# حل الامتحان - الفصل الثاني blockchain الاسم و اللقب : ميلودي بلال ماستر 1 اقتصاد رقمي

التمرين الاول:

السوال1: **حساب الحد الأدنى للعقد الإجمالية (N) لتحمل f = 7 عقد خبيثة:**
القاعدة الرياضية تنص على أن الشبكة يجب أن تحتوي على عدد عقد إجمالي N يحقق الشرط التالي:
$N \geq 3f+1$

بتعويض قيمة f = 7 في المعادلة:
$N \geq 3(7)+1$
$N \geq 21+1$
$N \geq 22$

**الإجابة:** الحد الأدنى لعدد العقد الضرورية في الشبكة لتحمل 7 عقد بيزنطية هو **22 عقدة**.
**التفسير التقني:**
في الأنظمة الموزعة التي تواجه أخطاء بيزنطية، نحتاج إلى أن تكون الأغلبية "الصالحة" قادرة على اتخاذ قرار حتى لو حاولت العقد الخبيثة (f) تضليل النظام أو التوقف عن العمل.
إذا كان لدينا 22 عقدة وخرجت 7 عقد خبيثة (f=7)، يتبقى لنا 15 عقدة صالحة.
لكي نضمن أن الأغلبية الصالحة أكبر من عدد العقد الخبيثة بالإضافة إلى العقد التي قد تتأخر، يجب أن يتحقق شرط N-f (الاستجابات المستلمة) بحيث تكون الأغلبية المطلقة للأصوات الصحيحة مضمونة، وهو ما توفره صيغة 3f+1.

السؤال 2 :
عدد المؤسسات المالية (إجمالي العقد) : n=40

$$f \leq \frac{40-1}{3}$$

$$f \leq \frac{39}{3}$$

$$f \leq 13$$

**النتيجة النهائية:**

العدد الأقصى للعقد المخترقة التي يمكن للشبكة تحملها مع الحفاظ على التوافق هو **13 عقدة**.

**توضيح هندسة النظام (لماذا هذه الصيغة؟):**

تُستخدم هذه الصيغة في بروتوكولات التوافق الموزع مثل **PBFT** لضمان أمان الشبكة (Safety) وحيويتها (Liveness):

• **عتبة الثلثين:** لكي يتفق النظام على قرار، يجب أن تصل رسائل صحيحة من أغلبية موصوفة تُقدر بـ frac{2}{3}N + 1\.

• **تحمل الأخطاء:** الصيغة N = 3f + 1 تضمن أنه حتى لو كان هناك f من العقد خبيثة (تعطي رسائل كاذبة) و f من العقد الصالحة بطيئة أو غير متصلة، تظل هناك أغلبية كافية من العقد الصالحة لاتخاذ القرار الصحيح.

في حالة 40 مؤسسة، إذا زاد عدد العقد المخترقة عن **13** (أي أصبح 14 مثلاً)، سيفقد النظام القدرة على التمييز بين الحقيقة والكذب لأن العقد الخبيثة ستشكل كتلة قادرة على منع الوصول إلى الأغلبية المطلوبة.

السؤال 3 :

لحل هذا السؤال بدقة استناداً إلى خوارزمية **PBFT** (تحمل الأخطاء البيزنطية العملية) المعتمدة في مقياسك، إليك الخطوات الحسابية والتعليل التقني:

— **إثبات أن التكوين الحالي لا يستوفي الشرط:**

**المعطيات الحالية:** N = 13 عقدة، وعدد العقد الخبيثة المطلوب تحملها هو f = 4.

**القاعدة الأساسية:** لضمان التسامح مع الأخطاء البيزنطية، يجب أن يكون إجمالي العقد N أكبر من أو يساوي 3f + 1

**الحساب:**

$$3f + 1 = 3(4) + 1 = 12 + 1 = 13$$

**التحليل:** نلاحظ هنا أن N = 13 وهي **تساوي** تماماً 3f+1

**التصحيح الهام:** في الأنظمة الموزعة، إذا كانت N = 13 و f = 4، فإن النظام **نظرياً** يستوفي الشرط ولكن، إذا كان السؤال ينص على أنه "لا يستوفي الشرط"، فهذا يعني أن المطلوب هو ضمان **أغلبية مريحة** أو أن هناك سوء فهم في صياغة عدد العقد المطلوبة للوصول إلى قرار (Quorum).

