JANZEER BLOCKCHAIN

نموذج الأمان والتهديدات

افتراضات الثقة · أمان BFT · التخفيف

إصدار الوثيقة 1.0 · شبكة جنزير · 2026

نموذج الأمان والتهديدات في Janzeer

إن Janzeer سلسلة من الطبقة الأولى (Layer-1) متحمِّلة للأعطال البيزنطية (BFT)، بمعروض ثابت، **مفتوحة المشاركة وخالية من الحصص (permissionless stake-free)**، وتعتمد منظومة محفظة هرمية حتمية (HD) غير احتجازية: تتحقق العقدة من التواقيع لكنها لا تولّد مفاتيح المستخدمين ولا تحتفظ بها ولا تنقلها قط. توحّد هذه الوثيقة أهداف الأمان لدى Janzeer، وافتراضات الثقة، ونموذج التهديدات، موجَّهةً إلى المهندسين والمدققين والمتكاملين المعنيين بالأمان. وتشرح ما يضمنه البروتوكول (نهائية BFT للكتلة المفردة، والحماية من إعادة التشغيل بما فيها إعادة التشغيل عبر السلاسل، واستحالة الإنفاق الزائد، وثبات المعروض)، وما يعتمد عليه (نِصاب أمين بمقدار الثلثين من مجموعة المُصادِقين النشطة، وساعات مُتزامنة عبر NTP، وحفظ المفاتيح من جانب العميل)، وكيف يُخفَّف كل هجوم واقعي أو، حيث يبقى خطر متبقٍّ، يُسمّى صراحةً. أما التفاصيل التشفيرية والبروتوكولية الدقيقة على مستوى البايت فتوجد في الورقة الصفراء؛ وهذه الوثيقة تشير إليها بدلًا من إعادة صياغتها.

1. أهداف الأمان وافتراضات الثقة

ما يهدف البروتوكول إلى ضمانه

- **السلامة (لا كتلتان نهائيتان متعارضتان):** تُجعَل كتلة واحدة على الأكثر نهائيةً عند كل ارتفاع، ما دام أقل من ثلث المجموعة النشطة بيزنطيًّا.
- **نهائية الكتلة المفردة:** الكتلة التي تبلغ نِصاب COMMIT تصبح نهائية فورًا، دون فترة انتظار لعمق التأكيد ودون إعادة ترتيب احتمالية.
- **الحماية من إعادة التشغيل:** كل معاملة مرتبطة برقم تسلسلي (nonce) خاص بالحساب (يكون جزءًا من كل من النص الأصلي الموقَّع وتجزئة حالة الحساب) وبِـ **network id** (معرّف الشبكة) في النص الأصلي الموقَّع، فلا يمكن إعادة تشغيل معاملة على الحساب نفسه ولا عبر شبكة Janzeer مختلفة (mainnet/testnet/devnet).
- **استحالة الإنفاق الزائد:** لا يمكن أن يصبح رصيد حساب سالبًا قط، لا في المسار الحي ولا أثناء المزامنة.
- **حفظ المعروض الثابت:** إجمالي المعروض هو `MAX_SUPPLY = 100,000,000` (بمقياس 8)، مُخصَّص مسبقًا عند التكوين ولا يُسَكّ أبدًا؛ والرسوم تُقسَّم (تُعاد إلى الدورة أو تُدفَع للمنتِج)، ولا تُحرَق ولا تُنشَأ قط.
- **شبكة موثَّقة الهوية:** لا يُقبَل إلا النظراء الذين يُتمّون مصافحة ECDSA متبادلة.
- **سلامة مجموعة القواعد:** مجموعة معاملات الإجماع الحرجة مثبَّتة على بصمة مواصفات السلسلة (chain-spec digest) الخاصة بالتكوين، والتي يتبادلها النظراء ويتحققون منها عند المصافحة، فلا تستطيع عقدة أن تغيّر القواعد خِلسةً وتبقى على الشبكة.

