اسم الطالبة : محي الدين مريم ،إقتصاد رقمي

حل امتحان

ماستر 1 اقتصاد رقمي Blockchain :

<u>التمرين 1 –</u> التسامح البيزنطي والتوافق الموزع

الشرط الأساسي : $n \geq 3f + 1$

1_ العدد الأدنى من العقد الضرورية لتحمل $f = 7$ عقد بيزنطية.

من الشرط: $n \geq 3f + 1$

$n \geq 3(7) + 1 = 21 + 1 = 22$ عقدة

2_شبكة من 40 مؤسسة، العدد الأقصى f من العقد المخترقة.

الصيغة العكسية: $f \leq (n-1)/3$

$f \leq (40-1)/3 = 39/3 = 13$

إذن $f_max = 13$ عقدة مخترقة , أقصى عدد للعقد المخترقة هو 13 عقدة.

3_شبكة من 13 عقدة

لدينا $n=13$ ونريد تحمل $f=4$.

بالحساب: $3f + 1 = 3(4) + 1 = 13$. القاعدة تقول $n \geq 3f + 1$.

هنا 13 \13 geq (الشرط محقق تقنياً كحد أدنى)، ولكن في أنظمة BFT التقليدية، لضمان استمرارية العمل (Liveness) والأمان (Safety) بشكل مطلق، يفضل دائماً أن يكون n أكبر من هذا الحد.

إذا اعتبرنا أن الشبكة الحالية (13 عقدة) هي الحد الأدنى لـ $f=4$، فهي مقبولة. لكن إذا كان المطلوب هو الوصول لشرط "أكثر من الثلث"، يفضل إضافة عقدة واحدة لتصبح $n=14$ لضمان هامش أمان.

4_ في شبكة مكونة من $n=22$ عقدة:

حساب f: من السؤال الأول، وجدنا أن $n=22$ تتحمل أقصى قيمة لـ f وهي 7 عقد.

الحد الأدنى من العقد النزيهة لضمان أغلبية بسيطة:

في أنظمة البلوكشين، الأغلبية المطلقة (أو النزيهة) هي $n - f$.

$22 - 7 = 15$

الحد الأدنى للعقد النزيهة هو 15 عقدة.

<u>التمرين 2 - إثبات العمل وتعديل الصعوبة :</u>

1_ أ _حساب عدد أجهزة ASIC \ S21 \ Pro:

معدل التجزئة الكلي للشبكة هو 800 \ EH/s (أي 800 \TH/s \ 10^6 \times).

نريد الوصول إلى 0.01\% من هذه القوة:

Target \ Hashrate = 800,000,000 \times× 0.0001 = 80,000 \ TH/s

عدد الأجهزة (حيث الجهاز الواحد ينتج 234 \ TH/s

80,000 / 234 \approx 341.88

الجواب: نحتاج إلى 342 جهازاً.

ب_ رأي معلل:

الاستثمار في تعدين البيتكوين بالجزائر صعب نسبيًا بسبب تكلفة الكهرباء، سعر أجهزة ASIC المرتفع، والمنافسة العالمية القوية (بمزارع عملاقة) تجعل من 342 جهازاً مشروعاً صغيراً جداً قد لا يغطي تكاليف الصيانة وتحديث العتاد وتناقص المكافآت (Halving). كما أن صعوبة التعدين ترتفع باستمرار، ما يقلل الربحية مع الوقت. من جهة أخرى، توفر الكهرباء الرخيصة نسبيًا قد

يساعد في تحسين المردودية إذا توفر تبريد جيد وبنية تحتية مستقرة. المشروع يحتاج رأس مال كبير وصيانة دائمة، إضافة إلى مخاطر تقلب سعر البيتكوين. لذلك يمكن اعتباره مشروعًا عالي المخاطرة ويتطلب دراسة مالية دقيقة قبل البدء.

2_ أ_ الوقت المستغرق لاختبار فضاء الـ 32^{2) nonces}):

قوة الجهاز 234 \ 12^{10 \times 234 = TH/s} تجزئة في الثانية.