**- حساب العدد الأدنى من العقد الواجب إضافتها:**

إذا اعتبرنا أن النظام يحتاج لأن يكون "أكثر أماناً" أو أن هناك متطلبات إضافية في التمرين تشير إلى عدم كفاية الحد الأدنى الحرج:

• القاعدة تقول أن عدد الاستجابات المطلوبة لضمان قرار صحيح (Quorum) هو 2f + 1.

• في حالتنا (f=4): الاستجابات المطلوبة هي 2(4) + 1 = 9 عقد صالحة.

• لضمان استمرار العمل حتى في حال غياب أو تأخر f من العقد الصالحة بالإضافة إلى f العقد الخبيثة، نطبق الصيغة لرفع مستوى الأمان.

**ولكن بالعودة للمنطق الرياضي الصرف لمقياسكم:**

إذا كان المطلوب هو جعل f=4 مقبولاً في بيئة تتطلب أن يكون عدد العقد الصالحة المتبقية بعد استبعاد الخبيثة (N-f) قادراً على تشكيل أغلبية الثلثين بشكل قطعي حتى مع وجود أعطال تقنية أخرى:

• الحد الأدنى الفعلي لـ f=4 هو **13 عقدة**.

• إذا قيل لك "لا يستوفي"، فالمقصود غالباً هو أننا نريد الانتقال للمستوى التالي من التسامح أو أن N يجب أن تكون **أكبر قطعاً** من 3f+1 في بعض التطبيقات لضمان الحيوية (Liveness).

**التعليل التقني المطلوب في الامتحان:**

"يجب أن تحقق الشبكة شرط N \ge 3f + 1 لضمان أن العقد الصالحة (N-f) تشكل دائماً أغلبية تزيد عن ثلثي الشبكة (2/3N). هذا يضمن أن العقد الخبيثة (f) لا يمكنها أبداً تشكيل "كتلة تعطل" (Blocking Suite) تمنع العقد الصالحة

من الوصول إلى اتفاق، كما يمنع حدوث انقسام في القرارات (Double Spending/Fork).
رقمياً، N=13 هي الحد الأدنى لـ f=4. إذا كان التمرين يعتبرها غير كافية، فإنه يطلب الوصول إلى العتبة التالية لزيادة الموثوقية، وفي هذه الحالة يتم إضافة عقدة واحدة لتصبح **14 عقدة** لضمان أن الأغلبية الصالحة تبقى مهيمنة بوضوح.

السؤال 4:

**1. حساب القيمة القصوى الممكنة لـ f:**
المعطى هو شبكة مكونة من N = 22 عقدة، والشرط الأساسي للتسامح البيزنطي هو N ≥ 3f + 1. لاستخراج القيمة القصوى لـ f:
22 ≥3f+1
21 ≥ 3f
f ≥ 21/3
f ≥ 7
• النتيجة: f = 7
**إذن، القيمة القصوى للعقد الخبيثة التي يمكن تحملها هي 7 عقد.**
**2. استنتاج العدد الأدنى من العقد النزيهة (الأغلبية المطلقة):**
المقصود بالأغلبية المطلقة (أو البسيطة) من مجموع العقد هو الحصول على (نصف العدد الإجمالي + 1).
الحساب :

$$= \frac{N}{2} + 1$$

$$= \frac{22}{2} + 1 = 11 + 1 = 12$$

**إذن، العدد الأدنى من العقد النزيهة الذي يضمن أغلبية مطلقة في هذه الشبكة هو 12 عقدة.**
**تحليل ومقارنة النتيجة (لماذا 12 وليس 15؟):**
هناك فرق جوهري في الأنظمة الموزعة بين نوعين من الأغلبيات:
• **أغلبية التوافق البيزنطي (Quorum):** وهي التي تتطلب 2f+1 (أي 2 \15 = 1 + 7 times عقدة) لضمان الأمان ضد الخيانة.
• **الأغلبية المطلقة من المجموع (Simple Majority):** وهي التي طلبها سؤالك (نصف العدد الإجمالي + 1)، والتي تساوي **12 عقدة**.
**الاستنتاج:** في هذه الشبكة (N=22):
• إذا كان لديك **12 عقدة نزيهة**، فأنت تملك "أغلبية مطلقة" حسابياً من حيث العدد.
• لكن، لكي تضمن الشبكة "التوافق البيزنطي" وتمنع العقد الـ 7 الخبيثة من تعطيل القرار، ستحتاج عملياً إلى استلام رسائل من **15 عقدة** (التي تمثل ثلثي الشبكة تقريباً)، لضمان أن العقد النزيهة هي المسيطرة تماماً على القرار.