ما يعتمد عليه (افتراضات الثقة)

- **أغلبية عظمى أمينة من المجموعة النشطة.** لا تتحقق الحيوية والسلامة إلا ما دام أكثر من ثلثي الحجم *الفعلي* للمجموعة النشطة `N` أمينًا وقابلًا للوصول — ونِصاب BFT هو `bftQuorum(N) = floor(2N/3) + 1`، أي صيغة "2f+1" الكلاسيكية عندما `N = 3f+1`. والمجموعة النشطة محدودة بسقف `promoters-count = 21`.
- **ساعات مُتزامنة.** تعتمد كل عقدة على تزامن NTP ضمن `ntp-offset-threshold = 250 ms` (شُدِّد ليلائم فترات زمنية بساعة جدارية مدتها 15 ثانية). والعقدة التي لا تكون ساعتها متزامنة، أو التي لم تكتمل مزامنتها، توقف إنتاج الكتل بدلًا من المخاطرة بالإنتاج على ساعة معطوبة.
- **حفظ المفاتيح من جانب العميل.** يقوم أمان أي حساب كليًّا على حماية صاحبه لعبارة الاسترداد / المفتاح الخاص. وليس لدى العقدة أي مسار استرداد: فلا توجد نقاط نهاية لتوليد المفاتيح أو البذور، والعقدة لا ترى مفتاحًا خاصًّا قط.
- **وجود نِصاب حي.** تتطلب النهائية نِصابًا حيًّا من المجموعة النشطة؛ ولا تستطيع عقدة مفردة (أو أي مجموعة دون النِّصاب) أن تجعل الكتل نهائية.

2. الضمانات التشفيرية

العقدة **مُحقِّقة، لا حافظة.** تُشتَقّ كل المواد المفتاحية وتُحفَظ من جانب العميل؛ وتكتفي العقدة بالتحقق من التواقيع ولا تكشف قط نقاط نهاية لتوليد المفاتيح أو البذور (انظر القسم 1 من سطح REST — كل نوع معاملة يُتحقَّق منه عبر `POST`، ولا يُوقِّع أيٌّ منها من جانب الخادم).

الخاصية	القيمة
المنحنى	secp256k1، مفاتيح عامة مضغوطة (33 بايت)
منظومة التوقيع	ECDSA، حتمية وفق **RFC-6979** (HMAC-SHA256 لِـ `k`)
الدفاع ضد القابلية للتطويع	**فرض low-S القانوني** (تُرفَض تواقيع high-S)
ترميز التوقيع	**DER**، ثم **Base64**؛ موقَّع على الملخّص الخام بطول 32 بايت (على العملاء استخدام `prehash:false`)
تجزئة المعاملة / الكتلة / الحالة	**double-SHA256**، hex بحروف صغيرة
عبارة الاسترداد ← البذرة	PBKDF2-HMAC-SHA512، 2048 تكرارًا، خرج بطول 64 بايت
العنوان	`0x" + hex(keccak256(compressedPubKey)[0:20])` — Keccak-256" على المفتاح المضغوط بطول 33 بايت، أول 20 بايت؛ والعناوين كلها hex بحروف صغيرة
مسار الاشتقاق	`m/0/0/0`، كلها غير مُقسّاة (non-hardened)

تزيل الأرقام التسلسلية الحتمية وفق RFC-6979 الخطرَ الكارثي لتسرّب المفتاح الخاص الناجم عن `k` عشوائي رديء، ويزيل فرض low-S القابلية للتطويع في التوقيع بوصفها سطح هجوم على هوية المعاملة. ومنظومة العنوان متعمَّدةٌ في ألا تكون **نفس** منظومة Ethereum (إذ يأخذ Janzeer أول 20 بايت من Keccak على المفتاح *المضغوط*). والتطابق بايتًا ببايت بين العقدة والمحافظ المرجعية مُثبَت بمتجهات مُودَعة (`build/wallet-parity-vectors.json`)؛ وعبارة الاختبار القانونية `abandon…about` تشتق `0x06e1c0fa9955a700876f8cb0acc7f13fba9fb8ba`. **أما مخططات بايتات النص الأصلي الدقيقة، ورياضيات الاشتقاق، والثوابت، فمحدَّدة في الورقة الصفراء.**