Time = 2^{32} / (234 × 10^{12}) \approx 4,294,967,296 / 234,000,000,000,000 \approx 0.0000183 \text{ ثانية}

أي حوالي 18.3 ميكروثانية.

ب_ لماذا يستخدم المعدنون coinbase extraNonce؟ لأن فضاء الـ 32 \ bit للـ nonce التقليدي صغير جداً ويتم استنفاده في أقل من ميلي ثانية بواسطة الأجهزة الحديثة، لذا يستخدمون مساحة إضافية في معاملة coinbase لتغيير "جذر ميركل" والحصول على فضاء بحث جديد.

3_أ) معامل تعديل الصعوبة:

معامل_التعديل = الزمن_المستهدف / الزمن_الفعلي =

0.778 = 18 / 14

ب) هل تزداد الصعوبة أم تنقص؟

المعامل < 1 ← تنقص الصعوبة (الشبكة أبطأ من المتوقع، فتُخفَّف الصعوبة لتسريع التعدين)

ت) الصعوبة الجديدة:

الصعوبة_الجديدة = الصعوبة_القديمة × معامل_التعديل

= 50 × 10^{12} × (14/18)

= 50 × 10^{12} × 0.778

= 38.9 × 10^{12} ≈ 3.89 × 10^{13}

<u>التمرين 3 - العقد، التخزين وأشجار ميركل:</u>

1_أ) احسب المساحة التخزينية اللازمة لعقدة SPV:

المساحة = عدد الكتل × حجم الرأس

= 1,080,000 × 80 بايت

= 86,400,000 بايت = 86.4 ميغابايت

ب) مقارنة بين العقدة الكاملة والعقدة SPV وتوصية للبنك

المعيار.	العقدة الكاملة.	العقدة SPV
المساحة :	~800 MB	~86.4. GB
الأمان.	كامل (تحقق مستقل)	جزئي (يعتمد على عقد أخرى)
الاتصال.	لا يحتاج ثقة.	يحتاج لعقدة موثوقة
الموارد.	عالية.	منخفضة جداً

ب) التوصية للبنك :

بما أن البنك لديه خادم بسعة 500 \ GB وسرعة 10 \ Mbps، فإن العقدة الكاملة (Full Node) هي الأنسب لضمان الأمان والتحقق الذاتي من المعاملات دون الاعتماد على أطراف ثالثة، فمساحة الـ 500 \ GB تكفي حالياً (حيث حجم السلسلة حوالي 800 \ GB وفق المعطيات، فإنه يحتاج لزيادة السعة قليلاً أو استخدام "Pruned Node

كذلك أن البنك مؤسسة مالية تحتاج أعلى مستوى أمان

التحقق المستقل من المعاملات أمر حيوي

2_كتلة تحتوي على 4096 معاملة، شجرة ميركل بـ 32) SHA-256 بايت لكل تجزئة)

أ) عدد التجزئات اللازمة لإثبات معاملة:
عمق الشجرة = 12 = $\log_2(4096)$
عدد التجزئات في مسار الإثبات = 12 تجزئة

ب) حجم الإثبات:
حجم الإثبات = 12 × 32 بايت = 384 بايت

ت) مقارنة: حجم الإثبات (384 بايت) صغير جداً مقارنة بحجم الكتلة الكلي (4096 \× 200 \text{ بايت}= approx 819.2 \text{ كيلوبايت})، مما يوضح كفاءة أشجار ميركل في التحقق.
الإثبات يمثل فقط 384/819,200 ≈ 0.047% من الكتلة

3_عقدة SPV تتلقى إثبات ميركل يحتوي على 14 تجزئة
أ) الحد الأقصى من المعاملات التي يمكن أن تحتويها الكتلة المقابلة:
عمق الشجرة = 14
عدد المعاملات = 2^{14} = 16,384 معاملة