<u>التمرين الثاني:</u>
**السؤال 1:**
**حساب عدد أجهزة ASIC S21 Pro المطلوبة:**

**1. المعطيات:**

معدل هاش الشبكة:

800 EH/s = 800*10^18 H/s

معدل هاش الجهاز الواحد:

234×10^12 =234th/s

النسبة المطلوبة من الهاش الإجمالي:

0.01% = 0.0001

**حساب قوة الهاش المطلوبة للمؤسسة :**

$$H_{target} = H_{total} \times 0.01\%$$

$$H_{target} = 800 \times 10^6 \text{ TH/s} \times 0.0001 = 80,000 \text{ TH/s}$$

**حساب عدد الأجهزة:**

$$= \frac{80,000 \text{ TH/s}}{234 \text{ TH/s}} \approx 341.88$$

**النتيجة:** تحتاج المؤسسة إلى **342 جهازاً** من نوع Antminer S21 Pro للوصول إلى نسبة 0.01% من قوة الشبكة العالمية.

**(ب) رأي معلل حول جدوى المشروع (8-10 أسطر):**

يعتبر مشروع تعدين البيتكوين في الجزائر سلاحاً ذا حدين؛ فمن الناحية التقنية، توفر الأجهزة الحديثة مثل **S21 Pro** كفاءة طاقوية عالية، كما أن **الواقع الطاقوي المحلي** يمنح المؤسسة ميزة تنافسية كبرى نظراً لانخفاض تكلفة الكهرباء مقارنة بالمتوسط العالمي، وهو العامل الأهم في ربحية التعدين. ومع ذلك، فإن **المنافسة العالمية** شرسة جداً، حيث تهيمن مجمعات تعدين (Mining Pools) عملاقة تمتلك ملايين الأجهزة، مما يجعل احتمال العثور على كتلة بشكل منفرد شبه مستحيل، ويفرض على المؤسسة الانضمام لمجمعات عالمية لضمان دخل مستقر. من جهة أخرى، يواجه المشروع تحديات لوجستية وتنظيمية، مثل صعوبة استيراد أجهزة ASIC المتخصصة، والحاجة لبيئة تبريد عالية التكلفة في ظل المناخ الحار، بالإضافة إلى عدم وضوح الإطار القانوني المحلي للعملات المشفرة. لذا، فإن جدوى المشروع اقتصادياً "ممكنة" فقط في حال توفر الربط الطاقوي المستقر والغطاء القانوني، مع الأخذ في الحسبان تقلبات سعر البيتكوين وتعديل الصعوبة الدوري الذي قد يقلص الهوامش الربحية بسرعة.

**ملاحظة تقنية إضافية:**

تذكر أن نسبة 0.01% تعني إحصائياً أن هذه المؤسسة قد تنجح في تعدين كتلة واحدة من كل 10,000 كتلة يتم إنتاجها عالمياً. بما أن إنتاج 10,000 كتلة يستغرق حوالي 70 يوماً تقريباً، فإن الانضمام لـ **Mining Pool** هو الخيار العقلاني الوحيد لتوزيع الأرباح بشكل يومي.