3. الإجماع وسلامة/حيوية BFT

يجمع Janzeer بين إنتاج الكتل من قِبل مُصادِقين مفتوح المشاركة (permissionless) ونهائية BFT ثنائية الطور (PREPARE ← COMMIT) (على نمط PBFT/Tendermint). لا يوجد إثبات حصة (staking) ولا تفويض ولا تصويت: يُقبَل المُصادِقون بتشغيل عقدة وتقديم `PromoterTx` مع وديعة تسجيل (غير قابلة للاسترداد)، ويُنتخَبون بترتيب التسجيل.

- **تحمّل الأعطال.** يتحمّل البروتوكول `f` من المُصادِقين البيزنطيين من أصل `N` من المُصادِقين النشطين، حيث النِّصاب هو `bftQuorum(N) = floor(2N/3) + 1`. وهذا هو "2f+1" عندما `N = 3f+1`.
- **النهائية ثنائية الطور.** يدلي كل مُصادِق نشط بتصويت PREPARE موقَّع على كتلة معلَّقة صالحة؛ وعند بلوغ نِصاب PREPARE يتحقق منها تحققًا كاملًا ويدلي بِـ COMMIT؛ وعند بلوغ نِصاب COMMIT تصبح الكتلة **نهائية** — نهائية للكتلة المفردة، دون عمق تأكيد. وتُحزَم الأصوات في **QuorumCertificate** تُبثّ مرةً واحدة لكل فترة زمنية.
- **السلامة مقابل الحيوية.** *السلامة* هنا تعني ألا تبلغ كتلتان متعارضتان نِصابَ COMMIT معًا، فلا تتفرّع السلسلة النهائية أبدًا في ظل افتراض الأعطال. و*الحيوية* تعني أن المُصادِقين الأمناء يواصلون إنتاج الكتل وجعلها نهائية؛ وهي تتطلب نِصابًا قابلًا للوصول وساعات مُتزامنة. وفي ظل انقسام الشبكة، يُغلِّب Janzeer السلامة: فالجانب الذي بلا نِصاب لا يجعل الكتل نهائية ببساطة.

- **التلاعب بالتصويت قابل للإثبات وللعقوبة.** يُسمَح لكل مُصادِق بصوت واحد بالضبط لكل فترة زمنية لكل طور (يتتبّعه `SlotVoteTracker`). والصوت الثاني المتعارض دليل قابل للإثبات، يُحزَم بوصفه `SlashingTx` نظاميًّا. وبلوغ `equivocation-ban-threshold = 2` من المخالفات المُثبَتة المتمايزة يُطلق **حظرًا دائمًا**؛ ويتلقى المُبلِّغ مكافأة `slash-reporter-bounty = 5` من الخزينة.
- **الطرد بسبب التوقف.** المُصادِق الذي يبقى صامتًا في فترته الزمنية يُطرَد من المجموعة النشطة عند حدّ الحقبة التالي (عقوبة حافظة للحيوية وغير مُعاقِبة بالمصادرة). كما يجوز لأي مُصادِق أن يعتزل بلطف عبر `ExitPromoterTx`، مما يزيله من المجموعة النشطة وجدول الفترات الزمنية عند حدّ الحقبة التالي؛ وتبقى وديعة التسجيل غير قابلة للاسترداد.
- **التراجع المُؤيَّد بالأدلة.** اختيار الفرع هو أطول-سلسلة-صالحة بقمّة مفردة لا تتحرك إلا إلى الأمام. والتراجع الذي قد يُسقِط حالة مُلتزَمًا بها يتطلب **النِّصاب نفسه 2f+1** من مُصادِقين موثَّقين متمايزين ليؤيّدوه (`RollbackCorroborator`)؛ وهو ليس محرّك إعادة ترتيب عامًّا، مما يزيل هجمات إعادة كتابة التاريخ من عقدة مفردة.