ب) الحجم الإجمالي للكتلة:
حجم الكتلة = 16,384 × 200 بايت = 3,276,800 بايت ≈ 3.28 ميغابايت
4_ نوع عقدة "أرشيفية" يحتفظ بالسجل الكامل + 15 تيرابايت ويتطلب 4 أسابيع متواصلة
أ) احسب معدل التحميل المتوسط:
4 أسابيع = 4 × 7 × 24 = 672 ساعة = 672 × 3600 = 2,419,200 ثانية
معدل التحميل = 15 × 10^{12} بايت / 2,419,200 ثانية
= 6.2 × 10^6 بايت/ثانية ≈ 6.2 Mbps ≈ 49.6 MB/s

ب) مقارنة مع عقدة كاملة تخزن 800 GB في 5 أيام:
5 أيام = 5 × 24 × 3600 = 432,000 ثانية
معدل العقدة الكاملة = 800 × 10^9 / 432,000 ≈ 1.85 Mbps ≈ 14.8 MB/s
العقدة الأرشيفية تستهلك ~3.4× أكثر من العقدة الكاملة.
نطاق ترددي 4 برر بالأرقام: العقدة الأرشيفية تحتاج ~50 Mbps لإتمام التزامن في 4 أسابيع، مما يجعلها مكلفة من حيث الموارد لكنها ضرورية للبحث والتدقيق التاريخي الكامل.

<u>التمرين 4 – بروتوكولات البث وعاصفة</u>

1_أ) العدد التقديري للقفزات (hops) لتغطية الشبكة بـ Gossip:
(hops = log_{D_g}(N) = $\log_8$(16,000
5 ← 4.66 ≈ = 9.68/2.079 = ln(16,000)/ln(8) = $\log_8$(16,000) قفزات

ب) زمن الانتشار للوصول إلى 99% من الشبكة:
زمن الانتشار = (60 × (1 + hops ميلي ثانية = 6 × 60 = 360 ميلي ثانية

ت) إذا تضاعف حجم الشبكة (N = 32,000):
(hops_جديد = $\log_8$(2) + $\log_8$(16,000) = $\log_8$(16,000 × 2) = $\log_8$(32,000)
= 4.66 + (1/3) ≈ 4.99 ← 5 قفزات

تعليق: النمو لوغاريتمي - مضاعفة الشبكة تزيد القفزات بـ $\log_8(2) \approx 0.33$ فقط، مما يدل على قابلية توسع ممتازة لبروتوكول Gossipو مما يجعله فعالاً جداً مع نمو الشبكة.

2_ أ) نسبة التوفير في الرسائل:

Flood: كل عقدة ترسل لـ $D_f = 48$ جار ← إجمالي رسائل $Flood = N \times D_f = 16{,}000 \times 48 = 768{,}000$

Gossip: كل عقدة ترسل لـ $D_g = 8$ أقران ← إجمالي رسائل $Gossip = N \times D_g = 16{,}000 \times 8 = 128{,}000$

نسبة التوفير = (768,000 - 128,000) / 768,000 = 640,000 / 768,000 = 83.3%

Gossip يوفر ~83% من عدد الرسائل مقارنة بـ Flood

ب) مذكرة تقنية (10-12 سطراً) – توصية بروتوكول لبريد الجزائر:

مذكرة تقنية: اختيار بروتوكول نشر البيانات

التوصية: بروتوكول Gossip

بناءً على تحليل الشبكة المكونة من 16,000 عقدة بلوكتشين:

1. الموثوقية: Gossip يضمن وصول المعلومة لـ 99% من الشبكة في ~360ms، كافٍ للتطبيقات المالية.
2. قابلية التوسع: النمو لوغاريتمي، مضاعفة الشبكة لا تؤثر تقريباً على زمن الانتشار.
3. كفاءة الموارد: يستهلك 83% أقل من الرسائل مقارنة بـ Flood، مما يوفر النطاق الترددي.
4. مقاومة الأعطال: بتوزيع البث على 8 أقران عشوائيين، لا توجد نقطة فشل واحدة.

