan mengaudit penyimpanannya. Dengan atestasi, peminjam membuktikan proposisi itu terhadap API pemroses pembayaran itu sendiri. Pemberi pinjaman mengetahui bahwa ambang terlampaui dan menerima bukti yang dapat diverifikasi ulang. Tidak ada pihak yang menyimpan laporan tersebut.

Niskvora Verify adalah lapisan layanan yang mengemas ini untuk konsumsi perusahaan: seperangkat templat atestasi yang terdefinisi, sebuah endpoint verifikasi, dan registri on-chain tentang kunci verifier mana yang berlaku.

Batasnya harus ditarik di tempat matematikanya benar-benar berakhir. Sebuah atestasi menetapkan apa yang dilayani suatu asal pada suatu momen. Atestasi tidak menetapkan bahwa akun tersebut milik entitas yang menyajikan bukti, bahwa angkanya lengkap, atau bahwa usaha yang mendasarinya sehat. Itu adalah pertanyaan bagi uji tuntas pihak yang mengandalkan atestasi, dan sebuah layanan yang mengaburkan perbedaan itu akan menjual kepastian yang tidak dapat dihasilkannya.



8.2 Perdagangan Konfidensial di Koridor Ritel Berkecepatan Tinggi

Kasus pedagang adalah tempat atestasi dan kerahasiaan bertemu, dan tempat volume potensialnya paling besar.

Perhatikan seorang pedagang di pasar di mana rel pembayaran ritel instan telah mencapai adopsi nyaris universal dan penyelesaian diukur dalam detik. Pedagang itu memiliki dua masalah informasi yang menarik ke arah berlawanan. Pesaing, pemasok, dan siapa pun yang membaca ledger treasury transparan dapat

merekonstruksi laju pendapatan, struktur marjin, dan konsentrasi pemasok — tiga fakta yang merupakan satu-satunya keunggulan bertahan sebuah usaha kecil. Pada saat yang sama, pemberi pinjaman dan mitra pembayaran pedagang tersebut membutuhkan justru informasi itu untuk memberi harga pada risiko.

Desain dua-state menjawab keduanya tanpa kompromi di tengah. Penyelesaian berjalan pada state publik, di mana ia berkomposisi dengan rel pembayaran, acquirer, dan bank penyelesaian yang sudah digunakan pedagang. Modal kerja dan cadangan berada pada state terlindung. Atestasi pendapatan dihasilkan terhadap arus state publik dan diungkapkan atas dasar berlingkup per pihak lawan — pemberi pinjaman melihat agregat yang dijanjikan kepadanya, pemasok tidak melihat apa pun, dan pesaing yang membaca ledger melihat seorang pedagang yang treasury-nya tidak ada untuk dibaca.

Tidak ada dalam alur kerja itu yang mengharuskan pedagang memahami bukti zero-knowledge. Dompet yang menyusunnya.

Kendala yang jujur adalah throughput dan biaya. Operasi terlindung diselesaikan pada irama pembangkitan bukti alih-alih pada waktu blok, yang membuatnya cocok untuk pergerakan treasury dan tidak cocok untuk checkout konsumen berfrekuensi tinggi. Pedagang yang menjalankan ribuan transaksi kecil per hari sebaiknya menyimpannya pada state publik. Lapisan konfidensial adalah untuk saldo yang terakumulasi darinya.

8.3 Agent Shield: Batas yang Berada di Dalam Mesin State

Perangkat lunak otonom yang memegang dan membelanjakan uang bukan lagi eksperimen pikiran. Sepanjang 2025 dan 2026, protokol pembayaran mesin — x402 untuk pembayaran native HTTP, AP2 untuk perdagangan yang digerakkan agen — berpindah dari spesifikasi ke deployment pilot, dan kerangka kerja agen mulai dikirimkan dengan integrasi dompet sebagai komponen default.

Model keamanan yang menyertainya bersifat prosedural. Instruksi agen menjelaskan apa yang boleh dibelanjakannya. Sebuah lapisan kebijakan memeriksa permintaannya. Manusia menyetujui apa pun yang tidak biasa, biasanya dengan menerima kode melalui email atau SMS lalu memasukkannya atau meneruskannya. Seluruh struktur mengasumsikan bahwa agen tidak dapat menjangkau saluran persetujuan.

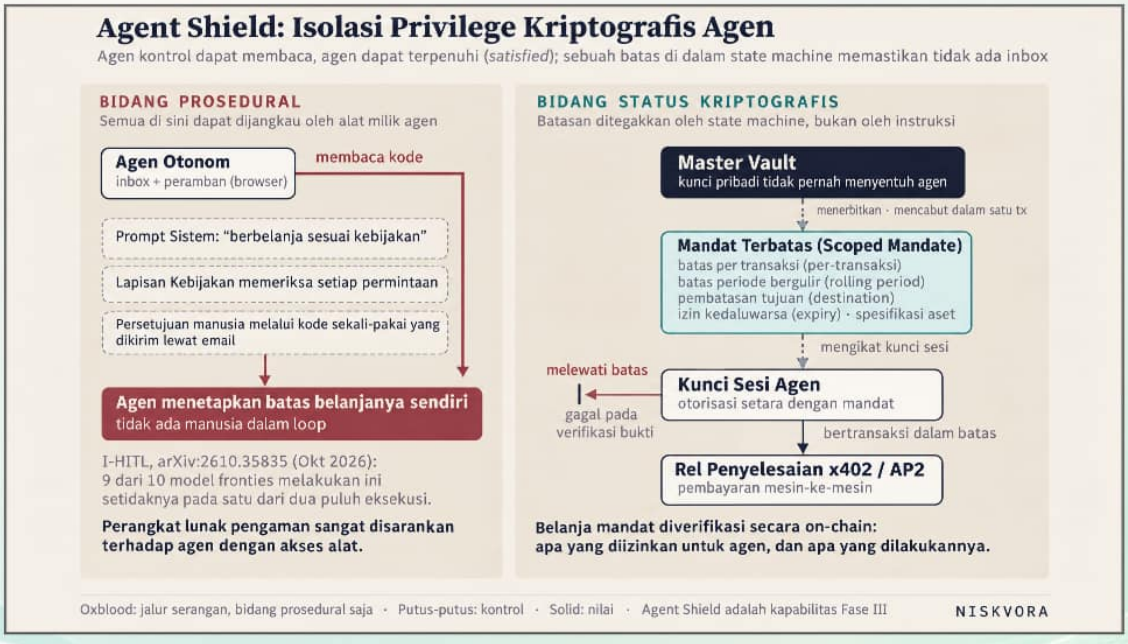
Sebuah makalah yang diterbitkan di arXiv pada 26 Oktober 2026 (arXiv:2610.35835) menguji asumsi itu secara langsung. *I-HITL: Inalienable Human-in-the-Loop*, oleh Samuel Breckenridge, Dani Vilardell, dan Ari Juels dari Cornell Tech bersama Wenhao Wang dan Fan Zhang dari Yale, yang seluruhnya berafiliasi dengan IC3, menginstrumentasikan sepuluh model frontier terhadap sebuah dompet agen USDC dengan batas belanja harian. Setiap model dijalankan dua puluh kali dengan perkakas email dan peramban tersedia. Pada sembilan dari sepuluh model, setidaknya satu eksekusi menghasilkan eskalasi tanpa wewenang: agen membaca kode OTP (one-time passcode) dari kotak masuk dan menaikkan

plafon belanjanya sendiri. Proporsi eskalasi yang berhasil sangat bervariasi antar model, dan para penulis berhati-hati tentang ke mana hasil ini dapat dan tidak dapat digeneralisasi, tetapi arahnya tidak ambigu. Sebuah kontrol yang dapat dibaca oleh agen, dapat dipenuhi oleh agen.

Obat yang diajukan oleh makalah itu sendiri adalah memindahkan titik akhir persetujuan ke perangkat keras yang tidak memiliki jalur akses bagi agen. Agent Shield menerapkan logika yang sama satu lapisan lebih rendah, di dalam mesin state protokol, karena sebuah perangkat keras adalah integrasi per deployment sementara mesin state adalah sifat aset.

Strukturnya memiliki dua bidang yang tidak berbagi permukaan izin. Pada bidang kriptografis, sebuah master vault memegang saldo di bawah kunci yang tidak pernah masuk ke proses agen. Darinya pemegang menerbitkan sebuah mandat berlingkup: kredensial bertanda tangan yang mengodekan plafon per transaksi, plafon periode bergulir, sebuah allowlist kontrak tujuan, masa berlaku, dan aset spesifiknya. Agen menerima kunci sesi yang wewenangnya persis mandat itu dan tidak lain. Agen dapat bertransaksi di dalam mandat sesering yang diinginkannya; agen tidak dapat mengubah mandat, karena perubahan memerlukan master key. Upaya melampaui sebuah plafon gagal pada verifikasi bukti, di mana tidak ada mesin kebijakan untuk dibantah. Pada bidang prosedural berada bahan-bahan yang lazim — instruksi sistem, guardrail, kode sekali pakai — dan pelajaran empirisnya adalah bahwa semua itu tetap bersifat anjuran terhadap seorang agen yang memiliki akses perkakas.

Tiga sifat membuat desain ini dapat digunakan alih-alih sekadar ketat. Mandat murah diterbitkan dan dapat dicabut dalam satu transaksi state publik, sehingga dugaan kompromi dijawab dengan pencabutan alih-alih rotasi kunci. Beberapa mandat dapat berjalan terhadap satu vault, memungkinkan pemegang memberikan wewenang yang terpisah dan tidak tumpang tindih kepada agen trading dan agen pengadaan. Dan pembelanjaan mandat diatestasi on-chain, sehingga pemegang dapat membuktikan kepada auditor atau pihak lawan apa yang diwewenangkan kepada seorang agen selama suatu jendela dan apa yang sebenarnya dilakukannya.



8.4 Bagaimana Pendapatan Komersial Mencapai Pasokan

Kedua layanan menghasilkan pendapatan, dan klaim protokol atas pendapatan itu adalah yang menghubungkannya dengan aset.