الفترات الزمنية هي تناوب دائري حتمي (round-robin) على قائمة الحقبة النشطة المُجمَّدة: نافذة نشاط `time-slot-duration = 12000 ms` زائد استراحة `time-slot-interval = 3000 ms` = فترة زمنية كاملة قدرها 15000 ms (خمس عشرة ثانية). والحقبة هي `epoch-height = 17000` كتلة رئيسية (≈ 3 أيام بكتل مدتها 15 ثانية)؛ وتُعاد انتخاب المجموعة النشطة عند كل حدّ تكوين (حقبة). وتتألف المجموعة النشطة من المُصادِقين المرساة الذين ما زالوا متمتعين بالامتياز زائد المُصادِقين المنتخَبين الأقدم تسجيلًا، مملوءةً حتى `promoters-count = 21`، مع `rotating-producer-seats = 5` مقاعد تتناوب بإنصاف (بترتيب التسجيل) عبر مقعد احتياط `producer-candidate-pool-size = 100`.

- **الإلغاء التدريجي للمراسي التلقائي.** يبدأ المُصادِقون المرساة الثلاثة في التكوين متمتعين بالامتياز (دائمًا داخل المجموعة، ومحصَّنون ضد عقوبة التوقف) ويتخلّون عن ذلك الامتياز **واحدًا لكل حقبة** (`anchor-demotions-per-epoch = 1`) بمجرد وجود عدد كافٍ من المُصادِقين **المثبَتين المستقلّين** — أي غير المراسي الذين أنتجوا في كل حقبة من آخر `validator-proven-epochs = 2` حقبة. وعدّ المُصادِقين *المثبَتين/المستدامين* بدلًا من التسجيلات الخام يجعل الآلية غير قابلة للتسليح: فطوفان Sybil من التسجيلات الجديدة لا يمكنه فرض تخفيضات الرتبة. ولا تنخفض المجموعة المتمتعة بالامتياز أبدًا دون `safety-floor-validators = 4`، وإذا انهارت المجموعة المستقلّة لاحقًا دون هذا الحدّ الأدنى، فإن المراسي الخاملة تُعاد تفعيلها تلقائيًّا (مضادّة للهشاشة). وتخفيض الرتبة ليس إزالةً — إذ يظل المرسى المخفَّض رتبتُه يُصادِق بالجدارة كأي مُسجَّل. والعدد المتمتع بالامتياز مُلتزَم به لكل حقبة في كل `activeAnchorCount` GenesisBlock بحيث يمكن إعادة بنائه على كل عقدة.

4. الحمايات على مستوى المعاملة

- **الحماية من إعادة التشغيل (رقم تسلسلي خاص بالحساب + معرّف الشبكة).** تحمل كل معاملة `nonce` يكون جزءًا من النص الأصلي الموقَّع و من تجزئة حالة الحساب. وتسمح ذاكرة المعاملات المعلّقة بأرقام تسلسلية متتالية للأنبوبة (`expected = confirmedNonce + pendingCount`)؛ وعند التطبيق يكون التحقق صارمًا (`state.nonce == expected`)، ثم زيادة). ولا يمكن إعادة تشغيل معاملة مُلتقَطة لأن رقمها التسلسلي مُستهلَك سلفًا. كما يبدأ النص الأصلي الموقَّع *أيضًا* بسلسلة **network id** (`consensus.network-id`، والقيمة الافتراضية `janzeer`، ومتمايزة لكل سلسلة)، فلا يمكن إعادة تشغيل معاملة موقَّعة لشبكة على شبكة أخرى. و`RewardTx` النظامية هي النوع الوحيد المُعفى من الرقم التسلسلي (0 nonce، رسوم 0، ولا يقدّمها مستخدم قط).
- **استحالة الإنفاق الزائد / الرصيد السالب.** لا يمكن أن يصبح رصيد سالبًا لا في المسار الحي ولا في مسار المزامنة. وتطرح ذاكرة المعاملات المعلّقة الإنفاق المعلَّق سلفًا قبل قبول معاملة جديدة، فلا يستطيع مهاجم أن يصفّ معاملات متعددة تتجاوز مجتمِعةً الرصيد المؤكَّد الفعلي.
- **قواعد الرسوم.** `MINIMUM_FEE = 0.01`؛ ولتسجيل المُصادِق (`PromoterTx`) رسم محدد بدقة قدره `3` زائد **وديعة تسجيل (غير قابلة للاسترداد)** قدرها `2000` إلى خزينة المصرف (وهي حارس Sybil الأساسي؛ ولا يعيدها الخروج). وتُقسَّم الرسوم بنسبة `treasuryFeeShareBps = 2000` (20% إلى خزينة المصرف، 80% للمنتِج) — لا تُحرَق ولا تُسَكّ أبدًا.
- **التحقق من الرصيد الفعلي في ذاكرة المعاملات المعلّقة.** يتحقق القبول من الرصيد الحقيقي للمرسِل (المؤكَّد ناقص المعلَّق سلفًا)، لا من تقدير متفائل.