المعايير المقارنة: Gossip: التوفير 83%، Flood: انتشار أسرع لكن يسبب عاصفة بث.

3_

أ) لماذا Flood أكثر عرضة لعاصفة البث من Gossip؟

في Flood، كل عقدة تُعيد إرسال الرسالة لـ جميع جيرانها ($D_f = 48$). هذا يُولّد نمواً أسياً في عدد الرسائل مع كل قفزة (k^{48})، مما يُشبع الشبكة بالرسائل المكررة. أما Gossip فيختار عدداً محدوداً (8) أقران عشوائيين، مما يُقلل الانتشار الانفجاري بشكل كبير.

ب) تقنية تخفيف (غير مرشح بلوم):

تقنية TTL (Time-To-Live): تُضاف لكل رسالة عداد يتناقص مع كل قفزة، فإذا وصل إلى صفر لا تُعاد إعادة إرسالها، مما يحدّ من انتشار الرسائل إلى عمق معين ويمنع عاصفة البث.

4_نريد تغطية كاملة في أقل من 400 ميلي ثانية

أ) مع Gossip، ما الدرجة D اللازمة لعدد القفزات ≥ 4؟

زمن التغطية = $(hops + 1) \times 60ms \leq 400ms$

$hops \leq 400/60 - 1 = 6.67 - 1 = 5.67 \rightarrow hops \leq 5$

لكن الشرط: $hops \leq 4$ (من حل $\log_D(N \geq 4)$)

$\log_D(16{,}000) \leq 4$

$D^4 \geq 16{,}000$

$D \geq 16{,}000^{(1/4)} = (16{,}000)^{0.25}$

$11.3 \approx 0.25^{(10^4 \times 1.6)} = 0.25^{(16{,}000)}$

إذن $D \geq 12$ (عدد صحيح)

التحقق: $\log_{12}(16{,}000) = \ln(16{,}000)/\ln(12) = 9.68/2.485 = 3.9 \leq 4$ ✓

ب) هل تبدو هذه الدرجة واقعية؟

نعم، $D = 12$ واقعية تماماً؛ فكل عقدة تحتاج لـ 12 اتصالاً نشطاً فقط، وهو معتاد في شبكات P2P (بيتكوين يستخدم $D \approx 8$-125).

التكلفة الإجمالية = 16,000 × 12 / 2 = 96,000 اتصال، وهو عبء معقول لشبكة بهذا الحجم.

<u>التمرين 5 – قابلية التوسع: التجزئة (Sharding) ومرشح بلوم:</u>

1_أ_الإنتاجية اللازمة بـ TPS:

4 ملايين معاملة / 43,200 ثانية (12 ساعة) = ≈ 92.6 TPS

لكن المعطيات تذكر 43,200 ثانية (12 ساعة)، إذن:
TPS 92.6 = 43,200 / 4,000,000
ب _عدد الأجزاء اللازمة:
عدد الأجزاء = TPS_المطلوب / TPS_لكل_جزء = 92.6 / 15 = ≈ 7 أجزاء (nshards = 7)

ت_تعتبر تقنية التجزئة (Sharding) حلاً فعالاً لزيادة الإنتاجية من خلال تقسيم الشبكة إلى أجزاء متوازية، وفي حالة نظام التذاكر المذكور (الذي يتطلب TPS 92.6)، فإن توفير 8 أجزاء بسعة TPS 15 لكل منها يغطي الاحتياج رقمياً. ومع ذلك، الرقم وحده لا يكفي لضمان استقرار النظام. فالتجزئة تزيد من تعقيد التواصل بين الأجزاء (Cross-shard communication) مما قد يرفع زمن الوصول (Latency). هنا تبرز أهمية الجمع بين الحلول؛ فقنوات الحالة (State Channels) تعتبر مثالية للمتعاملين الدائمين (مثل وكالات السفر التي تشتري مئات التذاكر يومياً)، حيث تخرج هذه المعاملات المتكررة من السلسلة تماماً ولا تسجل إلا النتائج النهائية، مما يخفف الضغط عن الـ Shards نفسها. أما الـ Rollups، فهي ضرورية لضغط البيانات (Data Compression) وتخفيض تكلفة التخزين على السلسلة الرئيسية. بالنتيجة، التجزئة توفر "المساحة" اللازمة، لكن الحلول الأخرى تضمن "كفاءة" استهلاك هذه المساحة، مما يجعل الجمع بينهما ضرورياً لمواجهة ذروة الطلب (Peak load) وضمان أمان الشبكة ضد هجمات الـ DoS.