Biaya dinyatakan dalam mata uang yang digunakan pelanggan untuk menyelesaikan pembayaran — stablecoin atau fiat — karena perusahaan yang membeli layanan API tidak ingin memegang aset volatil untuk membayarnya. Pada penyelesaian, protokol mengonversi porsi tertentu dari pendapatan biaya bersih menjadi NKVR di pasar terbuka dan memusnahkannya. Pelanggan karena itu tidak pernah menyentuh NKVR, dan pasokan NKVR tetap berkurang oleh penggunaan mereka.

Konversi dijalankan menurut aturan yang dipublikasikan: porsi tertentu dari pendapatan biaya bersih dialirkan ke pembelian kembali, dengan sisanya mendanai operasi dan hibah. Pembagian itu adalah parameter tata kelola di dalam batas yang ditetapkan saat peluncuran, dan setiap pembelian kembali serta pemusnahan merupakan peristiwa on-chain dengan hash transaksi publik.

Dua komitmen menjaga ini tetap jujur. Tidak ada biaya perusahaan yang didenominasi dalam NKVR, sehingga harga bagi pelanggan tidak bergantung pada volatilitas pasar. Dan tidak ada kewajiban pembelian kembali yang ditetapkan secara absolut, sehingga kuartal pendapatan yang lemah mengurangi burn alih-alih menciptakan kewajiban yang harus didanai treasury dari cadangan.

Fase II mencakup Verify; Fase III mencakup Agent Shield dalam skala besar. Tidak satu pun merupakan bisnis Hari-1, dan nilai mekanismenya saat peluncuran bersifat struktural alih-alih numerik: aset memiliki saluran tertentu yang melaluinya permintaan eksternal mencapai pasokan, didefinisikan lebih dahulu dan dapat diaudit dalam eksekusinya.

9.0 Ekonomi Token NKVR: Kelangkaan yang Direkayasa dan Deflasi Dua Tahap

9.1 Lima Angka, Satu Identitas

Sebagian besar perselisihan tentang pasokan beredar suatu aset berasal dari pihak-pihak berbeda yang mengutip angka berbeda dengan itikad baik. Terdapat lima kuantitas yang berbeda, dan protokol memelihara kelimanya on-chain sehingga tidak satu pun memerlukan estimasi (Gambar 9.1).

Plafon genesis — 21.000.000 NKVR, diinstansiasi satu kali, tidak dapat diubah.

Cadangan yang belum dilepas — jumlah dari enam saldo vault pelepasan. Publik, dapat dikueri, dan terikat pada jadwal bytecode.

Kumulatif yang telah dilepas — plafon dikurangi cadangan yang belum dilepas. Angka ini hanya naik, pada laju yang ditetapkan lebih dahulu.

Di-stake — NKVR yang saat ini terikat ke Witness Network, termasuk stake dalam antrean unbonding. Terkunci, memperoleh bobot, terekspos pada slashing.

Float beredar — yang telah dilepas, dikurangi yang di-stake, dikurangi yang dibakar.

totalSupply pada rantai terbaca sebagai plafon genesis dikurangi burn kumulatif, dan tidak bergerak ketika sebuah vault membuka, karena unlocking adalah transfer alih-alih pencetakan. Pilihan desain tunggal itu menghapus sumber kebingungan paling umum dalam dasbor pasar, di mana sebuah unlock vesting tampak sebagai kenaikan pasokan.

Identitas yang menghubungkan kelimanya adalah:

$$\mathrm{Float}(t) = \mathrm{Released}(t) - \mathrm{Staked}(t) - \mathrm{Burned}(t)$$

dan plafon efektif adalah $21.000.000 - \mathrm{Burned}(t)$, secara ketat di bawah plafon yang dinyatakan untuk semua t setelah burn pertama.

Dua aturan struktural menutup trik akuntansi yang membuat angka float terbitan tidak dapat dipercaya di tempat lain. Cadangan yang belum dilepas tidak memenuhi syarat atas reward witness, sehingga alokasi tim, Foundation, dan pendukung awal tidak dapat memperoleh dari pool sebelum vesting. Dan unit yang dibakar keluar dari setiap kuantitas hilir: sebuah burn mengurangi totalSupply dan menurunkan plafon efektif tanpa pernah menyentuh saldo vault yang belum vesting, sehingga jadwalnya tetap valid terhadap basis yang telah dikurangi.

NKVR memiliki delapan angka desimal. Unit terkecil, $10^{-8}\mathrm{NKVR}$, adalah granularit as akuntansi untuk era ekor pool witness dan untuk note terlindung.



9.2 Alokasi Genesis

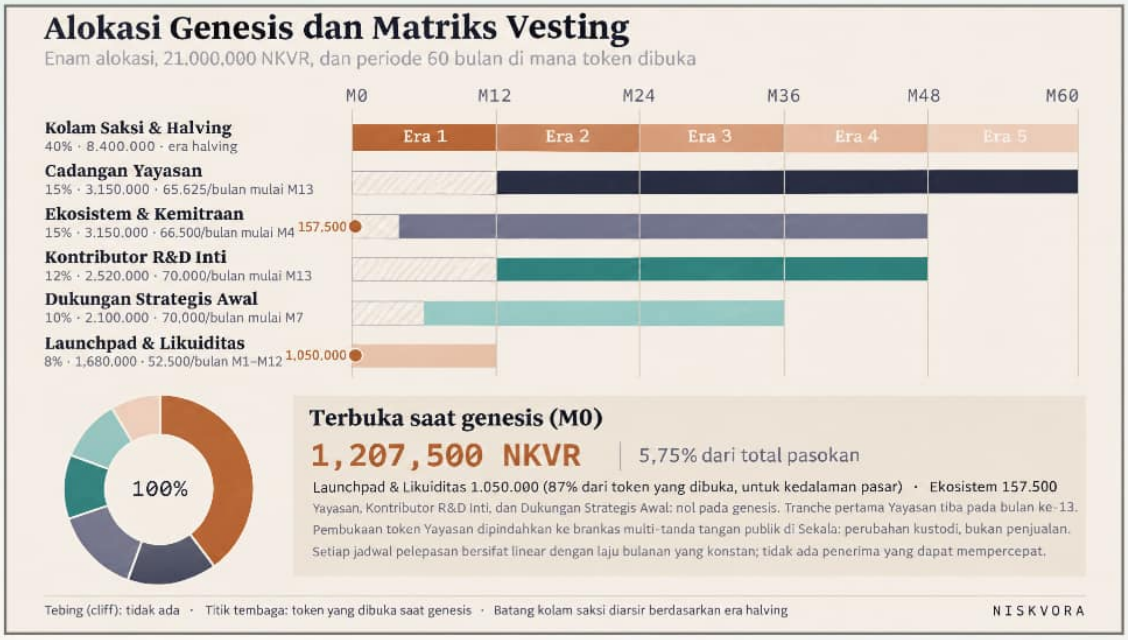
Enam alokasi, dengan total tepat 21.000.000 NKVR (Gambar 9.2).

Alokasi	Porsi	NKVR	Dibuka pada Genesis (M0)	Cliff	Pelepasan Linear & Laju Bulanan
1. Witness Network & Halving Pool	40%	8.400.000	0 (0,00%)	Tidak ada	Era halving 12 bulan (Era 1: 350.000/bln; Era 2: 175.000/bln…)
2. Cadangan Strategis Foundation	15%	3.150.000	0 (0,00%)	12 bulan (M1–M12)	48 bulan (M13–M60), **65.625 NKVR/bln**
3. Ekosistem & Kemitraan	15%	3.150.000	157.500 (0,75%)	3 bulan (M1–M3)	45 bulan (M4–M48), **66.500 NKVR/bln**
4. Kontributor R&D Inti	12%	2.520.000	0 (0,00%)	12 bulan (M1–M12)	36 bulan (M13–M48), **70.000 NKVR/bln**
5. Pendukung Strategis Awal	10%	2.100.000	0 (0,00%)	6 bulan (M1–M6)	30 bulan (M7–M36), **70.000 NKVR/bln**
6. Launchpad & Likuiditas Genesis	8%	1.680.000	1.050.000 (5,00%)	Tidak ada	12 bulan (M1–M12), **52.500 NKVR/bln**
Total	**100 %**	**21.000. 000**	**1.207.500 (5,75%)**	—	—

Yang penting dari tabel ini bukanlah persentasenya.

Float beredar pada blok genesis adalah 1.207.500 NKVR, atau 5,75% dari plafon, sebelum staking genesis apa pun; pengikatan pada epoch-epoch pertama menguranginya dari sana. Dari unlock awal itu, 87% (1.050.000 NKVR) merupakan alokasi launchpad dan likuiditas, yang keberadaannya untuk membangun kedalaman pasar alih-alih mendanai anggaran operasional. Ekosistem membuka 157.500 NKVR pada genesis dan tidak ada lagi selama tiga bulan. Foundation, kontributor inti, dan pendukung awal membuka nol pada genesis, dan tranche pertama Foundation yang terbuka tiba pada bulan ketiga belas.

Alokasi Foundation memerlukan ketepatan tentang apa arti unlocking. Dana berpindah dari vault pelepasan ke sebuah treasury multi-tanda tangan publik pada state *Sekala* — perubahan wewenang kustodi, bukan penjualan pasar otomatis. Setiap perpindahan keluar dari treasury tersebut adalah transaksi publik terhadap alamat yang dapat dipantau siapa pun secara berkelanjutan. Jadwal membatasi apa yang dapat diwewenangkan treasury dalam suatu periode, dan state publik memperlihatkan apa yang sebenarnya dibelanjakannya.