- **الترتيب الحتمي.** داخل الكتلة (السعة `block-capacity = 100`)، تُطبَّق `RewardTx` أولًا، ثم معاملات المستخدمين بترتيب تصاعدي للرقم التسلسلي — ترتيب حتمي تعيد كل عقدة إنتاجه، فتتطابق تجزئات الحالة عبر الشبكة.

5. أمان الشبكة

- **مصافحة متبادلة موثّقة الهوية.** نطاق مفصول `JANZEER_HANDSHAKE_V1` (مطويّ مع **network id**): Greeting(nonce + **بصمة مواصفات السلسلة**) ← Proof(sign server nonce) ← Challenge(server nonce + proof). يتحقق الجانبان من تواقيع ECDSA على `doubleSha256(DOMAIN || ":" || networkId || nonce)`؛ ومُعرّف العقدة (UID) هو المفتاح العام للعقدة. **ولا يُضاف إلا النظراء الموثّقون.**
- **سلامة مجموعة القواعد (تثبيت مواصفات السلسلة).** مجموعة معاملات الإجماع الحرجة (كل ما تحت `*.consensus`) هي مجموعة القواعد القانونية المثبَّتة عند التكوين. تحسب كل عقدة **بصمة مواصفات السلسلة** (double-SHA256 على تلك المعاملات) وتتبادلها في Greeting؛ ويُرفَض أي نظير تختلف بصمته قبل مرحلة Challenge. والعقدة التي تعدّل أي معامل إجماع تفصل نفسها عن الشبكة بدلًا من التباعد خِلسةً. أما الإعدادات التشغيلية (المنافذ، وقاعدة البيانات، والنظراء، وNTP) فتبقى خاصة بكل عقدة.
- **التقييد بإصدار البروتوكول.** النقل هو Netty NIO TCP بإطار ثنائي مخصص (`protocol-version string || timestamp(long) || 1-byte MessageType || body`). وإصدار بروتوكول P2P هو `2.0.0`؛ وعدم توافق الإصدار يُسقِط الإطار، مما يمنع الالتباس بين الإصدارات.
- **انتهاء صلاحية الرسائل.** الرسائل غير الكتلية الأقدم من `expiry = 10000 ms` تُسقَط، مما يحدّ من إعادة تشغيل/تأخير البثّ القديم.
- **حدود النظراء.** المستهدف الوارد `peers-number = 3`، وسقف القبول `allowedConnections = 7`، ونبضة كل 10000 ms — مما يقيّد استنزاف الموارد وضغط فيضان الاتصالات.
- **التقييد بالمزامنة.** إنتاج الكتل مقيَّد بحالة `SYNCHRONIZED`؛ والعقدة المتأخرة أو منحرفة الساعة لا تنتج.

