JANZEER BLOCKCHAIN

الورقة البيضاء

الرؤية والاقتصاد والإجماع

إصدار الوثيقة 1.0 · شبكة جنزير · 2026

الورقة البيضاء لـ Janzeer

إن Janzeer سلسلة كتل من الطبقة الأولى (Layer-1) ذات معروض ثابت، ومقاومة للأعطال البيزنطية، وعديمة الأذونات (permissionless)، يقع في صميم تصميمها مبدأ عدم الحفظ (غير احتجازي): فالعقدة تتحقق من التواقيع ولا تحتفظ بمفاتيح المستخدمين ولا تولّدها ولا تخزّنها أبداً. وللعملة الأصلية سقف صارم قدره 100,000,000 وحدة لا تُسكّ أبداً — فكل عملة موجودة منذ الكتلة التكوينية، وتُدفع مكافآت الكتل من خزينة ممولة مسبقاً على السلسلة بدلاً من إنشائها من العدم. ولا يوجد إثبات حصة ولا تفويض ولا تصويت: إذ يُنفَّذ إنتاج الكتل بواسطة مُصادِقين يسجّلون على نحو عديم الأذونات مقابل وديعة غير قابلة للاسترداد، وينتجون الكتل في تناوب ثابت، ويجعلون كل كتلة نهائية عبر تصويت BFT من مرحلتين. تشرح هذه الورقة ماهية Janzeer، والمشكلة التي تعالجها، ونموذجها الاقتصادي، وكيفية عمل المعاملات والرسوم، وكيف يتكامل الإجماع وقبول المُصادِقين والأمن معاً — مستخدمةً المعطيات الفعلية من قاعدة الشيفرة ومُصرِّحةً بصدق عن تحفظاتها الحالية الخاصة ببيئة التطوير/الشبكة التجريبية.

1. ما هي Janzeer والمشكلة التي تعالجها

تُجبر معظم سلاسل الكتل المستخدمين على أحد موقفين غير مريحين. فإمّا أن تكون المفاتيح محفوظة لدى جهة حافظة — منصة تداول أو محفظة مستضافة — وهو ما يعيد تماماً مخاطر الطرف المقابل التي وُجدت سلاسل الكتل العامة أصلاً لإزالتها، وإمّا أن يعتمد اقتصاد الشبكة على تضخم دائم يخفّض قيمة حصص المالكين بهدوء لتمويل الأمن. وقد بُنيت Janzeer لتجنّب كلا الأمرين.

إن Janzeer شبكة من الطبقة الأولى تجمع بين:

- بنية **غير احتجازية** تُشتق فيها المفاتيح الخاصة وتُستخدم على جانب العميل فقط. فلا تملك العقدة أي نقطة نهاية لتوليد البذور أو المفاتيح؛ بل تكتفي بالتحقق من التواقيع وتطبيق انتقالات الحالة.
- **معروض ثابت لا يُسكّ أبداً** قدره 100,000,000 عملة، حيث تُموَّل مكافآت الأمن من خزينة على السلسلة ومن إعادة تدوير رسوم المعاملات بدلاً من التضخم.
- إنتاج كتل **عديم الأذونات وخالٍ من إثبات الحصة** مقروناً بـ**نهائية BFT من مرحلتين**، بحيث تصبح الكتل نهائية لحظة اعتمادها — فلا يوجد عمق تأكيد احتمالي ينبغي انتظاره.

والنتيجة شبكة يحتفظ فيها المالكون بحفظ أصولهم الخاصة، ويكون المعروض الإجمالي قابلاً للتنبؤ ومحدوداً بسقف، وتكون النهائية سريعة وحتمية. وأي شخص يشغّل عقدة ويودع وديعة غير قابلة للاسترداد لمرة واحدة يمكنه أن يصبح مُصادِقاً — فلا يوجد تصويت أو موافقة أو قفل يُتفاوض عليه. أما الحزمة التقنية فهي Kotlin على Spring Boot وعلى الـ JVM؛ وبرمجية العقدة في الإصدار 0.1.0. وليس للعملة الأصلية رمز تداول مُعرَّف في الشيفرة — وتشير هذه الورقة إليها بـ"العملة الأصلية".