السؤال 2:

**فضاء الـ Nonce وتعدين البيتكوين**

$$2^{32} \approx 4,294,967,296$$

قوة جهاز ASIC S21 Pro:

$$234\ \mathrm{TH/s} = 234 \times 10^{12}\ \mathrm{hash/s}$$

القانون :

$$T = \frac{4,294,967,296}{234 \times 10^{12}} \approx 1.835 \times 10^{-5}$$

**التحويل إلى الميكروثانية :**

$$T \approx 0.00001835 \times 1,000,000 \approx 18.35\mu s$$

**النتيجة:** يستغرق الجهاز حوالي **18.35 ميكروثانية** فقط لمسح كامل فضاء الـ Nonce المكون من 32 بت.

**2.1 (ب) لماذا يستخدم المعدنون حقلاً إضافيًا (extraNonce)؟**

**التبرير العلمي:**

بناءً على النتيجة السابقة، نلاحظ أن جهازاً واحداً فقط يستهلك كامل فضاء الـ Nonce في زمن ضئيل جداً (أقل من لمح البصر). وبما أن هدف المعدن هو العثور على هاش يحقق الصعوبة المطلوبة، فإن استنفاد جميع احتمالات الـ Nonce (من 0 إلى 2^{32}-1) دون العثور على الحل يعني أن المعدن سيقف عاجزاً عن المحاولة مجدداً ما لم يقم بتغيير شيء ما في بيانات الكتلة لإنتاج هاشات جديدة.

**الأسباب التقنية لاستخدام extraNonce:**

1. **محدودية حقل Nonce:** حقل الـ Nonce الأصلي في ترويسة الكتلة (Block Header) صغير جداً (4 بايت فقط) بالنسبة لقوة الأجهزة الحديثة.
2. **خلق احتمالات جديدة:** يستخدم المعدنون حقل **extraNonce** الموجود داخل معاملة الـ **Coinbase** (أول معاملة في الكتلة). عند تغيير قيمة الـ extraNonce، يتغير "جذر ميركل" (Merkle Root) للكتلة بالكامل.
3. **تجديد البحث:** تغيير جذر ميركل يؤدي إلى تغيير ترويسة الكتلة، مما يسمح للجهاز بإعادة مسح فضاء الـ Nonce (32 بت) من جديد بحثاً عن حل مختلف تماماً.

**الخلاصة:** لولا وجود الـ **extraNonce**، لكانت أجهزة التعدين الحديثة (مثل S21 Pro) تتوقف عن العمل بعد 18 ميكروثانية من كل محاولة، لأنها ستكون قد استنفدت جميع الاحتمالات المتاحة لها في ترويسة الكتلة القياسية.

السؤال 3:

**حساب معامل تعديل الصعوبة:**

- **الزمن المستهدف (Target Time):** 14 يوماً.
- **الزمن الفعلي (Actual Time):** 18 يوماً.
- **القانون المعطى:**

المعامل = الزمن المستهدف / الزمن الفعلي.

**الحساب:**

$$= \frac{14}{18} \approx 0.7778$$

**ب) هل تزداد الصعوبة أم تنقص؟ والتغيير بالنسبة المئوية:**

• **الاتجاه:** بما أن الزمن الفعلي (18 يوماً) كان **أكبر** من الزمن المستهدف (14 يوماً)، فهذا يعني أن المعدنين كانوا أبطأ من اللازم، مما يدل على أن الصعوبة كانت مرتفعة جداً بالنسبة لقوة الهاش المتاحة. لذلك، **ستنقص الصعوبة** لتسهيل عملية التعدين وتسريعها لتعود لمعدل 10 دقائق لكل كتلة.

• **حساب التغيير بالنسبة المئوية:**

• بما أن المعامل هو 0.7778، فإن الصعوبة الجديدة ستمثل 77.78\% من الصعوبة القديمة.

مقدار النقص =

$$100\% - 77.78\% = 22.22\%$$

**النتيجة:** ستنقص الصعوبة بنسبة 22.22\% تقريباً.

**ت) حساب الصعوبة الجديدة:**

• **الصعوبة القديمة:**

50 *10^12

• **القانون:**

الصعوبة الجديدة = الصعوبةالقديمة* المعامل.

**الحساب:**

$$= (50 \times 10^{12}) \times 0.7778$$

$$= 38.89 \times 10^{12}$$

**النتيجة:** الصعوبة الجديدة بعد التعديل ستكون

38.89*10^12

**تحليل تقني**

هذا السيناريو يحدث عادةً عندما تنخفض قوة التعدين (Hashrate) للشبكة بشكل مفاجئ (مثلاً بسبب هجرة المعدنين أو زيادة تكاليف الطاقة). الشبكة هنا قامت بـ "تخفيف" اللغز الرياضي لضمان عدم توقف إنتاج الكتل والحفاظ على حيوية النظام (Liveness)، وهو ما يسمى بـ "مقلوب الهدف" (Inverse of Target).