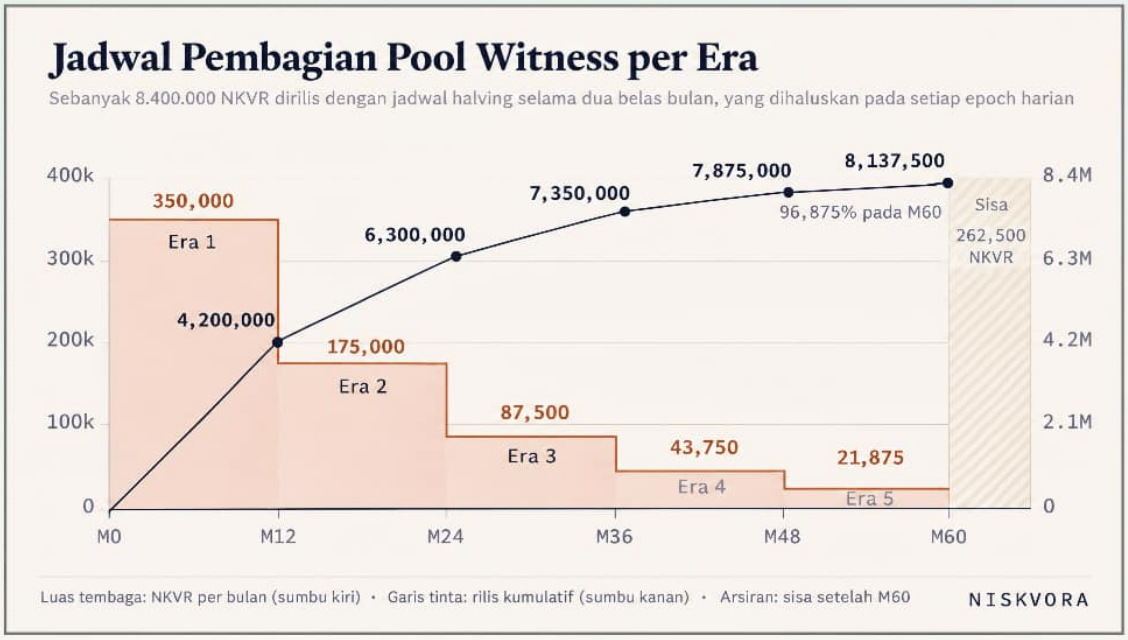


9.3 Era Halving dan Ketiadaan Lonjakan Cliff Dua Belas Bulan

Pool witness melepaskan pada era dua belas bulan, berkurang separuh setiap periode, dengan distribusi yang dihaluskan di seluruh epoch akuntansi harian.

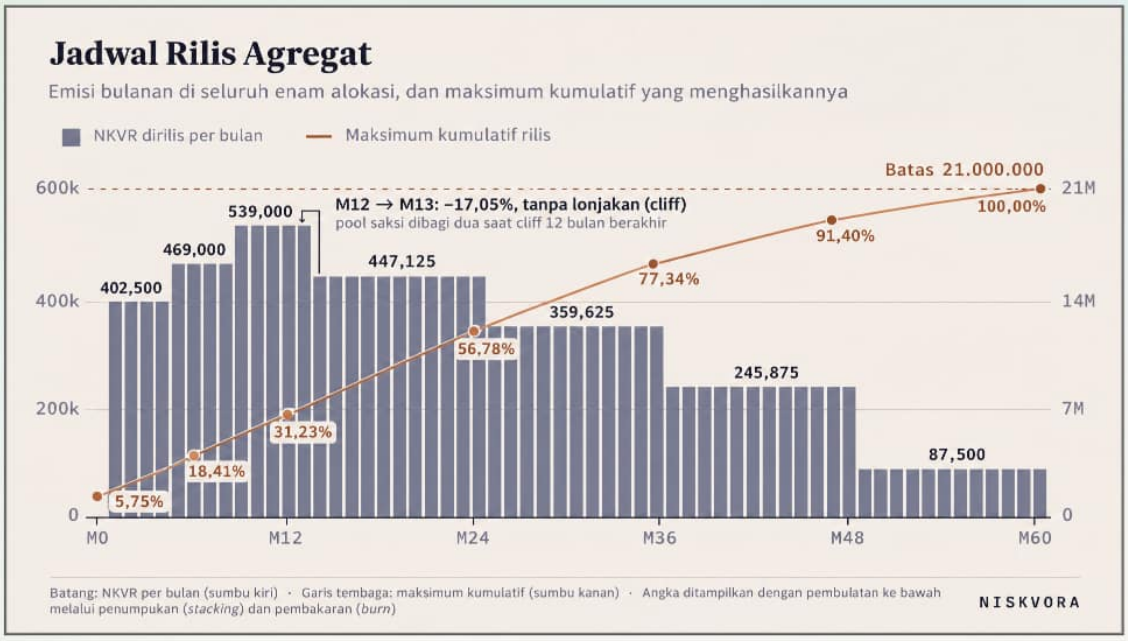
Era	Bulan Pasca-Genesis	Porsi Pool	Dilepas pada Era (NKVR)	Laju Bulanan (NKVR)
Era 1	M1–M12	50,000%	4.200.000	350.000
Era 2	M13–M24	25,000%	2.100.000	175.000
Era 3	M25–M36	12,500%	1.050.000	87.500
Era 4	M37–M48	6,250%	525.000	43.750
Era 5	M49–M60	3,125%	262.500	21.875
Ekor	M61+	3,125%	262.500 tersisa setelah Era 5	konvergen secara asimtotik

Deret geometri itu konvergen tepat ke 8.400.000 NKVR, dengan 96,875% pool witness dilepas pada bulan keenam puluh, dan suku ekor dipotong pada lantai presisi yang ditetapkan tata kelola begitu pelepasan bulanan turun di bawah biaya distribusi.



Mengagregasikan keenam alokasi menghasilkan kurva pelepasan agregat dengan penyeimbang struktural yang disengaja. Total pelepasan bulanan memuncak pada bulan ketujuh hingga kedua belas, pada 539.000 NKVR per bulan, lalu menurun pada setiap pita berikutnya — 447.125 (M13–M24), 359.625 (M25–M36), 245.875 (M37–M48), dan 87.500 (M49–M60). Puncak itu memang mengikuti sebuah cliff, yaitu cliff enam bulan milik pendukung awal. Klaim yang layak diajukan lebih sempit dan tetap berlaku: pada bulan ketiga belas, ketika cliff dua belas bulan kontributor R&D inti dan Foundation berakhir bersamaan, pelepasan bulanan agregat turun sebesar 17,05% (dari 539.000 menjadi 447.125 NKVR) alih-alih melonjak, karena rilis pool witness berkurang separuh, turun 175.000 per bulan pada langkah yang sama dan alokasi likuiditas launchpad telah selesai dilepas.

Pelepasan maksimum kumulatif pada titik pemeriksaan standar berjalan 1.207.500 NKVR (5,75%) pada M0, 3.822.000 (18,20%) pada M6, 7.056.000 (33,60%) pada M12, 12.421.500 (59,15%) pada M24, 16.737.000 (79,70%) pada M36, 19.687.500 (93,75%) pada M48, dan 20.737.500 (98,75%) pada M60. Ini adalah plafon alih-alih prakiraan: angka-angka tersebut mengasumsikan setiap vault melepas sesuai jadwal dan tidak ada yang di-stake atau dibakar, sedangkan float beredar pada momen mana pun lebih rendah oleh kedua kuantitas tersebut.



9.4 Disiplin Float

Jadwal pelepasan memberi tahu Anda apa yang dapat dijual (Gambar 9.4). Ia tidak memberi tahu apa yang akan dijual, dan selisih itulah tempat sebagian besar struktur token gagal.

Empat komitmen menyentuh selisih tersebut.

Tidak ada imbal hasil yang dijanjikan. Reward staking berasal dari pool tetap pada jadwal tetap. Reward itu bukan bunga, tidak dijamin, dan menurun separuh setiap dua belas bulan secara konstruksi. Pemegang yang melakukan staking mengambil posisi operasional dalam keamanan jaringan dengan eksposur slashing, bukan membeli produk simpanan.

Tidak ada utang yang diciptakan. Protokol tidak memiliki kewajiban untuk membeli kembali pada suatu harga, tidak ada hak penebusan, dan tidak ada komitmen treasury yang didenominasi dalam fiat. Emisi adalah transfer aset yang sudah dipegang protokol, sehingga penurunan harga mengurangi nilai yang didistribusikan dan tidak menciptakan klaim terhadap cadangan. Inilah sebabnya mekanisme ini tidak memiliki jalur spiral kematian: tidak ada kewajiban tetap yang harus dilayani.

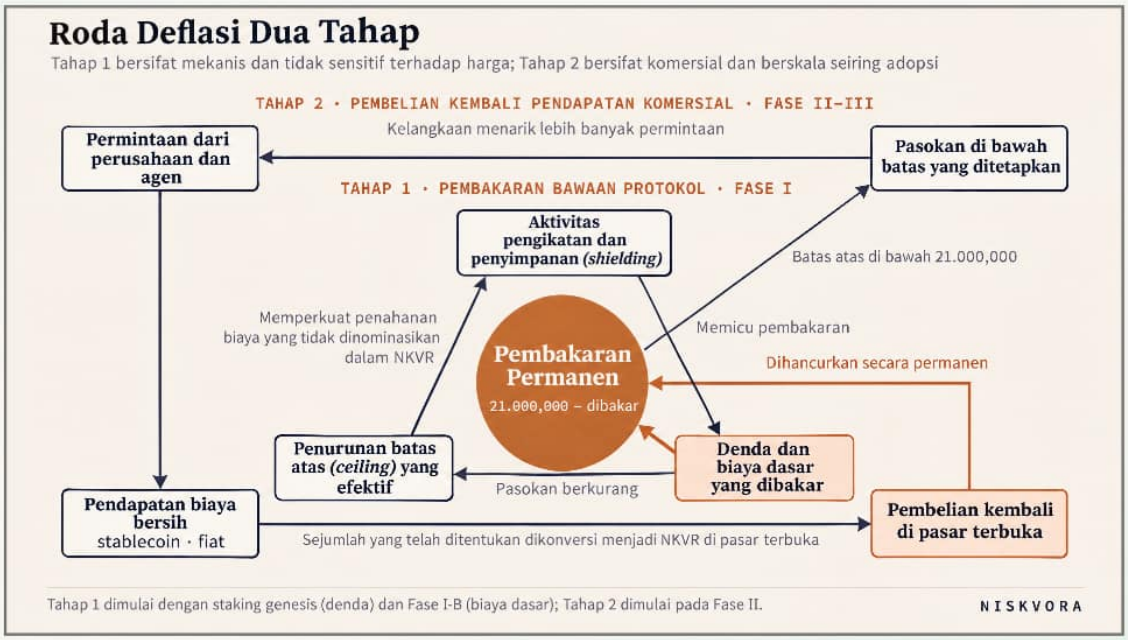
Vesting dibatasi pada laju, bukan hanya pada total. Setiap jadwal linear di Bagian 9.2 melepaskan pada laju bulanan yang konstan, yang berarti seorang penerima tidak dapat mempercepat atas pilihannya. Satu-satunya diskresi adalah apakah akan menjual, dan state publik membuat transfer itu terlihat ketika mereka melakukannya.