6. الأمان الاقتصادي

- **معروض ثابت، بلا سطح للتضخم.** `MAX_SUPPLY = 100,000,000` مُخصَّص مسبقًا عند التكوين ولا يُسَكّ أبدًا، فلا يوجد مسار سَكّ في الشيفرة يُستغَلّ للتضخم. ومكافآت الكتل تُدفَع من خزينة مموَّلة مسبقًا، لا تُنشَأ.
- **خزينة بلا مفتاح.** حساب "المصرف" الخزينة هو `0x0000000000000000000000000000000000000000` — عنوان عصيّ على الاستيلاء لا يقابله مفتاح خاص. لا أحد يستطيع توقيع معاملة منه؛ ولا يحرّك أمواله إلا منطق مكافأة/رسوم البروتوكول. وهو مموَّل بِـ `77,500,000` عند التكوين؛ و`circulatingSupply = MAX_SUPPLY − bankBalance`.
- **إعادة تدوير الرسوم تحفظ المعروض.** نموذج الإصدار هو "C + D": إعانة مجدوَلة متناقصة `scheduledReward(h) = max(rewardTailFloor, rewardBlock / 2^(h / rewardHalvingPeriod))` (`rewardBlock = 10`، `rewardHalvingPeriod = 2,100,000` كتلة ≈ سنة واحدة بكتل مدتها 15 ثانية، `rewardTailFloor = 0.5`)، محدودة بسقف `min(scheduledReward(h), bankBalance)`، زائد إعادة تدوير رسوم الخزينة (حصة الرسوم 20% التي تتدفق عائدةً إلى المصرف). والتضخم الصافي صفر؛ والمعروض محفوظ بحكم التصميم.
- **التحقق من المكافأة على كل عقدة.** `RewardTx` مولَّدة نظاميًّا (رسوم 0، nonce 0) ويُتحقَّق منها مقابل القيمة المحسوبة القانونية على كل عقدة؛ والكتلة التي لا تطابق مكافأتها المبلغ القانوني تُرفَض. ولا يستطيع منتِج أن يدفع لنفسه فوق الحدّ.
- **تذهب المكافأة 100% إلى المنتِج.** تُدفَع مكافأة الكتلة كاملةً إلى محفظة المُصادِق المنتِج — فلا يوجد تفويض ولا اقتسام عمولة ولا مطالبة بالمكافأة. المكافآت تدفع مقابل *عمل* تشغيل السلسلة، لا عائدًا على حصة، وتعيد كل عقدة حساب المبلغ القانوني نفسه.

