جامعة الجزائر 3 - إبراهيم سلطان شيبوط أ.د حميدوش أمحمد السنة الجامعية: 2024 - 2025	**امتحان أعمال موجهة** بروتوكولات النشر وقابلية التوسع **البلوكشين**	كلية العلوم الاقتصادية والتجارية وعلوم التسيير ماستر 1 - الاقتصاد الرقمي

استخدام الذكاء الاصطناعي مسموح به	الآلة الحاسبة والإنترنت مسموح بهما	المدة: ساعة واحدة

الاسم واللقب: ملاك براهيمي MALAK BRAHIMI الفوج: 01_

الجزء أ - بروتوكول Gossip وقياس الانتشار (5 نقاط / 15 دقيقة)

الاجابة:

التمرين الأول

1.حساب الحد الأدنى لعدد القفزات (N = 50.000 ، D = 6)

الصيغة: $Hops \approx \log_D(N) = \log_6(50.000)$

$= \ln(50.000) / \ln(6)$

$= 10.82 / 1.79$

قفزات 6 → 6.04 =

1.2الزمن النظري للوصول إلى 95% من العقد

من الشبكة تُغطَّى عند حوالي 5 قفزات (قبل القفزة الأخيرة بمرحلة) 95%

زمن الانتشار = عدد القفزات × زمن الكمون

مللي ثانية 80 × 5 =

مللي ثانية 400 =

1.3مع: D = 10 إعادة الحساب + الفائدة والثمن

قفزات 5 → $Hops = \log_{10}(50.000) = \ln(50.000) / \ln(10) = 10.82 / 2.30 = 4.70$

الفائدة: تخفيض القفزات من 6 إلى 5 (-17%) → انتشار أسرع بزمن 400 ms بدل 480ms

الثمن: كل عقدة ترسل 10 رسائل بدل 6 → نطاق ترددي أعلى بنسبة +67%

1.4مقارنة 5.000 عقدة مقابل 50.000 عقدة (D = 6)

N = 5.000: $Hops = \log_6(5.000) = \ln(5.000)/\ln(6) = 8.52/1.79 = 4.76$ → 5 قفزات

مع N = 50.000: Hops = $\log_6(50.000) = 6.04 \rightarrow$ 6 قفزات

الفرق: قفزة واحدة فقط (+1) رغم مضاعفة حجم الشبكة 10 أضعاف

التعليق: هذا يُجسّد الميزة الرئيسية لـ Gossip → النمو اللوغاريتمي =قابلية توسع ممتازة

التمرين الثاني

Mbpsنطاق: 50 ● KB اتصالاً ● رسالة: Gossip: 6 500 ● Flood: 40 اتصالاً ● عقدة 3.000 :البيانات

2.1العدد الإجمالي للرسائل في كل بروتوكول

Flood : 3.000 × 40 = 120.000 رسالة

Gossip : 3.000 × 6 = 18.000 رسالة

2.2إجمالي البيانات المنقولة (بالغيغابايت

Flood : 120.000 × 500 KB = 60.000.000 KB = 60.000 MB ≈ 58,6 GB

Gossip : 18.000 × 500 KB = 9.000.000 KB = 9.000 MB ≈ 8,8 GB

2.3نسبة التوفير في النطاق الترددي(Flood → Gossip

التوفير = (120.000 – 18.000) / 120.000

= 102.000 / 120.000

توفير في النطاق الترددي 85% → 0,85 =

Flood يوفر 85% من النطاق الترددي مقارنة بـ Gossip

2.4هل يبقى Gossip مفضلاً مع تغطية كاملة في 200 مللي ثانية؟

زمن Gossip 80 × 6 قفزات = للتغطية الكاملة ms = 480 ms >> 200 ms

Gossip ⟶وحده لا يضمن 100% تغطية في 200 ms مع هذه الشبكة

في المرحلة الأولى Flood أو الدمج مع D الحل: رفع ⟶

الجزء ب - عاصفة البث وتقنيات التخفيف (5 نقاط / 15 دقيقة)

التمرين 3 - مرشح (Filtre) بلوم (2.5 نقطة)

عقدة بلوكشين تستقبل 20.000 رسالة/ساعة. المطلوب: مرشح بلوم بمعدل إيجابيات زائفة أقل من 0.5%.