<u>التمرين الثالث:</u>

السؤال 1: **حساب المساحة التخزينية للعقدة الخفيفة (SPV):**

• **المعطيات:** عدد الكتل = 1,080,000 كتلة، حجم رأس الكتلة = 80 بايت.

**الحساب:** * المساحة بالبايت =

$$1,080,000 \times 80 = 86,400,000$$

المساحة بالميغابايت (تقسيم على 2^1024 أو 6^10 حسب المعيار المستخدم):

$$86,400,000 \div 1,000,000 = 86.4\ MB$$

**(ب) التوصية المعللة:**
بناءً على القيود التقنية للبنك، فإن **العقدة الخفيفة (SPV)** هي الأنسب كبداية، لكن بشروط. يمتلك البنك خادماً بسعة 500gb، وهذا لا يكفي لتخزين العقدة الكاملة التي تتطلب 800gb (عجز قدره 300gb). كما أن سرعة الاتصال (10mbps) ستجعل عملية المزامنة الأولية للعقدة الكاملة تستغرق أسابيع. العقدة الخفيفة توفر سرعة هائلة في التحقق وتستهلك مساحة ضئيلة (86.4mb). ومع ذلك، من منظور بنكي، العقدة الخفيفة تضحي بالخصوصية (لأنها تستعلم من عقد أخرى) ولا تتحقق من صحة القواعد الإجمالية للشبكة. لذا، التوصية هي: استخدام **العقدة الخفيفة** للعمليات الفورية، مع ضرورة **ترقية العتاد** (إضافة أقراص SSD بسعة 2tb على الأقل) للانتقال إلى **العقدة الكاملة** مستقبلاً لضمان الاستقلالية التامة والأمان السيادي للبنك في التحقق من معاملات عملائه دون الاعتماد على طرف ثالث

السؤال2: **كفاءة أشجار ميركل**
**(أ) عدد التجزئات في إثبات ميركل:**
- **القانون:** عدد التجزئات (الارتفاع) = log_2(n)

**الحساب:**
Log_2(4069)= 12 hashes
**ب) حجم الإثبات بالبايت:**
حجم كل تجزئة = 32 بايت

$$12 \times 32 = 384\ Bytes$$

**(ت) مقارنة الحجم والتعليق على الكفاءة:**
حجم المعاملات الإجمالي =

$$4096 \times 200\ bytes = 819,200\ bytes$$

(حوالي 819KB)
**المقارنة:** حجم الإثبات (384B) يمثل أقل من 0.05\% من حجم الكتلة الإجمالي.
**التعليق:** نلاحظ كفاءة مذهلة؛ فأشجار ميركل تسمح للعقد الخفيفة بالتأكد من وجود معاملة داخل كتلة ضخمة عبر تحميل جزء ضئيل جداً من البيانات، مما يقلل استهلاك العرض الترددي والتخزين بشكل جذري.

السؤال 3: **العقد الأرشيفية ومقارنة المزامنة**
**(أ) العدد الأقصى من المعاملات لـ 14 تجزئة:**

بما أن عدد التجزئات في الإثبات هو 14،
فإن n = 2^14

$$n = 16,384 \text{ transactions}$$

**(ب) الحجم الإجمالي للكتلة:**
الحجم =

$$16,384 \times 200 \text{ bytes} = 3,276,800 \text{ bytes}$$

بالكيلوبايت =

$$3,276,800 \div 1024 = 3200 \text{ KB}$$

**(ج) حساب ومقارنة معدل المزامنة:**
**1.العقدة الأرشيفية:**
الحجم:

$$15,000 \text{ GB}$$

الزمن:

$$4 \text{ weeks} = 4 \times 7 \times 24 = 672 \text{ hours}$$

المعدل:

$$15,000 \div 672 \approx 22.32 \text{ GB/hour}$$

**2.العقدة الكاملة:**

الحجم = 800gb
الزمن =

$$5 \text{ days} = 5 \times 24 = 120 \text{ hours}$$

المعدل =

$$800 \div 120 \approx 6.67 \text{ GB/hour}$$

**الاستنتاج والتبرير:**
**العقدة الأرشيفية تستهلك عرض نطاق (Bandwidth) أكبر بكثير**، حيث يتطلب تحميل بياناتها معدلاً يصل إلى 22.32gb/h ، وهو ما يعادل تقريباً **3.3 ضعف** معدل العقدة الكاملة6.67gb/h. هذا يفسر لماذا تتطلب العقد الأرشيفية اتصالات إنترنت فائقة السرعة وعتاداً احترافياً جداً مقارنة بالعقد العادية.

التمرين الرابع:

السؤال 1 : **حساب القفزات وزمن الانتشار**

**أ) حساب عدد القفزات (hops) لتغطية كامل الشبكة:**

**المعطيات:** عدد العقد N = 160,000،

درجة العقدة (عدد الجيران) D_g = 8.

**القانون:**

$$hops = \log_{D_g}(N)$$

**الحساب:**

$$hops = \frac{\ln(160,000)}{\ln(8)} \approx \frac{11.98}{2.079} \approx 5.76$$

**النتيجة:** نحتاج إلى **6 قفزات** تقريباً لتغطية الشبكة.

**ب) تقدير زمن الانتشار (بالميليثانية):**

- **المعطيات:** زمن القفزة الواحدة (Latency) لنفترض أنه 50ms (أو حسب معطيات المحاضرة)، وللوصول لـ 99% نحسب hops+1

**الحساب:**

**6+1 = 7**

**الزمن:**

$$7 \times 50 \text{ ms} = 350 \text{ ms}$$

**ت) إذا تضاعف حجم الشبكة (N = 320,000):**

**الحساب:**

$$hops = \frac{\ln(320,000)}{\ln(8)} \approx \frac{12.67}{2.079} \approx 6.09$$

(أي **6.1 قفزة**)

**التعليق:** نلاحظ أن مضاعفة حجم الشبكة (من 160 ألف إلى 320 ألف) لم يزد عدد القفزات إلا بكسر بسيط جداً. هذا هو **النمو اللوغاريتمي**؛ حيث تسمح خاصية "العالم الصغير" (Small World) في بروتوكول Gossip بتوسيع الشبكة بشكل هائل دون زيادة مقابلة كبيرة في زمن التأخير، مما يجعله مثالياً لقابلية التوسع (Scalability).

السؤال 2 : **حساب ومذكرة تقنية لبريد الجزائر**

**أ) حساب الرسائل ونسبة التوفير:**

**الرسائل في Flood:**

$$M_{flood} = N \times D_f = 16,000 \times 48 = 768,000$$

**الرسائل في Gossip:**

$$M_{gossip} = N \times D_g = 16,000 \times 8 = 128,000$$

**نسبة التوفير:**

$$\frac{768,000 - 128,000}{768,000} \times 100 = 83.33\%$$

**ب) مذكرة تقنية موجهة لإدارة بريد الجزائر:**
**الموضوع: توصية بتبني بروتوكول Gossip لشبكة تتبع الطرود.**
بناءً على التحليل الرقمي لشبكة بريد الجزائر المكونة من 16,000 عقدة، نوصي رسمياً باستخدام بروتوكول **Gossip** بدلاً من Flood. الأرقام تظهر أن Gossip يقلل عبء الرسائل بنسبة **83.3%**، مما يوفر موارد هائلة في عرض النطاق الترددي للشبكة. بالإضافة إلى الكفاءة، يتميز Gossip بـ **قابلية توسع** فائقة؛ ففي حال توسع البريد لإضافة مكاتب جديدة، لن يزداد زمن الانتشار إلا بشكل طفيف (لوغاريتمي). كما يوفر البروتوكول **موثوقية عالية** ضد الفشل؛ فإذا تعطلت بعض العقد، ستجد الرسالة مسارات بديلة تلقائياً بفضل الطبيعة العشوائية للنشر. في المقابل، يستهلك Flood موارد المعالجة في كل عقدة بشكل غير مبرر ويخاطر بانهيار الشبكة. لذا، نوصي بـ Gossip لضمان استقرار نظام تتبع الطرود وتدفق البيانات بأقل تكلفة تشغيلية ممكنة.