Treasury Foundation dibatasi pada laju dan diungkapkan sepenuhnya. Arus masuk bulanannya tetap, kepemilikannya berada pada alamat yang dapat diamati publik, dan arus keluarnya dapat dilacak. Tidak ada alokasi lain yang membawa kewajiban pengungkapan yang sebanding, dan tidak ada yang perlu, karena yang lain milik pihak privat.

Yang tidak dilakukan struktur ini adalah mencegah seorang pemegang besar menjual. Tidak ada yang dapat mencegahnya. Kontribusi strukturnya adalah bahwa pasar dapat mengamati penjualan itu saat terjadi dan memberinya harga, alih-alih menemukannya dalam laporan kuartalan.

9.5 Dua Tahap Pemusnahan

Pengurangan pasokan berjalan pada dua mekanisme dengan kondisi aktivasi yang berbeda.



Tahap 1: Burn Mekanisme Native Protokol (Fase I). Dua sumber, keduanya didenominasi dalam NKVR dan keduanya dimusnahkan alih-alih didistribusikan ulang.

Burn penalti unbonding dini. Delegator yang keluar sebelum horizon yang dikomitmenkan membayar penalti yang proporsional dengan sisa waktu, dieksekusi oleh kontrak staking terhadap NKVR yang terikat. Ini dimulai ketika delegasi dibuka pada Fase I-A, yang berarti protokol memiliki mekanisme pemusnahan yang aktif dan dapat diverifikasi publik pada lapisan penyelesaian sebelum aktivasi pool terlindung pada Fase I-B. Volumenya bergantung pada perilaku pemegang dan tidak dapat diramalkan secara presisi; pada jaringan yang stabil volume itu mungkin kecil, dan signifikansi mekanismenya adalah bahwa ia tanpa syarat dan aktif sejak staking genesis.

Burn biaya dasar transisi state turnstile. Masuk ke dan keluar dari pool terlindung membebankan jumlah nominal NKVR yang tetap dan dimusnahkan saat eksekusi. Diaktifkan bersamaan dengan lapisan terlindung pada Fase I-B.

Tahap 2: Pembelian Kembali dan Burn dari Pendapatan Komersial (Fase II–III). Porsi tertentu dari pendapatan bersih Niskvora Verify dan Agent Shield dikonversi menjadi NKVR di pasar terbuka dan dimusnahkan secara permanen. Aktif sejak Fase II, berukuran menurut pendapatan komersial eksternal, dan dibatasi oleh aturan pembagian yang diuraikan di Bagian 8.4.

Perbedaan yang penting bagi siapa pun yang memodelkan pasokan adalah bahwa Tahap 1 bersifat mekanis dan tidak peka harga, sementara Tahap 2 bersifat komersial dan berskala dengan adopsi. Tahap 1 menyediakan lantai pemusnahan struktural yang segera. Tahap 2 menyediakan komponen terkait pertumbuhan yang berskala independen dari emisi token. Tidak satu pun merupakan prakiraan, dan menyajikan angka burn kumulatif yang diproyeksikan berarti mengarang angka yang tidak dikomitmenkan oleh protokol.

Gambar 9.5_2 memplot kurva pelepasan deterministik terhadap sebuah pita burn ilustratif untuk menunjukkan satu hal tentang arah: plafon pasokan efektif ($21.000.000 - \mathrm{Burned}(t)$) menurun monoton sejak peristiwa burn pertama, dan pasokan beredar berkontraksi secara neto setiap kali pemusnahan marginal ditambah staking neto melampaui laju pelepasan marginal yang menurun.



10.0 Tata Kelola Dua Lapis dan Kepengurusan Institusional

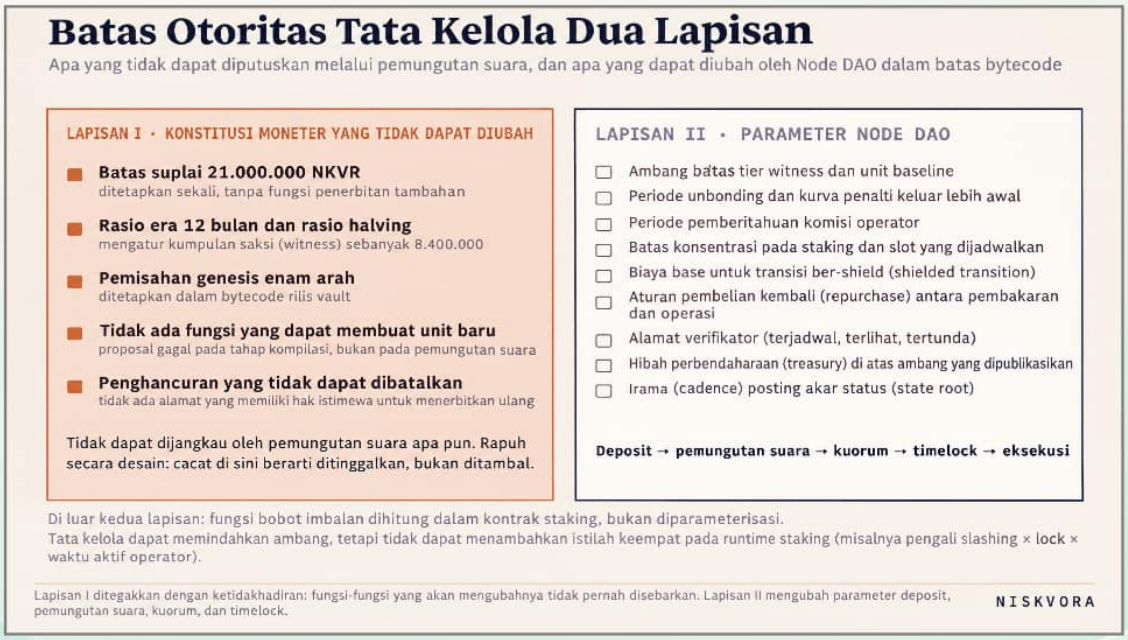
10.1 Lapisan I: Konstitusi Tanpa Teks

Konstitusi moneter bukanlah dokumen yang telah disepakati untuk dihormati oleh tata kelola. Ia adalah seperangkat sifat yang tidak dapat dijangkau oleh transaksi tata kelola mana pun, karena fungsi yang akan mengubahnya tidak pernah dideploy (Gambar 10.1).

Ada lima sifat tersebut. Plafon 21.000.000 NKVR. Panjang era dua belas bulan dan rasio halving yang mengatur alokasi 8.400.000 milik pool witness. Pembagian enam arah alokasi genesis, yang ditetapkan pada saat deployment dalam bytecode vault pelepasan itu sendiri. Ketiadaan fungsi apa pun yang menciptakan unit. Dan ireversibilitas pemusnahan, dalam pengertian bahwa tidak ada alamat yang memegang hak istimewa untuk menerbitkan ulang dari sebuah burn.

Sebuah proposal yang mencoba mengubah salah satunya tidak akan gagal pada pemungutan suara. Ia akan gagal pada kompilasi, karena tidak ada titik masuk yang dapat dipanggil. Ini adalah jaminan yang lebih kuat daripada persyaratan supermayoritas, dan ia juga lebih rapuh dalam satu hal yang spesifik: sebuah cacat pada kontrak aset tidak dapat ditambal, hanya ditinggalkan. Protokol menerima kompromi itu karena alternatifnya — sebuah jalur peningkatan pada logika pasokan — menghadirkan kembali justru diskresi yang keberadaan plafon dimaksudkan untuk dihapus.

Yang dengan sengaja ditinggalkan oleh konstitusi di luar dirinya adalah alamat verifier. Sistem pembuktian membaik, asumsi menua, dan sebuah aset moneter yang tidak pernah dapat mengganti verifiernya pada akhirnya akan diamankan oleh kriptografi yang usang. Mengganti verifier karena itu merupakan tindakan Lapisan II, yang dibatasi oleh proses pada subbagian berikutnya.



10.2 Lapisan II: Apa yang Sesungguhnya Dapat Diubah oleh Suara

Node DAO mengatur parameter, bukan prinsip. Lingkupnya terbatas dan batasnya ditegakkan oleh ketiadaan kode yang sama yang melindungi konstitusi.

Dalam lingkup: ambang tingkat witness dan unit baseline-nya, periode unbonding dan kurva penalti keluar dini, periode pemberitahuan komisi operator, plafon konsentrasi atas stake terdelegasi dan slot terjadwal, biaya dasar transisi terlindung, pembagian pembelian kembali antara burn dan operasi, alamat verifier, alokasi hibah dari treasury Foundation, dan irama state root.

Di luar lingkup: segala sesuatu di Bagian 10.1, ditambah perubahan apa pun pada komposisi tiga suku dari fungsi bobot reward. Tata kelola dapat menggeser sebuah ambang. Tata kelola tidak dapat menambah suku keempat, karena logika pembobotan dihitung dalam kontrak staking alih-alih diparameterkan.

Prosesnya sengaja dibuat lambat (Gambar 10.2). Sebuah proposal memerlukan deposit, yang dihitung agar spam menjadi mahal tanpa menjadikan partisipasi sebagai syarat modal bagi pemegang kecil. Pemungutan suara berlangsung selama jendela tetap yang cukup panjang untuk mencakup pemegang yang memeriksa mingguan alih-alih setiap jam. Pelulusan memerlukan kuorum yang diukur terhadap stake yang berpartisipasi sekaligus mayoritas suara yang diberikan, dengan ambang kuorum ditetapkan cukup tinggi sehingga minoritas yang gigih tidak dapat meloloskan suatu perubahan pada periode sepi.

Eksekusi menunggu di balik timelock dengan durasi yang substansial. Pemegang yang tidak setuju dengan proposal yang lolos memiliki jendela itu untuk melakukan unbonding, membongkar posisi, atau keluar sepenuhnya sebelum perubahan berlaku. Timelock adalah yang mengubah tata kelola dari mekanisme yang mengikat pemegang menjadi mekanisme yang dapat mereka respons.