2. فلسفة التصميم غير الاحتجازي

تعامل Janzeer إدارة المفاتيح بوصفها مسؤولية العميل، والتحقق بوصفه المهمة الوحيدة للعقدة. وهذا حدّ مقصود ومفروض، لا مجرد عُرف.

- **لا تصل المفاتيح إلى العقدة أبداً.** فالمحافظ هرمية حتمية (HD): إذ تُوسَّع عبارة الاسترداد إلى بذرة (seed) ثم إلى شجرة مفاتيح بالكامل على جهاز المستخدم. ولا تكشف العقدة عن أي نقطة نهاية تولّد بذوراً أو مفاتيح، ولا تخزّن مفتاحاً خاصاً أبداً.
- **العميل يبني ويوقّع ويرسل؛ والعقدة تتحقق.** تُبنى المعاملة وتُوقَّع على جانب العميل. وتتلقى العقدة معاملة مكتملة التكوين وموقَّعة، فتتحقق من التوقيع مقابل المفتاح العام للمرسل وعنوانه، وتتحقق من الرقم التسلسلي (nonce) والرصيد، ثم تقبلها أو ترفضها. وتستخدم التواقيع خوارزمية ECDSA على منحنى secp256k1 مع أرقام تسلسلية حتمية وفق RFC-6979 وبفرض الصيغة المعيارية منخفضة-S (low-S).
- **تُشتق العناوين على نحو حتمي وقابل للتحقق.** فعنوان Janzeer هو `"0x"` متبوعاً بأول 20 بايت من تجزئة Keccak-256 (hash) للمفتاح العام المضغوط ذي الـ 33 بايت. والصيغة المعيارية المخزَّنة كلها بأحرف hex صغيرة؛ ويُطبَّق مجموع تحقق (checksum)

حقيقي مختلط الأحرف وفق **EIP-55** عند حدّ العرض في المحفظة/الـ API ويُتحقَّق منه عند الإدخال، لكنه عرضيٌّ وغير ذي صلة بالإجماع. ويمكن لأي شخص إعادة حساب عنوان من مفتاح عام، وتُثبت متجهات اختبار التطابق عبر المنصات المودعة في المستودع التوافق بايتاً ببايت بين العقدة وبين تطبيقات المحافظ المستقلة (إذ تتطابق جميعها في الاشتقاق الهرمي الحتمي والعنوان وتجزئة المعاملة والتوقيع).

ولأن العقدة لا تحتفظ بأي مفاتيح، فلا يوجد مستودع مغرٍ لأسرار المستخدمين لسرقته، ولا تستطيع عقدة مخترَقة تحريك أموال المستخدمين. وهذا الحدّ هو أساس نموذج الأمن في Janzeer.

كما تربط كل معاملة موقَّعة **معرّف الشبكة** (network-id، وقيمته الافتراضية `janzeer`، ويختلف لكل سلسلة) في صورتها الأولية، بحيث لا يمكن أبداً إعادة تشغيل معاملة موقَّعة لشبكة واحدة على شبكة أخرى.

3. النموذج الاقتصادي: المعروض الثابت وإصدار C + D

صُمِّم اقتصاد Janzeer حول مبدأ واحد: **التضخم الصفري**. فالمعروض ثابت، ولا تُسكّ العملات أبداً، ومع ذلك يظل المُصادِقون يُكافأون على نحو دائم. ويتحقق ذلك بالجمع بين دعم متناقص ممول من الخزينة (C) وإعادة تدوير الرسوم عبر الخزينة (D).

المعروض الثابت وتخصيص الكتلة التكوينية

يبلغ المعروض الأقصى `100,000,000` عملة (يُحتفظ به داخلياً بمقياس 8 منازل عشرية) ويُخصَّص بالكامل عند الكتلة التكوينية. ولا توجد دالة سكّ في أي موضع من البروتوكول. ويبلغ مجموع تخصيص الكتلة التكوينية المعروضَ الأقصى **بالضبط**، ويُفرَض ذلك بتأكيد ثابت لعدم تجاوز السقف (cap-invariant) يفشل سريعاً عند بدء التشغيل:

التخصيص	المقدار	ملاحظات
"بنك" الخزينة `0x000…000`	77,500,000	عديم المفاتيح، محصَّن ضد الاستيلاء
مجمع النظام البيئي / التوزيع	12,000,000	حنفية / إسقاط جوي / محكوم
المؤسِّس	7,500,000	يُقتطع من الخزينة عند توفير عنوان حفظ
المُصادِقون المرساة (3 × 1,000,000)	3,000,000	مُصادِقو الإقلاع (انظر §5)

ولأن عنوان الخزينة لا يملك مفتاحاً خاصاً، فلا يستطيع أحد إنفاقه مباشرة؛ ولا يمكن إلا لمنطق المكافآت والرسوم الخاص بالبروتوكول نفسه أن يحرّك العملات منه أو إليه. أما تخصيصا المؤسِّس والتوزيع (وحنفية صندوق التطوير الاختيارية) فلا تُقتطع من الخزينة إلا عند توفير عنوان حفظ؛ وفي غياب ذلك تعود إلى الخزينة، بحيث لا يُسكّ شيء أبداً يتجاوز السقف. ويُعرَّف المعروض المتداول بأنه `MAX_SUPPLY − bankBalance`.

C — الدعم المتناقص للكتلة

تحمل كل كتلة دعماً مجدولاً يُنصَّف بمرور الوقت ولا يهبط أبداً تحت حدٍّ أدنى دائم:

```
scheduledReward(h) = max(rewardTailFloor, rewardBlock / 2^(h / rewardHalvingPeriod))
```

مع `rewardBlock = 10`، وفترة تنصيف قدرها `2,100,000` كتلة، وحدٌّ أدنى ذيلي قدره `0.5`، يبدأ الدعم عند 10 عملات لكل كتلة، ويُنصَّف كل 2,100,000 كتلة. ولأن الكتل تُنتَج كل 15 ثانية، فإن فترة التنصيف هذه **تقارب عاماً واحداً**، فتُنصَّف مكافأة الكتلة فعلياً كل عام قبل أن تستقر عند حدٍّ أدنى دائم قدره 0.5 عملة لكل كتلة. أما المبلغ المدفوع فعلياً عند ارتفاع معيّن فهو `min(scheduledReward(h), bankBalance)`: فحين تفرغ الخزينة، يهبط الدفع المجدول إلى الصفر ما لم تُعَد تعبئة الخزينة.

D — إعادة تدوير الرسوم عبر الخزينة

يُعاد ملء الخزينة من رسوم المعاملات. إذ تعود حصة ثابتة من كل رسم إلى البنك (`treasuryFeeShareBps = 2000`، أي **20% من كل رسم ← الخزينة**)، بينما تذهب نسبة الـ **80% المتبقية إلى محفظة منتج الكتلة**. إضافة إلى ذلك، تتدفق الوديعة غير القابلة للاسترداد المدفوعة لتسجيل مُصادِق إلى الخزينة. وتعني إعادة التدوير هذه أن الخزينة تُملأ باستمرار من نشاط الشبكة، بحيث يمكن استدامة الدعم الذيلي الدائم إلى ما لا نهاية دون سكّ أي عملة جديدة على الإطلاق. والأثر الصافي لـ C + D هو ميزانية أمن تتناقص على نحو قابل للتنبؤ، ولا تُضخّم المعروض أبداً، وتظل دائمة.

تُدفع مكافأة الكتلة **بنسبة 100% إلى محفظة المُصادِق المنتِج** — فلا يوجد تفويض ولا اقتسام عمولة. وتُسلَّم المكافأة عبر معاملة مولَّدة من النظام (الرسوم 0، والرقم التسلسلي 0) تعيد كل عقدة حساب قيمتها بشكل مستقل مقابل الجدول المعياري؛ وتُرفض أي كتلة لا تطابق مكافأتها القيمة المعيارية.

4. المعاملات والرسوم

تستخدم Janzeer نموذج الحسابات. ولكل حساب رصيد قابل للإنفاق `balance` ورقم تسلسلي `nonce` للحماية من إعادة التشغيل. وتُتعقَّب المبالغ بدقة 8 منازل عشرية. أما الحدود الدنيا على مستوى البروتوكول فهي `MINIMUM_AMOUNT` قدره `0.1`، و`MINIMUM_FEE` قدره `0.01`، و`MAX_DATA_SIZE` قدره `256` بايت لمذكرة تحويل مرفقة.