السؤال 3: **عاصفة البث والتخفيف**

**أ) لماذا Flood أكثر عرضة؟**
لأن كل عقدة في Flood تعيد إرسال الرسالة إلى **جميع** جيرانها (D_f = 48) دون تمييز، مما يؤدي إلى نمو أسي هائل في عدد الرسائل المكررة التي تدور في الشبكة في آن واحد، مما يسبب تشبع قنوات الاتصال وانهيار الشبكة (Broadcast Storm)
**ب)تقنية تخفيف غير مرشح بلوم:**
**التقنية: الانتشار الاحتمالي (Probabilistic Broadcast).**
**المبدأ:** تقوم العقدة بإعادة توجيه الرسالة إلى جيرانها باحتمال p (مثلاً 0.6) بدلاً من إرسالها للجميع دائماً، مما يقلل عدد الرسائل الإجمالية بشكل كبير مع ضمان وصولها للكل.

السؤال 4: **حساب الدرجة الواقعية**
**أ) حساب الدرجة D اللازمة ليكون عدد القفزات 4:**
**المعادلة:**

$$4 = \log_D(16,000) \longrightarrow D^4 = 16,000$$

**الحساب:**

$$D = \sqrt[4]{16,000} \approx 11.24$$

**النتيجة:** يجب أن يكون لكل عقدة **12 جاراً** على الأقل (D ≈ 12).
**ب) هل هذه الدرجة واقعية؟**
**نعم، واقعية جداً.** في شبكات البلوكشين الحقيقية (مثل بيتكوين)، تتصل كل عقدة عادةً بـ 8 إلى 32 جاراً. وجود 12 جاراً لكل عقدة هو تصميم متوازن يضمن سرعة انتشار عالية (أقل من 400ms) دون استهلاك مفرط للنطاق الترددي أو إرهاق موارد العقدة.

التمرين الخامس:

السؤال 1: **حساب وتحليل التجزئة (Sharding)**
**(أ) حساب الإنتاجية اللازمة (TPS):**
**المعطيات:** عدد المعاملات = 4,000,000 تذكرة، الزمن = 12 ساعة (43,200 ثانية).
**الحساب:**

$$TPS_{required} = \frac{4,000,000}{43,200} \approx 92.59 \text{ TPS}$$

**(ب) حساب عدد الأجزاء (shards) والتحقق:**
**عدد الأجزاء:** بما أن كل جزء يعالج 15TPS:

$$Number\ of\ shards = \frac{92.59}{15} \approx 6.17$$

إذن، العدد الأدنى هو **7 أجزاء**.

**التحقق مع هامش أمان 20%:**

الإنتاجية القصوى لـ 7 أجزاء =
7×15= 105TPS
الإنتاجية المطلوبة مع الهامش =

$$92.59 \times 1.20 = 111.11 \text{ TPS}$$

**النتيجة:** نلاحظ أن 7 أجزاء غير كافية لتغطية هامش الأمان (لأن 105 < 111.11). لذا، يجب رفع العدد إلى **8 أجزاء** لتوفير 120TPS.

**(ت) تحليل جدوى التجزئة:**
يعتبر التجزئة (Sharding) حلاً فعالاً لزيادة الإنتاجية الإجمالية عبر المعالجة المتوازية، حيث ترفع السعة من 15 إلى ما فوق 100 TPS في حالتنا. ومع ذلك، فإن الاعتماد على التجزئة وحدها لمتعامل نقل جزائري قد يواجه تحديات تقنية؛

فالتجزئة تزيد من تعقيد التواصل بين الأجزاء (Cross-shard communication) مما قد يرفع زمن التأخير (Latency). بالأرقام، إذا كانت الذروة في طلب التذاكر تتجاوز المعدل المحسوب، فإن التجزئة قد تصل لحدودها القصوى. لذا، يُفضل الجمع بين التجزئة و**قنوات الحالة (State Channels)** للمعاملات المتكررة بين الوكالات، أو **Rollups** لتجميع آلاف التذاكر في معاملة واحدة على السلسلة الرئيسية. هذا المزيج يضمن "قابلية توسع هجينة"؛ حيث يوفر التجزئة سعة القاعدة، بينما توفر حلول Layer 2 سرعة استجابة فورية وتكلفة أقل، مما يحمي الشبكة من الازدحام خلال ساعات الذروة ويقلل من عبء التخزين على العقد.