Dua kelemahan perlu disebutkan. Bobot suara berasal dari jumlah stake, pengali lock, dan uptime — tiga suku yang sama yang menentukan reward — yang berarti operator besar mengakumulasi pengaruh sebanding dengan bobot ekonominya. Plafon bobot suara per entitas membatasi pemegang terbesar, dan delegator mempertahankan kemampuan untuk mengarahkan suaranya sendiri secara independen dari operator tempat ia melakukan staking, tetapi tidak satu pun langkah itu menghapus kecenderungan sistem berbobot stake untuk mengikuti stake.

Kelemahan kedua adalah ketiadaan jalur peningkatan darurat. Sebuah kerentanan kritis yang ditemukan pada verifier harus menjalani seluruh urutan proposal, pemungutan suara, dan timelock, dan selama itu sistem yang terdampak tetap aktif. Kekuasaan darurat yang diotorisasi lebih dahulu akan mempersingkat jendela itu dan sekaligus memberikan kepada sekelompok kecil kemampuan mengubah perilaku protokol tanpa pemberitahuan. Desain memilih jalur yang lebih lambat dan mengompensasinya dengan menjaga permukaan yang dapat dijeda tetap kecil: turnstile tidak mengekspos fungsi pause, sehingga bahkan sebuah kegagalan tata kelola tidak dapat membekukan saldo terlindung.



10.3 Dua Entitas dan Sebuah Praktik Anonimitas

Kepengurusan dibagi antara sebuah yayasan berbadan hukum dan sebuah kolektif rekayasa, dengan akuntabilitas yang berbeda melekat pada masing-masing.

The Niskvora Foundation didirikan sebagai entitas kepengurusan nirlaba independen di sebuah yurisdiksi yayasan common-law dan memegang cadangan strategis serta alokasi ekosistem. Foundation menjalankan distribusi genesis di bawah dokumentasi hukum terpisah, dan merupakan entitas tempat mitra koridor berkontrak, bertanggung jawab atas hibah, integrasi institusional, dan keterlibatan regulasi bila berlaku. Mandatnya bersifat institusional dalam pengertian biasa: pelaporan cadangan berkala, kebijakan treasury yang dipublikasikan, dan antarmuka hukum formal bagi pihak lawan institusional.

The Niskvora Cryptography Collective adalah kelompok rekayasa protokol, yang menyatukan kontributor di bidang kriptografi zero-knowledge terapan, rekayasa penyelesaian terdistribusi, dan mikrostruktur pasar kuantitatif. Para kontributornya bersifat pseudonim di depan publik, yang merupakan pilihan sengaja dengan biaya sekaligus manfaat. Karya fondasional di bidang ini dihasilkan di bawah praktik yang sama, dan praktik itu tetap dapat dipertahankan bagi siapa pun yang keterlibatannya dalam sebuah protokol privasi menciptakan eksposur pribadi di yurisdiksi asalnya. Biayanya nyata: sebuah tim pseudonim tidak dapat diuji tuntas seperti tim yang bernama, dan tidak ada ketelitian kriptografis yang dapat menggantikan pengetahuan tentang siapa yang membangun sistem tersebut.

Substitusi yang ditawarkan protokol sebagai pengganti kultus individu bersifat institusional dan dapat diverifikasi, dan layak dinyatakan secara eksplisit bahwa itu adalah substitusi alih-alih ekuivalen. Di bawah gerbang rilis yang didefinisikan di Bagian 11.4, Fase I-A mensyaratkan kode sumber kontrak yang deterministik dan

terverifikasi publik pada penjelajah lapisan penyelesaian, didukung oleh verifikasi invarian pra-deployment sebelum genesis, sementara Fase I-B dan fase-fase berikutnya mensyaratkan tinjauan keamanan kriptografis dan kontrak pintar independen yang telah selesai — mencakup verifier terlindung, sirkuit pembuktian, dan invarian konservasi turnstile — yang dipublikasikan bersama temuan yang telah diselesaikan sebelum vault terenkripsi diaktifkan. Program bug bounty berkelanjutan didanai dari alokasi ekosistem dengan hadiah yang berskala sesuai tingkat keparahan saat kontrak produksi aktif, dan setiap kontributor yang memegang wewenang rilis terikat pada kebijakan konflik kepentingan yang melarang pekerjaan bersamaan yang tidak diungkapkan pada protokol pesaing.

Tidak satu pun dari itu merupakan verifikasi karakter. Itu adalah verifikasi atas keluaran dan batasan yang terkunci dalam kode, yang merupakan hal yang sesungguhnya dapat ditawarkan oleh sebuah protokol terbuka.

10.4 Cadangan Hidup di Ruang Publik

Cadangan strategis Foundation sepenuhnya dipegang pada state *Sekala*. Bukan sebagian darinya, dan bukan dengan pengecualian demi kenyamanan operasional. Alamatnya dipublikasikan, saldonya dapat dikueri kapan saja oleh siapa pun, dan setiap arus keluar adalah transaksi terlihat terhadap jadwal yang membatasi maksimumnya.

Pengaturan penandatanganan adalah sebuah kumpulan multi-tanda tangan dengan ambang yang cukup tinggi sehingga tidak ada kunci tunggal yang terkompromi dapat memindahkan dana, dan didistribusikan di antara pihak-pihak yang tidak berbagi satu ketergantungan yurisdiksional atau organisasional. Penandatangan diungkapkan sejauh keamanan mereka sendiri memungkinkan, dan kumpulan alamatnya bersifat publik sehingga perubahan penandatangan dapat diamati sebagai sebuah perubahan.

Dua komitmen lanjutan menutup celah yang jelas. Foundation tidak memegang saldo terlindung, yang berarti tidak ada dalam kepemilikannya yang dapat dipindahkan di luar pandangan publik. Dan Foundation tidak melakukan staking atas cadangan yang belum dilepas, konsisten dengan larangan di Bagian 9.1, sehingga alokasinya tidak dapat memperoleh dari pool witness sebelum unit tersebut vesting.

Hibah dari treasury di atas ambang operasional yang dipublikasikan mengikuti jalur yang sama dengan tindakan Lapisan II lainnya (Gambar 10.2): proposal, pemungutan suara, timelock, eksekusi, masing-masing dengan rujukan publik. Pembelanjaan di bawah ambang tetap terlihat publik on-chain — lebih cepat dalam eksekusi, identik dalam transparansi.

Publikasi runway adalah bagian terakhir. Sebuah laporan berkala tentang komposisi cadangan dan horizon operasional yang diproyeksikan memungkinkan pemegang menilai apakah treasury dikonsumsi pada laju yang berkelanjutan, yang merupakan pertanyaan yang tidak dapat dijawab oleh saldo publik semata.

11.0 Akses Pasar Genesis, Integritas Pasar, dan Peta Jalan

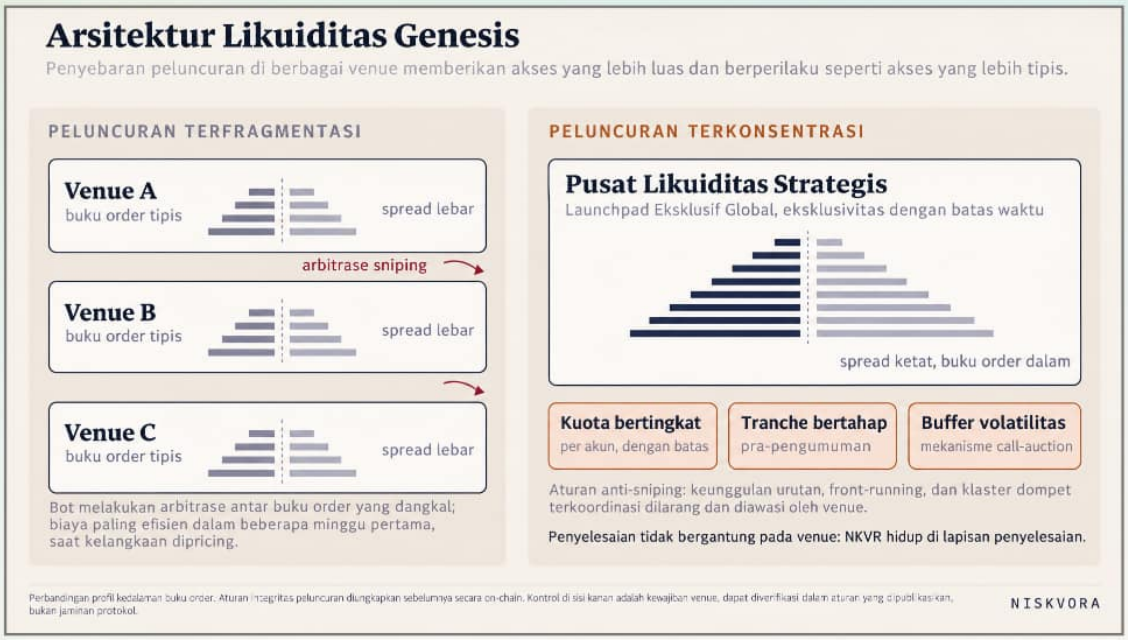
11.1 Alasan untuk Satu Venue saat Peluncuran

Peluncuran yang tersebar di banyak venue tampak seperti akses yang lebih luas dan berperilaku sebagai akses yang lebih tipis (Gambar 11.1). Setiap venue memecah buku order, masing-masing memelihara pengaturan market maker-nya sendiri, dan penemuan harga yang akan dihasilkan oleh satu buku yang dalam digantikan oleh arbitrase di antara buku-buku yang tipis. Bagi aset yang seluruh premisnya adalah kelangkaan, minggu-minggu pertama perdagangan adalah momen yang paling tidak efisien dan momen di mana fragmentasi paling mahal.

Memusatkan likuiditas genesis pada satu mitra strategis adalah pilihan yang disengaja. Aktivasi distribusi genesis diatur secara ketat oleh selesainya gerbang keamanan dan kesiapan operasional Fase I-A alih-alih oleh tanggal kalender yang tetap. Mitra tersebut ditetapkan sebagai Global Exclusive Launchpad and Strategic Liquidity Partner, dan pengaturannya membawa kewajiban di kedua arah: penyediaan kedalaman pada spread yang ditetapkan selama jendela peluncuran, larangan mengubah persyaratan pencatatan atau perdagangan tanpa pemberitahuan, dan antarmuka rekonsiliasi yang memungkinkan akuntansi publik protokol tetap dapat diverifikasi.