تُمنع إعادة التشغيل والإنفاق الزائد على مستوى البروتوكول. فكل معاملة تحمل رقماً تسلسلياً (nonce) لكل حساب يُدرَج في كل من البايتات الموقَّعة وتجزئة حالة الحساب؛ وتسمح ذاكرة المعاملات المعلّقة (mempool) بأرقام تسلسلية متتالية لأغراض الـ pipelining، ويكون الفرض عند التطبيق صارماً. ولا يمكن لرصيد حساب أن يصبح سالباً أبداً، سواء على المسار الحي أو أثناء المزامنة، وتطرح ذاكرة المعاملات المعلّقة الإنفاقات المعلّقة بالفعل قبل قبول معاملة جديدة.

أنواع المعاملات ورسومها:

النوع	الغرض	الرسوم	المبلغ	ملاحظات
TransferTx	نقل العملات، مع مذكرة اختيارية (≤256 بايت)	≥ 0.01	—	المبلغ ≥ 0.1 ما لم تُرفق مذكرة
PromoterTx	تسجيل عقدة بوصفها مُصادِقاً	3 (بالضبط)	2000 (← الخزينة، غير قابلة للاسترداد)	يجب أن يكون مفتاح المُصادِق فريداً
ExitPromoterTx	إحالة مُصادِق إلى التقاعد على نحو سلس	≥ 0.01	—	يُزال من المجموعة النشطة في الحقبة التالية؛ وتبقى الوديعة غير مستردة
RewardTx	دفع مكافأة كتلة (الخزينة ← المنتِج)	0 (نظام)	—	غير مُرسَلة من المستخدم
SlashingTx	إثبات التصويت المزدوج من مُصادِق	بلا رسوم (نظام)	—	يحظر المخالف، ويدفع للمُبلِّغ مكافأة

الرسوم تُقتسم ولا تُحرَق أبداً. فمن كل رسم، تعود 20% إلى الخزينة وتذهب 80% إلى منتج الكتلة. ويحافظ ذلك على المعروض سليماً مع مكافأة المنتجين مباشرة وإعادة تدوير القيمة إلى ميزانية الأمن طويلة الأمد. أما وديعة PromoterTx البالغة `2000` عملة فهي غير قابلة للاسترداد وتمثّل الحارس الأساسي ضد هجمات Sybil لدى الشبكة — وإحالة مُصادِق إلى التقاعد لا تعيدها.

كما يدعم Janzeer رموزاً **قابلة للاستبدال يعرّفها المستخدمون** (JZT-1) إلى جانب العملة الأصلية. فيمكن لأي مُصادِق مُسجَّل أن يُصدِر رمزاً بإمداد محدود بسقف قابل للتعديل، هو وحده من يسكّه أو يحرقه أو يعدّل سقفه، ويمكن لأي شخص حيازته ونقله. وتعيش الرموز على سجل منفصل تحمله معاملة `TokenTx` واحدة: فهي لا تسكّ العملة الأصلية ولا تؤثر فيها أبداً — إذ يبقى سقفها البالغ `100,000,000` سليماً — وكل عملية على رمزٍ تدفع رسومها ببساطة بالعملة الأصلية. ويوجد التخطيط الدقيق لمعاملة الرمز في الورقة الصفراء.

5. الإجماع وقبول المُصادِقين

عائلة الإجماع في Janzeer هي **إنتاج كتل بواسطة مُصادِقين عديم الأذونات مع نهائية BFT من مرحلتين (PREPARE → COMMIT)**، على نمط PBFT/Tendermint. والمنتجون يُسمَّون **المُصادِقين**.