السؤال 2: **قنوات الحالة (State Channels)**
**(أ) التعبير عن المعاملات الموفرة:**
إذا كانت k معاملة خارج السلسلة تُختصر في معاملتين فقط (فتح وإغلاق):
**عدد المعاملات الموفرة** k=-2 معاملة.
**(ب) حساب المعاملات التي يتم تجنبها:**
**المعطيات:** k = 200 معاملة يومياً.
**الحساب:**

$$200 - 2 = 198 \text{ transaction/day}$$

**الفائدة:** هذا يقلل الضغط على السلسلة الرئيسية بنسبة 99% لهذا الزوج من الوكالات.

السؤال 3: **مرشح بلوم (Bloom Filter)**
**(أ) حساب الحجم الأمثل** m **للمرشح:**
**المعطيات:**

$$n = 18,000$$

$$p = 0.01$$

**القانون:**

$$m = -\frac{n \times \ln(p)}{(\ln 2)^2}$$

**الحساب:**

$$m = -\frac{18,000 \times \ln(0.01)}{(0.693)^2} \approx -\frac{18,000 \times (-4.605)}{0.48} \approx 172,687 \text{ bits}$$

**التحويل للكيلوبايت:**
**172687\8000** ≈21.58 kb
**(ب) العدد الأمثل لدوال التجزئة** k:

**القانون:**

$$k = \frac{m}{n} \ln(2)$$

**الحساب:**

$$k = \frac{172,687}{18,000} \times 0.693 \approx 9.59 \times 0.693 \approx 6.64$$

(نستخدم **7 دوال هاش**).

**(ت) إذا تضاعف عدد الرسائل (n = 36,000):**
• **الحساب:** باستخدام الصيغة التقريبية

$$p \approx (1 - e^{-kn/m})^k$$

القيمة داخل الأس:

$$k \times n/m = 7 \times 36,000/172,687 \approx 1.459$$

$$p \approx (1 - e^{-1.459})^7 \approx (1 - 0.232)^7 \approx (0.768)^7 \approx 0.158$$

**التعليق:** ارتفع معدل الإيجابيات الكاذبة من 1% إلى حوالي 15.8\%. هذا يعني أن المرشح سيعتبر الكثير من الرسائل الجديدة على أنها مكررة (خطأ)، مما يؤدي لحذف رسائل مهمة وفشل في مزامنة البيانات بشكل صحيح.

السؤال 4: **تركيب وتصميم الشبكة**
**(أ) حساب الـ TPS المطلوب:**
**المعطيات:**
**150000تذكرة**
**الزمن=10ساعات**
**الحساب:**

$$TPS = 150,000 \div 36,000 \approx 4.17 \text{ TPS}$$

**(ب) اقتراح عدد الأجزاء:**
• بما أن عقدة واحدة تعالج 40 \text{ TPS}، والاحتياج هو فقط 4.17 \text{ TPS}، فإن **جزءاً واحداً (أو حتى عقدة واحدة)** كافٍ تماماً من حيث الإنتاجية. ومع ذلك، ولأغراض اللامركزية وتوزيع البيانات بين الـ 60 وكالة، نقترح تقسيم الشبكة إلى **3 أجزاء** (كل جزء يغطي 20 وكالة) لضمان توازن الحمل وتوافر

البيانات.
**عدد القفزات:**

$$hops = \log_6(60) = \frac{\ln(60)}{\ln(6)} \approx \frac{4.09}{1.79} \approx 2.28$$

(أي **3 قفزات**).
**تقدير الزمن:**

$$3 \text{ hops} \times 40 \text{ ms} = 120 \text{ ms}$$

**النتيجة:** نعم، البروتوكول يضمن القيد بامتياز؛ فزمن الانتشار (120ms)أقل بكثير من الحد الأقصى المطلوب (2000ms)، مما يترك مجالاً واسعاً لعمليات معالجة المعاملة والوصول للإجماع.