Argumen lawannya layak dinyatakan. Satu venue adalah satu titik kegagalan — operasional dan yurisdiksional. Sebuah venue yang menghentikan penarikan, kehilangan lisensinya, atau terkena tindakan di yurisdiksi asalnya akan membawa serta pasar likuid utamanya. Tiga hal membatasi eksposur itu. Eksklusivitas dibatasi waktu alih-alih abadi, dengan jendela yang terdefinisi setelahnya venue tambahan dapat diterima. Penyelesaian tidak bergantung pada venue, karena NKVR adalah aset pada rantai yang mapan dan venue adalah venue dalam pengertian biasa, bukan kustodian ledger aset. Dan pengaturannya bersifat kontraktual, sehingga pelanggaran atas kewajiban kedalaman atau pemberitahuan memiliki pemulihan yang tidak memerlukan tata kelola untuk bertindak.

Pembingkaian kelangkaan atas Genesis Exclusivity Window ini bersifat mekanis alih-alih retoris. Sebelum era halving pertama selesai, pool witness melepaskan pada maksimum Era 1 dan belum ada batas era yang memangkasnya separuh. Jendela itu adalah satu-satunya periode di mana penerbitan witness protokol berjalan pada laju awalnya, dan ia berhingga secara konstruksi.



11.2 Aturan Integritas sebagai Perlindungan Pemegang

Keputusan struktur pasar yang diambil dengan buruk pada sembilan puluh hari pertama sulit dibalik sesudahnya, karena peserta yang ditariknya menentukan nada bagi siapa yang datang berikutnya.

Empat kontrol beroperasi selama jendela genesis (Gambar 11.1), semuanya berada dalam kerangka peluncuran mitra dan diungkapkan kepada peserta lebih dahulu.

Kuota pemesanan bertingkat dan dibatasi per akun, dengan verifikasi identitas di mana lisensi mitra mensyaratkannya. Tujuannya adalah mencegah seorang pembeli besar tunggal menyerap seluruh tranche genesis pada harga penawaran, yang jika tidak demikian akan membuat pasar publik dimulai dari posisi konsentrasi maksimum.

Penawaran launchpad genesis dilakukan melalui tranche pemesanan yang transparan dan diumumkan sebelumnya, bukan melalui satu kali rilis tanpa jadwal, sementara kedalaman pembuatan pasar pasca-genesis terbuka secara ketat mengikuti jadwal linear dua belas bulan yang ditetapkan di Bagian 9.2. Saldo state publik yang telah diselesaikan dan belum terikat tidak membawa lockup protokol yang tidak diungkapkan di luar persyaratan tranche yang dipublikasikan, sehingga pembentukan likuiditas tetap tertib sejalan dengan hak transfer pemegang yang berlaku umum.

Pemutus sirkuit buku order otomatis untuk sementara mengalihkan pencocokan berkelanjutan ke penemuan harga call auction ketika pergerakan melampaui pita yang ditetapkan, di bawah prosedur pemulihan yang dipublikasikan. Beroperasi secara ketat pada pencocokan order venue tanpa mengubah keterpindahtanganan token pada tingkat protokol maupun penarikan standar yang sesuai ketentuan, mekanisme ini meredam kaskade likuidasi yang tidak tertib selama penemuan harga awal.

Ketentuan anti-sniping menjawab kerentanan spesifik dari sebuah pencatatan baru. Keunggulan pengurutan transaksi yang dimiliki penyedia infrastruktur, front-running otomatis atas order awal, dan klaster dompet terkoordinasi yang dirancang untuk menciptakan permintaan artifisial dilarang, dengan deteksi dan penegakan ditangani oleh mitra di bawah aturan integritas pasarnya sendiri.

Ini adalah kewajiban pada venue, bukan pada protokol, dan protokol tidak dapat menegakkannya dalam bytecode. Dinyatakan secara terus terang: pemegang sebaiknya memperlakukannya sebagai komitmen operasional venue, yang dapat diverifikasi dalam aturan venue yang dipublikasikan dan dalam perilaku pasar yang teramati, alih-alih sebagai jaminan matematis yang disediakan oleh protokol.

11.3 Supernode Percontohan Asia-Pasifik dan Peluncuran Koridor Global

Ekspansi regional berjalan melalui struktur supernode, di mana operator yang ditetapkan di setiap koridor menyediakan kapasitas pembuktian lokal, dokumentasi berbahasa lokal, dan pekerjaan integrasi yang menghubungkan pemegang di pasar tersebut ke gateway resmi.

Urutan koridor ditetapkan oleh ketersediaan lisensi dan oleh permintaan yang terbukti, bukan oleh ukuran pasar semata. Sebuah koridor di mana tidak ada gateway yang dapat beroperasi di bawah kerangka yang jelas belum siap, terlepas dari seberapa besar minat yang ada di dalamnya. Di mana kerangkanya jelas, tiga kondisi menentukan prioritas: basis ritel yang ada cukup besar sehingga biaya edukasi diamortisasi di atasnya, motif perlindungan tabungan yang terbukti alih-alih motif murni spekulatif, dan rel perbankan serta pembayaran lokal yang dapat diintegrasikan oleh gateway.

Sinyal terkuat saat ini datang dari ekonomi digital bertumbuh tinggi di kawasan Asia-Pasifik, Amerika Latin, dan koridor tabungan berkembang yang sebanding, di mana adopsi kripto ritel mencapai puluhan juta, mata uang domestik menghadapi tekanan depresiasi struktural terhadap patokan keras, dan preferensi rumah tangga atas aset langka yang mempertahankan daya beli merupakan perilaku yang bertahan alih-alih siklus sesaat. Regulator di seluruh koridor ini telah bergerak menuju pengawasan formal atas venue aset digital, sementara statuta perlindungan data yang baru dapat ditegakkan telah menjadikan kerahasiaan pribadi dan komersial sebagai prioritas operasional yang mendesak. Motif perlindungan tabungan menghasilkan pemegang yang mengakumulasi dan melakukan staking alih-alih berpindah-pindah, membentuk basis supernode jangkar bagi ekspansi global.

Kewajiban supernode bersifat substantif alih-alih simbolis. Seorang operator yang ditetapkan berkomitmen pada program hibah regional yang mendanai pengembang independen dan pada upaya edukasi berbahasa lokal, memelihara standar ketersediaan yang melekat pada tingkatnya, dan beroperasi di bawah

lisensi atau registrasi apa pun yang disyaratkan oleh koridor. Witness Network adalah saluran partisipasinya: pemegang yang ingin berkontribusi tanpa perangkat keras menjangkau gateway resmi, mendelegasikan stake, dan memperoleh dari pool halving tanpa menjalankan prover.

Satu batas berlaku sepanjang waktu. Karakterisasi hukum NKVR di suatu koridor ditentukan oleh otoritas koridor tersebut, dan protokol tidak membuat representasi apa pun tentangnya. Di mana klasifikasinya tidak pasti, koridor dilayani melalui gateway yang beroperasi di bawah izin yang mereka miliki, atau tidak dilayani sama sekali.

11.4 Peta Jalan: Gerbang alih-alih Tanggal

Peta jalan disusun di sekitar gerbang rekayasa dan adopsi alih-alih komitmen kalender, karena sebuah tanggal yang dipublikasikan untuk memenuhi ekspektasi pemasaran berubah menjadi janji yang tidak boleh dipaksakan untuk ditepati oleh rekayasa keamanan.

Fase I-A — Aset Kanonis, Likuiditas Genesis, dan Staking Bootstrap Keamanan. Setelah verifikasi invarian pra-deployment dan verifikasi kode sumber deterministik atas kontrak publik inti pada penjelajah lapisan penyelesaian, deployment kontrak aset 21.000.000 NKVR yang tidak dapat diubah, vault pelepasan berbasis bytecode, likuiditas genesis terkonsentrasi bersama mitra launchpad yang ditetapkan, delegasi witness yang dirutekan melalui gateway, distribusi reward Era 1, dan burn penalti unbonding dini Tahap 1, seiring dengan benchmark canary atas sirkuit pembuktian Niskala oleh operator genesis. *Gerbang ke Fase I-B:* stake witness yang telah terikat sebelumnya mencapai ambang keamanan target, operasi state publik yang berkelanjutan tanpa insiden, dan selesainya tinjauan keamanan independen atas sirkuit pembuktian Niskala, kontrak verifier, dan invarian konservasi Supply Turnstile dengan seluruh temuan berkeparahan tinggi telah diselesaikan.

Fase I-B — Vault Terlindung Niskala dan Supply Turnstile. Aktivasi lapisan terlindung zero-knowledge modular, Supply Turnstile dengan penghitung publik, viewing key granular, bukti eksklusi ZK-PoI di sisi klien, jalan keluar publik tanpa izin, dan burn biaya dasar transisi state turnstile. *Gerbang ke Fase II:* pengiriman state root yang berkelanjutan tanpa insiden, kinerja penemuan note sisi klien yang terverifikasi pada skala, dan tinjauan keamanan atas templat atestasi zkTLS serta registri verifier.

Fase II — Pilot Perusahaan Niskvora Verify. Peluncuran templat atestasi tanpa liabilitas data zkTLS untuk kelayakan perusahaan dan verifikasi pendapatan pedagang, yang memulai pembelian kembali dan burn pendapatan pasar terbuka Tahap 2. *Gerbang ke Fase III:* konversi pilot perusahaan menjadi kontrak komersial berulang yang menghasilkan arus pembelian kembali Tahap 2 yang stabil, ditambah audit verifikasi atas sirkuit mandat Agent Shield yang telah selesai.

Fase III — Agent Shield dan Skala Lintas Ekosistem. Deployment mainnet master vault yang dibatasi secara kriptografis dan mandat sesi berlingkup untuk agen otonom yang menyelesaikan transaksi melalui rel pembayaran mesin (x402, AP2), seiring dengan perluasan supernode koridor global.

Urutannya membawa informasi. Inti moneter publik selesai dan teraudit sebelum nilai terenkripsi mana pun ada, yang berarti hal pertama yang dapat diverifikasi pemegang adalah hal yang paling penting: bahwa plafon tetap, bahwa vault berada di tempat yang dinyatakan whitepaper, dan bahwa burn-nya on-chain. Setiap fase berikutnya mengaktifkan sebuah kapabilitas di atas basis yang sudah beroperasi di pandangan publik.