قبول عديم الأذونات وخالٍ من إثبات الحصة

لا يوجد في Janzeer إثبات حصة ولا تفويض ولا تصويت في أي موضع. فالانضمام بوصفك مُصادِقاً عديم الأذونات: **شغِّل عقدة وأرسل PromoterTx تحمل وديعة الـ `2000` غير القابلة للاسترداد** (المدفوعة إلى الخزينة). فلا يوجد تصويت ولا موافقة ولا قفل. والوديعة، مقرونةً بقاعدة "مقعد واحد لكل مفتاح"، هي الحارس ضد هجمات Sybil. وتذهب مكافآت الكتل بنسبة 100% إلى المنتِج — فهي تدفع مقابل *عمل* تشغيل السلسلة، لا مقابل عائد على رأس المال.

ويغادر المُصادِق على نحو سلس بإرسال **ExitPromoterTx**، التي تزيله من المجموعة النشطة ومن جدول الفترات الزمنية عند حدّ الحقبة التالي (بحيث يتوقف تخصيص فترات زمنية له فوراً، بدلاً من أن يتدهور نشاط الشبكة إلى أن يُطرد بسبب انقطاعه). وتبقى وديعة التسجيل غير قابلة للاسترداد عند المغادرة.

الاختيار بترتيب التسجيل

يُرتَّب المُصادِقون المؤهلون حسب **ترتيب التسجيل** — أي `createDate` (ثم المعرّف id)، فالأقدم تسجيلاً أولاً — لا حسب أي تقييم أو حصة أو وزن تصويت. وما دام عدد المُصادِقين المسجَّلين عند سقف المقاعد أو دونه، فجميعهم نشطون؛ وأي فائض يتناوب بإنصاف عبر مقعد احتياط (كما يلي).

الفترات الزمنية والحقب والمجموعة النشطة

يُقسَّم الزمن إلى **فترات زمنية** (slots) ثابتة. وكل فترة زمنية كاملة هي 15,000 مللي ثانية (15 ثانية): نافذة إنتاج نشطة قدرها `slot-duration = 12,000 ms` تتبعها استراحة قدرها `time-slot-interval = 3,000 ms`. ويُختار مالك الفترة الزمنية عبر تناوب دائري حتمي على قائمة المُصادِقين النشطين المجمَّدة للحقبة.

أما **الحقبة** (epoch) فهي `epoch-height = 17,000` كتلة رئيسية (≈ **3 أيام** عند كتل مدتها 15 ثانية). وعند كل حدّ من حدود الحقبة، تُنتَج كتلة تكوينية (GenesisBlock) تعيد انتخاب المجموعة النشطة وتزيد فهرس الحقبة. وتتألف **المجموعة النشطة** من:

- المُصادِقين **المراسي** (anchor) الذين ما زالوا يتمتعون بامتياز (انظر أدناه)، إضافة إلى
- المُصادِقين المنتخَبين الأقدم تسجيلاً، الذين يملؤون المجموعة حتى `promoters-count = 21`، مطروحاً منهم أي أعضاء غير متصلين أو محظورين أو مغادِرين.

وضمن تلك المجموعة، تتناوب `rotating-producer-seats = 5` مقاعد منتخَبة تناوباً دائرياً عبر مقعد احتياط (standby) يضم حتى `producer-candidate-pool-size = 100` مرشَّحاً بترتيب التسجيل، بما يتيح تداولاً عادلاً. أما المُصادِقون الذين يلتزمون الصمت في فترتهم الزمنية المخصَّصة فيُعامَلون بوصفهم في حالة تعطُّل ويُطرَدون في الحقبة التالية.

الإلغاء التدريجي التلقائي للمراسي

تنطلق Janzeer من ثلاثة مُصادِقين **مراسي**، لكنها تُحقِّق اللامركزية لنفسها تلقائياً. فالمراسي تبدأ متمتعة بامتياز — دائماً ضمن المجموعة النشطة ومحصَّنة ضد الطرد بسبب التعطُّل — وتتخلى عن ذلك الامتياز **بواقع واحدة لكل حقبة** (`anchor-demotions-per-epoch = 1`) بمجرد وجود ما يكفي من المُصادِقين **المستقلين المُثبَتين**: أي المُصادِقين غير المراسي الذين أنتجوا في كل حقبة من آخر `validator-proven-epochs = 2` حقبة. وعدّ المنتجين المُثبَتين المستمرين بدلاً من التسجيلات الخام يعني أن سيلاً من هجمات Sybil لا يمكن أن يُوظِّف الآلية سلاحاً.