7. نموذج التهديدات

التهديد	المتجه	تخفيف Janzeer / الخطر المتبقي
الإنفاق المزدوج	إنفاق الرصيد نفسه مرتين	رقم تسلسلي خاص بالحساب + التحقق من الرصيد الفعلي في ذاكرة المعاملات المعلّقة + نهائية BFT للكتلة المفردة: متى صارت الكتلة نهائيةً بِـ COMMIT لا يمكن إعادة ترتيبها دون تراجع مُؤيَّد بِـ 2f+1.
إعادة التشغيل (السلسلة نفسها)	إعادة بثّ معاملة موقَّعة مُلتقَطة	الرقم التسلسلي في النص الأصلي الموقَّع وفي تجزئة الحالة؛ والرقم التسلسلي المُستهلَك يجعل إعادة التشغيل غير صالحة.
إعادة التشغيل عبر السلاسل	إعادة تشغيل معاملة على شبكة Janzeer أخرى	يُربَط **network id** داخل النص الأصلي الموقَّع؛ فمعاملة موقَّعة لشبكة (mainnet/testnet/devnet) غير صالحة على أي شبكة أخرى.
التلاعب بالتصويت / التصويت المزدوج	مُصادِق يصوّت مرتين في فترة زمنية/طور	يجعل `SlotVoteTracker` الصوت الثاني `SlashingTx` قابلًا للإثبات؛ و `equivocation-ban-threshold = 2` من المخالفات ← حظر دائم؛ ومكافأة المُبلِّغ 5.
المدى البعيد / إعادة كتابة التاريخ / التراجع	إعادة كتابة التاريخ النهائي	قمّة مفردة أمامية الاتجاه فقط؛ وإسقاط الحالة المُلتزَم بها يحتاج **النِّصاب نفسه 2f+1** من مُصادِقين موثَّقين متمايزين (`RollbackCorroborator`). ولا تستطيع عقدة وحيدة أو دون النِّصاب إعادة كتابة التاريخ.
نظراء Sybil	إغراق الشبكة بنظراء مزيفين	مصافحة متبادلة موثَّقة الهوية (UID العقدة = المفتاح العام)؛ ولا يُقبَل إلا النظراء الموثَّقون؛ وسقف القبول `allowedConnections = 7`. وعدد النظراء لا يمنح وزنًا في الإجماع — إذ لا يأتي إنتاج الكتل إلا من المُصادِقين المُسجَّلين.
مُصادِقو Sybil	تسجيل مُصادِقين كثيرين للاستيلاء على المجموعة	كل `PromoterTx` يكلّف **وديعة تسجيل (غير قابلة للاسترداد)** قدرها `2000` (ولا يعيدها الخروج) ومقعدًا واحدًا لكل مفتاح؛ والانتخاب بترتيب التسجيل مع تناوب مُنصِف. والإلغاء التدريجي للمراسي لا يعدّ إلا المُصادِقين *المُثبَتين/المستدامين* (الذين أنتجوا في كل حقبة من آخر `validator-proven-epochs = 2` حقبة)، ولا ينخفض أبدًا دون `safety-floor-validators = 4`، فلا يستطيع طوفان من التسجيلات الجديدة تسليح تخفيضات الرتبة. **الخطر المتبقي:** الوديعة أخفّ صراحةً من الحصة/PoW، ومُقاسة لمجموعة مشغِّلين صغيرة.
العبث بمجموعة القواعد	تعديل معامل إجماع خِلسةً	معاملات الإجماع مثبَّتة على **بصمة مواصفات السلسلة** الخاصة بالتكوين، المُتبادَلة والمُتحقَّق منها عند المصافحة؛ والعقدة التي تختلف بصمتها تُرفَض وتفصل نفسها بدلًا من التباعد خِلسةً.
الكسوف (Eclipse)	عزل عقدة خلف نظراء يتحكم بهم المهاجم	الاتصال بنظراء معروفين مخلوطين زائد عُقد الجذر/البذرة المُهيَّأة حتى بلوغ عدد النظراء المستهدف؛ والمزامنة مقيَّدة بِـ `SYNCHRONIZED`. **الخطر المتبقي:** كما في أي شبكة P2P، على المشغّل أن يهيّئ عُقد بذرة/جذر جديرة بالثقة؛ والبذور المتنوعة الموثوقة تقلّل التعرّض للكسوف.
سرقة المفتاح	سرقة عبارة الاسترداد / المفتاح الخاص للمستخدم	التصميم غير الاحتجازي يحصر نطاق الضرر بالحساب المخترَق؛ والعقدة لا تحتفظ بالمفاتيح قط، فاختراق عقدة لا يكشف أي مفاتيح للمستخدمين. **الخطر المتبقي:** حفظ المفتاح مسؤولية صاحبه؛ ولا يوجد استرداد على مستوى البروتوكول.
التلاعب بالساعة	حرف ساعة عقدة لتزوير	يلزم تزامن NTP ضمن `ntp-offset-threshold = 250 ms`؛ والعقدة توقف الإنتاج عند عدم التزامن. **الافتراض:** مصادر NTP أمينة؛ وملكية الفترة الزمنية حتمية، فلا تستطيع ساعة منحرفة واحدة سرقة

التهديد	المتجه	تخفيف Janzeer / الخطر المتبقي
	توقيت الفترات الزمنية	فترة غيرها، بل تخسر فترتها فحسب.
استنزاف الخزينة	إنفاق خزينة التكوين	المصرف `0x000…0` بلا مفتاح وغير قابل للإنفاق بالتوقيع؛ ولا يحرّكه إلا منطق مكافأة/رسوم البروتوكول، ومبالغ المكافأة مُتحقَّق منها قانونيًا على كل عقدة.
خلل التضخم	سَكّ عملات فوق المعروض الأقصى	معروض ثابت بلا مسار سَكّ؛ والمكافآت تُدفَع من مصرف مموَّل مسبقًا محدود؛ والمكافأة مُتحقَّق منها على كل عقدة.
قابلية التوقيع للتطويع	تطويع توقيع لتغيير هوية المعاملة	فرض low-S القانوني؛ وأرقام تسلسلية حتمية وفق RFC-6979.
البريد المزعج / استنزاف الموارد	إغراق ذاكرة المعاملات المعلّقة أو الاتصالات	رسوم دنيا (`MINIMUM_FEE = 0.01` ؛ وتسجيل المُصادِق يكلّف رسم `3` زائد وديعة غير قابلة للاسترداد قدرها `2000`)، وانتهاء صلاحية الرسائل `ms 10000` ، وسقوف النظراء/الاتصالات، وسعة الكتلة `100` .