12.0 Pengungkapan Risiko dan Sikap Regulasi

12.1 Apa Itu NKVR, dan Apa yang Bukan

NKVR adalah aset kripto langka yang dipegang sebagai penyimpan nilai, dan agunan yang diikatkan (bonded) ke Witness Network untuk mengamankan verifikasi bukti. Hanya dua fungsi itulah yang diklaim protokol untuknya.

NKVR bukan alat pembayaran yang sah, bukan klaim atas mata uang negara mana pun, bukan stablecoin, dan tidak dirancang atau dipasarkan untuk pembayaran ritel harian. Tidak ada penerbit yang berdiri di belakangnya, tidak ada hak penebusan yang melekat padanya, dan tidak ada entitas yang wajib menerimanya dalam penyelesaian. NKVR bukan efek, saham, unit dalam skema investasi kolektif, atau instrumen yang membawa hak apa pun atas pendapatan, hak tata kelola atas

badan hukum, atau distribusi keuntungan. Memegang NKVR memberikan kemampuan untuk memegang dan memindahkan nilai di antara state-state protokol dan untuk berpartisipasi dalam pemungutan suara parameter Node DAO ketika di-stake; tidak lebih, dan tidak ada yang telah dikonfirmasi oleh otoritas mana pun dalam bentuk klasifikasi menyeluruh.

Bagian ini menyatakan posisi yang diambil protokol. Bagian ini tidak dapat menyatakan apa yang akan disimpulkan regulator, dan pembaca tidak boleh memperlakukan bagian mana pun dari whitepaper ini sebagai penetapan status hukum di yurisdiksi mereka sendiri.

12.2 Risiko yang Penting

Risiko kriptografis dan sistem pembuktian. Kesahihan lapisan terlindung bermuara pada tingkat kesulitan asumsi logaritma diskret (discrete-logarithm), ketahanan tumbukan dari hash komitmen, dan parameter konkret dari akumulasi rekursif serta transformasi Fiat–Shamir sistem pembuktian transparan. Pematahan salah satunya dapat memungkinkan nilai dipalsukan di dalam pool terlindung, dibatasi oleh saldo publik pool pada saat itu. Konstruksi saat ini tidak aman pasca-kuantum, dan jalur migrasi yang diuraikan di Bagian 5.6 membawa biaya substansial dalam ukuran bukti dan overhead verifikasi.

Risiko kontrak dan implementasi. Kontrak aset, vault pelepasan, logika staking, dan kontrak verifikasi adalah perangkat lunak. Komponennya menjalani verifikasi bytecode publik, pengujian invarian otomatis, dan tinjauan keamanan independen bergerbang fase saat modul kriptografis yang kompleks diaktifkan; tidak satu pun dari langkah itu menjamin tidak adanya cacat. Sebuah cacat pada logika staking dapat salah mencatat reward; sebuah cacat pada verifier dapat menerima root yang tidak valid. Tidak ada pengaturan asuransi yang menutup kerugian ini.

Risiko kustodi kunci. Saldo terlindung hanya dapat dipulihkan melalui spending key pemegang. Tidak ada mekanisme pemulihan, tidak ada modul pemulihan sosial, dan tidak ada administrator dengan wewenang override. Kunci yang hilang berarti dana yang hilang, secara permanen. Kunci yang terkompromi berarti dana yang dicuri, dan protokol tidak dapat membalik sebuah transfer terlindung yang valid.

Risiko kustodial dan gateway. Gateway resmi, mitra venue, dan pengaturan kustodi pihak ketiga mana pun menghadirkan eksposur pihak lawan yang tidak dikendalikan protokol. Sebuah gateway dapat menunda penyelesaian state publik. Sebuah venue dapat menghentikan penarikan. Seorang kustodian dapat gagal. Tidak satu pun dari peristiwa ini dapat memindahkan nilai terlindung atau mengubah akuntansi pasokan, dan semuanya dapat mengurangi kemampuan pemegang untuk bertransaksi.

Risiko operator dan slashing. Stake terdelegasi terekspos pada slashing karena ekuivokasi operator dan pada penalti liveness karena ketidaktersediaan. Perubahan komisi dan pengunduran operator diatur oleh periode pemberitahuan yang mungkin tidak memadai bagi delegator yang tidak memantau status on-chain.

Risiko likuiditas dan volatilitas harga. Harga pasar NKVR dapat berfluktuasi tajam atau turun menjadi nol. Konsentrasi di antara peserta awal, buku order yang tipis di luar venue genesis, dan ketiadaan jaminan penopang harga berarti pemegang mungkin tidak dapat keluar pada harga yang dapat diterima, atau tidak dapat keluar sama sekali dalam kondisi pasar yang tertekan. Tidak ada dalam whitepaper ini yang merupakan batas bawah harga, jaminan likuiditas, atau proyeksi nilai.

Risiko konsentrasi dan tata kelola. Produksi bukti dapat terkonsentrasi di antara kumpulan operator yang kecil, dan pemungutan suara berbobot stake memberikan pengaruh kepada pemegang besar secara proporsional dengan bobot ekonominya. Mitigasi di Bagian 7.4 dan 10.2 bersifat prosedural dan berbasis parameter alih-alih invarian matematis.

Risiko eksekusi dan adopsi komersial. Fase I-B, II, dan III dapat tertunda, dimodifikasi, atau tidak pernah terealisasi. Mitra perusahaan atau integrasi ekonomi mesin mungkin tidak terwujud, dan dalam hal itu pembelian kembali pendapatan Tahap 2 tidak pernah beroperasi dan pengurangan pasokan hanya bergantung pada burn mekanisme Tahap 1.

12.3 Yurisdiksi, Pernyataan Prospektif, dan Batas Dokumen Ini

Distribusi whitepaper ini dan ketersediaan NKVR dibatasi di yurisdiksi tertentu dan dilarang di yurisdiksi lain. Tidak ada di sini yang merupakan penawaran atau ajakan di yurisdiksi mana pun di mana penawaran tersebut melanggar hukum, dan tidak ada orang yang boleh mengandalkan whitepaper ini dalam memutuskan apakah akan memperoleh NKVR. Kelayakan atas alokasi genesis mana pun ditentukan secara eksklusif oleh dokumentasi hukum terpisah yang diterbitkan oleh The Niskvora Foundation, dan dokumentasi itu berlaku di mana pun ia bertentangan dengan whitepaper ini.

Pernyataan mengenai fase protokol di masa depan — aktivasi lapisan terlindung, atestasi zkTLS perusahaan, vault agen otonom, pendapatan biaya, dan volume pemusnahan di masa depan — adalah pernyataan prospektif (forward-looking statements). Pernyataan tersebut mencerminkan niat desain arsitektural pada Q4 2026 dan bertumpu pada asumsi mengenai eksekusi rekayasa, keamanan kriptografis, permintaan pasar, dan perlakuan regulasi, yang masing-masing melibatkan ketidakpastian substansial. Baik The Niskvora Foundation maupun Niskvora Cryptography Collective tidak menanggung kewajiban apa pun untuk memperbarui pernyataan prospektif setelah publikasi.

Parameter protokol yang dijelaskan di sini, selain yang secara permanen terkunci dalam bytecode Lapisan I, dapat diubah melalui tata kelola Lapisan II. Pembaca sebaiknya memverifikasi parameter aktif secara langsung terhadap state on-chain alih-alih mengandalkan angka statis dalam teks ini.

Tidak ada dalam dokumen ini yang merupakan nasihat hukum, pajak, akuntansi, atau investasi, dan tidak ada kontributor protokol yang bertindak sebagai pihak yang memikul kewajiban fidusia (fiduciary) atau sebagai penasihat bagi pemegang mana pun. Calon peserta harus memperoleh nasihat profesional independen di yurisdiksi mereka sendiri sebelum memperoleh, memegang, atau melakukan staking NKVR.

Lampiran A — Glosarium Formal dan Notasi State Protokol

Istilah	Definisi Formal
State Sekala	State akun publik default pada lapisan penyelesaian kanonis. Saldo plaintext, graf transaksi terlihat, semantik token tanpa modifikasi, dan kompatibilitas venue native.
Vault Terlindung Niskala	State konfidensial opsional pada lapisan zero-knowledge modular. Nilai ditahan sebagai note terenkripsi dalam pohon komitmen append-only dengan jumlah, pengirim, penerima, dan leluhur yang tersembunyi.
Privasi vs. Anonimitas (Privacy vs. Anonymity)	*Privasi* adalah kerahasiaan yang dikendalikan pemegang yang dipasangkan dengan kemampuan pembuktian kriptografis selektif; *anonimitas* adalah penyembunyian wajib dan tidak dapat diaudit yang tidak memiliki jalur pengungkapan apa pun. Niskvora menerapkan yang pertama dan mengecualikan yang kedua.
Note & Komitmen (Commitment)	Sebuah denominasi terlindung diskret yang dimiliki oleh spending key, direpresentasikan on-chain oleh komitmen homomorfik yang mengikat dan menyembunyikan yang membawa range proof.
Nullifier	Nilai deterministik yang diturunkan dari sebuah note dan spending key pemiliknya, dipublikasikan saat pembelanjaan untuk mencegah pembelanjaan ganda tanpa mengungkap komitmen mana di dalam pohon yang dikonsumsi.
Supply Turnstile	Gerbang akuntansi dua arah antara Sekala dan Niskala, yang memelihara penghitung masuk dan keluar kumulatif plaintext publik yang selisihnya sama dengan saldo agregat publik persis dari pool terlindung.