ولا يُسمح أبداً لمجموعة المُصادِقين السليمة بأن تهبط دون `safety-floor-validators = 4`. وإذا انهارت المجموعة المستقلة لاحقاً دون ذلك الحدّ الأدنى، فإن المراسي الخاملة تعود تلقائياً إلى **الانخراط** — فالنظام مضاد للهشاشة. والتخفيض ليس إزالة: إذ يظل المرساة المُخفَّض يُصادِق على أساس الجدارة كأي مسجِّل آخر. ويُثبَّت عدد المراسي المتمتعين بامتياز في كل GenesisBlock (`activeAnchorCount`) بحيث تكون المجموعة قابلة لإعادة البناء على كل عقدة.

نهائية BFT من مرحلتين

تستخدم النهائية نِصاباً مُعرَّفاً على حجم المجموعة النشطة الفعلي N:

```
bftQuorum(N) = floor(2N / 3) + 1
```

وهذا هو حدّ "2f+1" المألوف حين N = 3f+1. ويعمل البروتوكول في مرحلتين. فكل مُصادِق نشط يُدلي بتصويت **PREPARE** موقَّع على كتلة معلّقة صالحة؛ وبمجرد أن يبلغ PREPARE النِّصاب، يتحقق كل مُصادِق من الكتلة تحققاً كاملاً ويُدلي بتصويت **COMMIT**؛ وبمجرد أن يبلغ COMMIT النِّصاب، تصبح الكتلة **نهائية**. وهذه **نهائية خلال كتلة واحدة** — فلا توجد فترة انتظار لعمق التأكيد. وتُجمَّع الأصوات في **شهادة نِصاب** (QuorumCertificate) وتُنشَر عبر النميمة مرة واحدة في كل فترة زمنية. ويلزم حدٌّ أدنى قدره **4** مُصادِقين (N ≥ 3f+1، بتحمّل عطل واحد) للإطلاق.

التصويت المزدوج والمصادرة

لا يجوز للمُصادِق أن يُدلي إلا بتصويت واحد لكل فترة زمنية ولكل مرحلة، وتتعقّب العقدة ذلك. وأي تصويت ثانٍ متعارض هو تصويت مزدوج قابل للإثبات (double-vote) ويُنتج SlashingTx. ويؤدي بلوغ `equivocation-ban-threshold = 2` مخالفتين مثبتتين متمايزتين إلى **حظر دائم**، ويتلقى المُبلِّغ مكافأة قدرها `slash-reporter-bounty = 5` من الخزينة. ومن ثمّ فالمصادرة قائمة على الأدلة: إذ يُثبَت سوء السلوك تشفيرياً، لا أن يُدّعى مجرد ادّعاء.

اختيار التفرّع والساعات وسلامة مجموعة القواعد

اختيار التفرّع هو أطول-سلسلة-صالحة بقمة واحدة لا تتحرك إلا إلى الأمام. أما التراجع (rollback) الذي قد يلغي حالة معتمَدة بالفعل فيتطلب النِّصاب نفسه 2f+1 من مُصادِقين مصادَق عليهم متمايزين لتأكيده؛ فـ Janzeer نظام أحادي القمة، لا محرّك إعادة ترتيب (reorg) عام. والعقد متزامنة عبر NTP (`ntp-offset-threshold = 250 ms`، مشدَّد لأجل الفترات الزمنية الجدارية البالغة 15 ثانية)، وتتوقف العقدة عن الإنتاج إذا لم تكن ساعتها متزامنة أو إذا لم تكن متزامنة بالكامل. ويمكن لكل كتلة أن تحمل حتى `block-capacity = 100` معاملة؛ وضمن الكتلة تُطبَّق معاملة المكافأة أولاً، ثم معاملات المستخدمين بترتيب تصاعدي للرقم التسلسلي، بما يجعل التطبيق حتمياً بالكامل.

أما معاملات الإجماع الحرجة (كل ما يقع تحت `*.consensus`) فتُشكِّل مجموعة قواعد معيارية ثابتة عند الكتلة التكوينية. وتحسب كل عقدة **بصمة مواصفات السلسلة** (chain-spec digest) على تلك المعاملات وتتبادلها أثناء مصافحة P2P؛ ويُرفض أي نظير تختلف بصمته. ومن ثمّ فإن العقدة التي تعدّل أي معامل إجماع تفصل نفسها عن الشبكة بدلاً من أن تتباعد بصمت.