2_أ) المعاملات على السلسلة الموفَّرة لـ 3 معاملات خارج القناة:
القناة تحتاج معاملتين فقط على السلسلة (فتح وإغلاق)، مهما كان عدد المعاملات داخلها.
3 معاملات خارج السلسلة ← معاملتان على السلسلة (فتح + إغلاق)
التوفير = 3 - 2 = 1 معاملة (بدلاً من 3)
ب) إذا تم 200 معاملة بين الطرفين يومياً:
المعاملات على السلسلة يومياً = 2 (فتح وإغلاق مرة واحدة)
المعاملات التي يتم تجنبها يومياً = 200 - 2 = 198 معاملة/يوم
3_أ) الحجم الأمثل m للمرشح:
m = -(18,000 × ln(0.01)) / (ln 2)²
ln(0.01) = -4.605
ln 2)² = (0.693)² = 0.480)
m = -(18,000 × (-4.605)) / 0.480 = 82,890 / 0.480 = 172,688 بت ≈ 172,688 بت
تحويل: 172,688 / 8 = 21,586 بايت ≈ 21.1 كيلوبايت (قريب من 8,000 بايت المذكورة في الصيغة – نستخدم النتيجة الحسابية)
ملاحظة: الرقم 8,000 بايت في النص قد يكون ناتجاً بقيم مختلفة. بقيمنا الحسابية: m ≈ 172,688 بت
ب) عدد دوال التجزئة k:
k = (m/n) × ln 2 = (172,688 / 18,000) × 0.693 = 9.594 × 0.693 ≈ 6.65 → k = 7 دوال
ت) إذا تضاعف عدد الرسائل إلى 36,000:
p_جديدة ≈ (1 - e^(-k×n/m))^k
بإبقاء m ثابتاً و k = 7:
k×n/m = 7 × 36,000 / 172,688 = 252,000 / 172,688 ≈ 1.46
p_جديدة ≈ (1 - 0.232)^7 = (0.768)^7 ≈ 0.116 = (1 - e^(-1.46))^7 أي ~11.6%
تعليق: تضاعف الرسائل يرفع معدل الإيجابيات الكاذبة من 1% إلى ~11.6%، مما يُظهر حساسية المرشح لعدد العناصر. يجب زيادة حجم المرشح أو إعادة ضبطه دورياً.
4_أ) احسب الـ TPS المطلوب:
TPS = 150,000 / (10 × 3600) = 150,000 / 36,000 = 4.17 TPS
ب) إذا كانت عقدة واحدة تعالج 40 TPS، كم عدد الأجزاء (shards):
عدد الأجزاء = TPS_المطلوب / TPS_لكل_عقدة
4.17 / 40 = 0.1 → جزء واحد (shard = 1) كافٍ
(لا حاجة للتجزئة، عقدة واحدة تكفي بمريح)

ت) هل يمكن لـ Gossip بدرجة D = 6 وتأخير 40ms ضمان زمن التأكيد < 2 ثانية؟ (N = 60)

hops = $\log_6(60)$ = ln(60)/ln(6) = 4.094/1.792 = 2.28 → 3 قفزات

زمن الانتشار = (3 + 1) × 160 = 40ms ميلي ثانية

2) 160ms << 2,000ms ثانية)

نعم، بروتوكول Gossip بدرجة D = 6 كافٍ تماماً لضمان زمن تأكيد أقل من 2 ثانية لشبكة 60 عقدة، مع هامش أمان كبير جداً (زمن فعلي ~160ms فقط).