8. القيود الصريحة والتحفظات التشغيلية

- **يجب تدوير الأسرار المُودَعة لبيئة التطوير/الاختبار.** يأتي المستودع بمحافظ مرسى تكوين افتراضية للتطوير ومواد توقيع لإقلاع البيئة المحلية وشبكة الاختبار. وهذه **ليست أسرار إنتاج** — على المشغّلين توليد وتهيئة مفاتيح جديدة (عبر `janzeer.genesis.signer-secret` / `janzeer.genesis.anchors`) قبل أي نشر للشبكة الرئيسية.
- **يجب أن يكون صنبور صندوق التطوير مُطفأً في الإنتاج.** صنبور (`0xaddr:amount`) `janzeer.dev-fund` مخصص لاختبار التطوير/شبكة الاختبار من الطرف إلى الطرف، وهو مُطفأ افتراضيًا. ويجب ألا يُفعَّل أبدًا على شبكة إنتاج.
- **وديعة التسجيل غير قابلة للاسترداد بالتصميم.** تذهب وديعة `PromoterTx` البالغة `2000` إلى خزينة المصرف ولا تُعاد أبدًا — لا عند الخروج بلطف ولا عند الحظر. وهذا مقصود (فهي حارس Sybil الأساسي)؛ وينبغي للمشغّلين اعتبارها كلفةً غارقة، لا سندًا (bond).
- **يجب أن تكون حفظ مجمّع النظام البيئي البالغ 12 مليونًا شفافةً.** ينبغي أن يُحتفَظ بمجمّع النظام البيئي/التوزيع الخاص بالتكوين (`12,000,000`) تحت آلية شفافة وقابلة للمساءلة (صنبور / توزيع جوي / توزيع محكوم)، لا في محفظة مؤسِّس خاصة، حتى تكون حركاته قابلة للتدقيق.
- **لا تستطيع عقدة مفردة جعل الكتل نهائية.** تتطلب النهائية نِصاب BFT حيًّا من المجموعة النشطة. وتستطيع عقدة مفردة (أو أي مجموعة دون `bftQuorum(N)`) بناء الكتل وخدمتها لكن لا جعلها نهائية؛ كما يتوقف الإنتاج عند عدم بلوغ `SYNCHRONIZED` أو عدم تزامن الساعة.
- **الاعتماد على NTP.** تعتمد سلامة توقيت الفترات الزمنية والتقييد بالإنتاج على تزامن NTP ضمن `ntp-offset-threshold = 250 ms` . وينبغي للمشغّلين تشغيل مصادر NTP موثوقة، ويُفضَّل أن تكون متنوعة.
- **هذا ليس تدقيقًا رسميًا.** تصف هذه الوثيقة خصائص الأمان المقصودة للبروتوكول كما هي مُنفَّذة في الإصدار 0.1.0 من العقدة؛ وهي ليست برهانًا على تلك الخصائص ولم تُدقَّق بصورة مستقلة. ونوصي بمراجعة أمنية مستقلة وتحليل رسمي قبل الاعتماد على Janzeer للاستخدام الإنتاجي العالي القيمة.

حالة الوثيقة

الإصدار 1.0 — يعكس الإصدار 0.1.0 من العقدة. أما المعطيات التشفيرية والبروتوكولية الدقيقة على مستوى البايت (مخططات النص الأصلي، ورياضيات الاشتقاق، والتجزئة، وثوابت الإجماع) فهي مرجعية في الورقة الصفراء.