معاملات الإجماع في لمحة

المعامل	القيمة	المعنى
`MAX_SUPPLY`	100,000,000	السقف الصارم، مخصَّص بالكامل عند الكتلة التكوينية، لا يُسكّ أبداً
تخصيص الخزينة	77,500,000	بنك ممول مسبقاً عند `0x000…000`
`rewardBlock`	10	الدعم المجدول الأولي للكتلة
`rewardHalvingPeriod`	blocks 2,100,000	فترة تنصيف الدعم (≈ عام واحد عند كتل مدتها 15 ثانية)
`rewardTailFloor`	0.5	الحد الأدنى الدائم للدعم
`treasuryFeeShareBps`	2000 (20%)	حصة الرسوم المُعاد تدويرها إلى الخزينة (80% للمنتِج)
`MINIMUM_AMOUNT`	0.1	الحد الأدنى لمبلغ التحويل (بدون مذكرة)
`MINIMUM_FEE`	0.01	الحد الأدنى لرسوم المعاملة
`MAX_DATA_SIZE`	bytes 256	الحد الأقصى لحجم المذكرة المرفقة
`fee-promoter-tx`	3	رسوم تسجيل مُصادِق
`amount-promoter-tx`	2000	وديعة التسجيل غير القابلة للاسترداد (← الخزينة)
`promoters-count`	21	سقف المجموعة النشطة
`rotating-producer-seats`	5	المقاعد المنتخَبة المتناوبة
`producer-candidate-pool-size`	100	مقعد المرشَّحين الاحتياطي
`epoch-height`	17,000	الكتل الرئيسية لكل حقبة (≈ 3 أيام)
`time-slot-duration`	ms 12,000	نافذة الإنتاج النشطة
`time-slot-interval`	ms 3,000	استراحة الفترة الزمنية
الفترة الزمنية الكاملة	ms (15 s) 15,000	الطول الإجمالي للفترة الزمنية
`bftQuorum(N)`	floor(2N/3)+1	نِصاب النهائية (2f+1)
`equivocation-ban-threshold`	2	المخالفات المثبتة ← حظر دائم
`slash-reporter-bounty`	5	المكافأة المدفوعة لمُبلِّغ المصادرة
`safety-floor-validators`	4	لا تُخفَّض المجموعة السليمة دون هذا الحدّ أبداً
`anchor-demotions-per-epoch`	1	امتيازات المراسي المتخلّى عنها لكل حقبة
`validator-proven-epochs`	2	الحقب التي يجب أن يُنتج فيها المُصادِق ليُحتسب مُثبَتاً
`ntp-offset-threshold`	ms 250	حدّ تحمّل تزامن الساعة
`block-capacity`	100	الحد الأقصى للمعاملات لكل كتلة

6. خصائص الأمن

يرتكز أمن Janzeer على عدة خصائص يعزّز بعضها بعضاً:

- **غير احتجازي بحكم التصميم.** فالمفاتيح لا توجد إلا على العميل. ولا توجد نقطة نهاية لتوليد البذور أو المفاتيح، ومن ثمّ لا يوجد مخزن مركزي لأسرار المستخدمين يمكن اختراقه، ولا تستطيع عقدة مخترَقة إنفاق أموال المستخدمين.
- **الحماية من إعادة التشغيل والإنفاق الزائد.** فالرقم التسلسلي (nonce) لكل حساب في كل معاملة مرتبط بكلٍّ من الصورة الأولية الموقَّعة وتجزئة حالة الحساب، ومعرّف الشبكة (network-id) مرتبط بالصورة الأولية لمنع إعادة التشغيل عبر السلاسل. ولا يمكن للأرصدة أن تصبح سالبة أبداً، سواء على المسار الحي أو مسار المزامنة.
- **تواقيع حتمية ومعيارية.** فخوارزمية ECDSA على secp256k1 مع أرقام تسلسلية حتمية وفق RFC-6979 وفرض صيغة منخفضة-S (low-S) تزيل قابلية تشكيل التوقيع ومخاطر إعادة استخدام الرقم التسلسلي.
- **مقاومة هجمات Sybil دون حصة أو إثبات عمل.** فالقبول مقيَّد بوديعة غير قابلة للاسترداد وبمقعد واحد لكل مفتاح، مُلطَّفاً بتناوب عادل وإلغاء تدريجي متحفّظ للمراسي يعدّ المُصادِقين المُثبَتين المستمرين فقط ويصحّح نفسه بإعادة انخراط المراسي إذا انهارت المجموعة.
- **سلامة BFT.** تتحمل الشبكة حتى f من المُصادِقين البيزنطيين من أصل $N = 3f+1$، مع اشتراط النهائية نِصاباً قدره `floor(2N/3)+1`. والتصويت المزدوج قابل للإثبات وللمصادرة، مع حظر دائم بعد مخالفتين مثبتتين.
- **نظير إلى نظير مصادَق عليه.** فالنظراء يُكملون مصافحة تحدٍّ واستجابة متبادلة، ويتحققون من تواقيع ECDSA لبعضهم البعض، ويقارنون بصمات مواصفات السلسلة قبل قبولهم؛ ولا يُضاف إلا النظراء المصادَق عليهم الذين يشغّلون مجموعة القواعد نفسها.
- **خزينة عديمة المفاتيح.** فخزينة الكتلة التكوينية لا تملك مفتاحاً خاصاً، ومن ثمّ لا يمكن إنفاقها مباشرة أبداً — ولا يمكن إلا لمنطق المكافآت والرسوم الخاص بالبروتوكول أن يحرّك عملاتها. وتُبقي الكتلة التكوينية المدفوعة بالإعدادات القيمَ الافتراضية المودعة قابلة لإعادة الإنتاج عبر جميع العقد.

7. تحفظات صادقة

التزاماً بعرض دقيق خالٍ من المبالغة، ينبغي فهم القيود والقيم الافتراضية التالية بوضوح:

- **القيم الافتراضية الراسية لبيئة التطوير/الشبكة التجريبية.** فأسرار المُصادِقين المراسي والقيم الافتراضية للكتلة التكوينية المودعة في المستودع مخصَّصة للاستخدام في التطوير والشبكة التجريبية. ويجب تدويرها لأي نشر إنتاجي.
- **حنفية صندوق التطوير أداة اختبار.** توجد حنفية اختيارية لبيئة التطوير/الشبكة التجريبية لأغراض الاختبار الشامل (end-to-end). وهي معطّلة افتراضياً ويجب أن تظل معطّلة في الإنتاج.
- **يجب أن يكون حفظ مجمع النظام البيئي شفافاً.** فمجمع النظام البيئي/التوزيع البالغ 12,000,000 عملة ينبغي أن يُحفَظ ضمن حفظ شفاف (حنفية أو إسقاط جوي أو عملية محكومة)، لا في محفظة مؤسِّس.
- **النهائية تتطلب نِصاباً حياً.** فلا تستطيع عقدة واحدة أن تجعل الكتل نهائية. إذ تعتمد النهائية على نِصاب حيّ من مجموعة المُصادِقين النشطين، ومن ثمّ تلزم شبكة حقيقية ذات مجموعة كافية من المُصادِقين النشطين الأمناء لكي تصمد ضمانات BFT.
- **وديعة التسجيل غير قابلة للاسترداد بحكم التصميم.** فمغادرة المُصادِق، سواء على نحو سلس أو غير ذلك، لا تعيد الوديعة.

وهذه التحفظات خصائص للإعدادات الحالية ووضع النشر الراهن، لا لقصد تصميم البروتوكول، وينبغي معالجتها من قِبل أي شخص يقيم شبكة إنتاجية.

حالة الوثيقة. الإصدار 1.0. تعكس هذه الورقة البيضاء الإصدار 0.1.0 من عقدة Janzeer. أما المعطيات الدقيقة على مستوى البايت — البدائيات التشفيرية، واشتقاق المفاتيح والعناوين، ومخططات بايتات المعاملات والكتل، والتجزئة، ومقياس المبالغ — فتوجد في الورقة الصفراء.