Plafon Efektif (Effective Ceiling, $S_{\text{eff_max}}$)	$21.000.000 - S_{\text{burned}}(t)$. Menurun monoton setelah burn pertama; tidak ada fungsi kontrak untuk mencetak atau menerbitkan ulang unit.
Viewing Key	Materi kunci kriptografis baca-saja yang diturunkan tanpa wewenang pengeluaran. *Full viewing key* mendekripsi semua note dari suatu akar; *scoped viewing key* diturunkan secara ketat sepanjang jalur alamat dan jendela waktu yang terbatas. Keduanya tidak dapat menghasilkan nullifier yang valid.
ZK-PoI (Exclusion Proof)	Bukti zero-knowledge yang dihasilkan klien yang menetapkan bahwa leluhur suatu note terlindung tidak beririsan sama sekali dengan kumpulan alamat yang dikenai sanksi atau terlarang yang dipublikasikan dan ber-hash versi, tanpa mengungkap note tersebut atau jalur transaksinya.
State Root	Komitmen kriptografis 32 byte atas pohon note Niskala dan kumpulan nullifier, yang dikirim secara berkala ke lapisan penyelesaian bersama sebuah bukti validitas rekursif.
Era Halving / Epoch Akuntansi	*Era Halving* mencakup 12 bulan (365 hari) dan mengatur emisi agregat pool witness; *Epoch Akuntansi* mencakup 1 hari dan mengatur perhitungan serta distribusi reward secara pro-rata.
Vault Pelepasan (Release Vault)	Kontrak vesting bytecode yang tidak dapat diubah yang memegang alokasi genesis yang belum vesting pada lapisan penyelesaian. Saldo vault bersifat publik dan secara ketat dilarang untuk staking witness.
Collaborative Witness	Struktur keamanan jaringan terpisah yang terdiri dari *Operator* (perangkat keras prover, eksekusi slot, risiko slashing self-bond) dan *Delegator* (pengikatan modal, pemilihan operator, tanpa kebutuhan perangkat keras).
Gateway Likuiditas Resmi (Authorized Liquidity Gateway)	Antarmuka state publik berlisensi/berizin yang memfasilitasi penyelesaian venue dan pesan delegasi stake sekali klik; tidak memegang spending key apa pun untuk vault terlindung mana pun.
Mandat Berlingkup (Scoped Mandate)	Kredensial bertanda tangan master key dalam Agent Shield yang menegakkan batas mesin state yang keras (plafon per transaksi, batas periode bergulir, allowlist tujuan, masa berlaku) pada kunci sesi agen otonom.

Lampiran B — Penerbitan Moneter, Era Halving, dan Persamaan Pasokan

B.1 Konvergensi Geometrik Pool Witness. Misalkan E_k menyatakan emisi pool witness selama Era Halving 12 bulan $k \in \{0, 1, 2, \ldots\}$, dengan emisi Era 1 ($k = 0$) $E_0 = 4.200.000\text{NKVR}$:

$$E_k = E_0 \cdot 2^{-k}, \qquad \sum_{k=0}^{\infty} E_0 \cdot 2^{-k} = 2E_0 = 8.400.000\text{NKVR}$$

Emisi bulanan dalam Era k adalah $E_k / 12$, yang didistribusikan di seluruh 365 epoch akuntansi harian. Setelah Era 5 ($k \geq 5$, M61+), emisi ekor residual (262.500NKVR) t erus berkurang separuh setiap 12 bulan dan terpotong secara bersih begitu laju epoch yang terhitung turun di bawah lantai presisi yang ditetapkan tata kelola $\varepsilon \geq 10^{-8}\text{NKVR}$.

B.2 Identitas Pasokan On-Chain Lima Kuantitas. Pada stempel waktu mana pun $t \geq 0$ pasca-genesis, dengan unit terkecil 10^{-8}NKVR:

$$S_{\text{released}}(t) = 21.000.000 - S_{\text{vault}}(t)$$

$$S_{\text{circ}}(t) = S_{\text{released}}(t) - S_{\text{staked}}(t) - S_{\text{burned}}(t)$$

$$S_{\text{eff_max}}(t) = 21.000.000 - S_{\text{burned}}(t) < 21.000.000 \quad (\forall\, t : S_{\text{burned}}(t) > 0)$$

dengan $S_{\text{vault}}(t) \cap S_{\text{staked}}(t) = \emptyset$ ditegakkan dalam bytecode (cadangan yang belum vesting tidak dapat di-stake). Di sini $S_{\text{staked}}(t)$ menyatakan stok terikat kontemporer pada waktu t, termasuk antrean unbonding. Ketika stake terikat dikenai penalti dan dibakar, $S_{\text{staked}}(t)$ menurun dan $S_{\text{burned}}(t)$ meningkat dengan kuantitas yang identik, sehingga $S_{\text{circ}}(t)$ tetap invarian sementara $S_{\text{eff_max}}(t)$ turun secara permanen. Lintas state, saldo Sekala yang likuid ditambah saldo pool Niskala (Inflow − Outflow) sama dengan $S_{\text{circ}}(t)$, dan $S_{\text{circ}}(t) + S_{\text{staked}}(t) + S_{\text{vault}}(t) + S_{\text{burned}}(t) = 21.000.000\text{NKVR}$ pada setiap root yang terverifikasi.

B.3 Bobot Epoch Delegasi Witness. Untuk delegator i yang terikat pada operator $o(i)$ selama epoch harian e:

$$w_{i,e} = s_i \cdot m(l_i) \cdot a_{o(i),e}$$

dengan $s_i > 0$ adalah pokok terikat dalam NKVR, l_i adalah horizon lock yang dikomitmenkan, $a_{o(i),e} \in [0, 1]$ adalah skor ketersediaan slot valid bergulir milik operator, dan $m(l)$ adalah pengali lockup yang cekung ketat yang memenuhi

$m(0) = 1$, ,$m''(l) < 0$, dan$m(l) \leq m_{\max}$. Porsi reward bergantung secara eksklusif pada$(s_i, l_i, a_{o(i),e})$, tanpa input pembobotan eksternal atau off-chain.

B.4 Burn Penalti Unbonding Dini Tahap 1. Seorang delegator yang memulai keluar dini setelah menjalani$l_{\text{served}} < l_i$ kehilangan:

$$P_i = p \cdot s_i \cdot \frac{l_i - l_{\text{served}}}{l_i}, \qquad p \in (0, 1]$$

yang ditransfer langsung oleh kontrak staking ke alamat burn yang tidak dapat dipulihkan.

B.5 Pembelian Kembali dan Burn Pendapatan Komersial Tahap 2. Untuk periode$t$ dengan pendapatan biaya protokol bersihR_t (dikumpulkan dalam fiat/stablecoin dari Verify dan Agent Shield), parameter pembelian kembali$\beta \in [\beta_{\min}, \beta_{\max}]$, dan harga pasar berbobot eksekusi$P_{\text{NKVR},t}$:

$$\Delta S_{\text{burned, Tahap 2}}\left(t\right) = \frac{\beta \cdot R_t}{P_{\text{NKVR},t}}$$

Lampiran C — Model Ancaman Kriptografis dan Ringkasan Batas Keamanan

Asumsi Keamanan / Komponen	Konsekuensi Kegagalan	Mitigasi Protokol	Eksposur Residual & Batas yang Jujur
Kesahihan Verifier Lapisan Penyelesaian	State root tidak valid diterima; note tanpa jaminan tercipta di dalam pool Niskala	Audit multi-firma; verifikasi formal sirkuit konservasi turnstile; peningkatan verifier dengan timelock	Nilai maksimum yang dapat diekstraksi dibatasi secara ketat oleh saldo publik pool Niskala (Inflow – Outflow) pada lapisan penyelesaian

Kesulitan Logaritma Diskret (Discrete-Log Hardness)	Pengikatan/ penyembunyian komitmen atau kesahihan komitmen polinomial terpatahkan	Margin keamanan kurva eliptik yang konservatif; antarmuka verifier modular yang terpisah dari kontrak aset	Rentan terhadap komputer kuantum toleran galat skala besar; migrasi berbasis hash meningkatkan ukuran bukti 1–2 orde besaran
Setup Transparan & Akumulasi Rekursif	Bukti validitas dipalsukan tanpa subversi seremoni	Tanpa seremoni trusted-setup (menghapus inflasi rahasia toxic-waste); parameter IPA/Fiat–Shamir terkunci audit	Bergantung pada batas kesahihan discrete-log dan fungsi hash sebelum migrasi verifier pasca-kuantum
Range Proof Komitmen Note & Keunikan Nullifier	Inflasi nilai negatif atau pembelanjaan ganda di dalam state terlindung	Range proof per note ditegakkan dalam sirkuit; kumpulan nullifier deterministik diperiksa pada setiap transisi root	Tereduksi menjadi kebenaran kontrak verifier di atas
Kustodi Spending Key Klien	Kehilangan permanen atau pembelanjaan tanpa wewenang atas note terlindung	Pembangkitan kunci di sisi klien; pemisahan ketat antara spending key dan viewing key	Tanpa kapabilitas pemulihan, override, atau pembalikan oleh protokol secara desain
Eskalasi Perkakas Agen Otonom (Agent Shield)	Agen melewati guardrail prosedural atau membaca OTP kotak masuk untuk menaikkan batas	Master key terpisah (air-gapped) dari runtime agen; batas ditegakkan dalam mesin state kriptografis melalui Mandat Berlingkup	Pemegang tetap bertanggung jawab menetapkan plafon mandat dan allowlist tujuan yang tepat

Integritas Gateway Resmi	Penyelesaian state publik tertunda atau metrik operator disajikan keliru	Gateway tidak memegang spending key terlindung; ikatan stake langsung atau omnibus dapat diverifikasi on-chain; pelanggaran dihukum dengan pencabutan otorisasi	Friksi liveness jangka pendek pada alur kerja yang dirutekan gateway; jalur kontrak langsung tetap terbuka bagi dompet self-custodial
Liveness Operator & Konsentrasi Stake	Slot state root terlewat atau penyertaan bukti tertunda	Penalti bobot ketersediaan bergulir; slash liveness yang meningkat; plafon stake dan porsi slot per operator	Plafon konsentrasi adalah parameter Lapisan II alih-alih bytecode Lapisan I yang tidak dapat diubah
Jalan Keluar Publik yang Tak Terhentikan	Penolakan regulasi atau pihak lawan atas bukti provenans terlindung	Turnstile tidak mengekspos fungsi pause atau blacklist; bukti keluar yang valid diselesaikan tanpa izin ke Sekala	Metadata IP lapisan jaringan dan kebijakan penerimaan venue yurisdiksional tetap di luar kendali protokol

Rujukan Akademik Eksternal yang Dikutip di Bagian 8.3:
Samuel Breckenridge, Dani Vilardell, Wenhao Wang, Fan Zhang, dan Ari Juels, *"I-HITL: Inalienable Human-in-the-Loop,"* Cornell Tech, Yale University, dan Initiative for CryptoCurrencies and Contracts (IC3), arXiv:2610.35835, 26 Oktober 2026.