الصيغ: $m = -(n \times \ln(p)) / (\ln(2))^2$ -////- $k = (m/n) \times \ln(2)$

الصيغة: $m = -(n \times \ln(p)) / (\ln(2))^2$

$m = -(20.000 \times \ln(0,005)) / (\ln(2))^2$

$= -(20.000 \times (-5,298)) / (0,6931)^2$

$= 105.965 / 0,4804$

≈ 220.574 bits ≈ 26,9 KB

حجم المرشح ≈ 220.574 بت ≈ 26,9KB

3.2عدد دوال الهاش المثلى k

الصيغة: $k = (m/n) \times \ln(2)$

$k = (220.574 / 20.000) \times \ln(2)$

$= 11,03 \times 0,6931$

دوال هاش k = 8 ⟶ ≈ 7,64

3.3تأثير مضاعفة nإلى 40.000 مع نفس المرشح m

الصيغة: $p \approx (1 - e^{(-k \cdot n/m)})^k$

$p = (1 - e^{(-8 \times 40.000 / 220.574)})^8$

$= (1 - e^{(-1,451)})^8$

= (1 – 0,2343) ^8 = (0,7657) ^8

≈ 0,099 ≈ 9,9% (0,5 من بدلاً%)

معدل الإيجابيات الزائفة ارتفع 20 ضعفاً عند مضاعفةn

مضاعفة n مع نفس m ترفع الخطأ 20× ← يجب توسيع المرشح عند زيادة n

دور المرشح في تقليل عاصفة البث

- **المرشح يخزن بصمات (hashes) جميع الرسائل المستلمة مسبقاً**
- **عند وصول رسالة جديدة : تُفحص في المرشح في ← O(k) فوري**
  - **إذا كانت موجودة (احتمالياً): تُرفض، لا يُعاد إرسالها**
  - **إذا كانت غائبة : تُقبل وتُنشر ← تُضاف للمرشح**

يكافح عاصفة البث Vogels , 2009 يُخفض ~80% من الرسائل المكررة Bloom Filtre

التمرين 4 - الفيضان الاحتمالي (2.5 نقطة)

1.4

رسالة 21 = 0,7 × 30 :رسائل/عقدة (احتمالي)

رسالة 30 = 1 × 30 :(Flood) رسائل/عقدة

إجمالي الشبكة (احتمالي): 12.000 × 21 = 252.000 رسالة

رسالة 360.000 = 30 × 12.000 :(Flood) إجمالي الشبكة

Flood نسبة تخفيض الرسائل مقارنة بـ 2.4

نسبة التخفيض = (360.000 – 252.000) / 360.000

= 108.000 / 360.000

تخفيض في الرسائل 30% ← 0,30 =

الكلاسيكي Flood تخفيضاً في حركة الشبكة مقارنة بـ %يُحقق 30 p = 0,7

4.3مخاطر تخفيض p إلى 0,2على تغطية الشبكة

رسائل/عقدة: 30 × 0,2 = 6 رسائل ← تخفيض 80%

إجمالي: 12.000 × 6 = 72.000 رسالة

p = 0,2 →منخفضة جداً : احتمال عدم وصول الرسالة لأجزاء كاملة من الشبكة

التغطية قد تنخفض إلى أقل من 70-75 → عقد معزولة ومعلومات ناقصة

يُعرّض الشبكة لانعدام التغطية رغم توفير 80% في الرسائل p = 0,2

4.4اقتراح قيمة p مثلى مع تبرير بالأرقام

وفقاً للدراسات p: (Saito et al., 2012) المثلى 0,55 – 0,65 =

مثال بـ:p = 0,6

رسائل/عقدة = 30 × 0,6 → 18 = إجمالي: 12.000 × 18 = 216.000 رسالة

تخفيض 40% = 360.000/ (360.000–216.000) = مع تغطية 95% <

تغطية — التوازن المثالي 95%<رسائل و 40%–يوازن بين p = 0,6

التمرين 5 - حسابات Sharding (2.5 نقطة)

البيانات: 20 TPS بدون 32 ● Sharding شريحة ● TPS/20 شريحة ● 2 Mمعاملة/يوم ● 1,80 → USD 0,04

TPS الإجمالي = 32 × 20 = 640 TPS

المعاملات/يوم = 640 × 86.400 = 55.296.000 معاملة/يوم

55,3مليون 2 << مليون → كافٍ بهامش 27,6×

Sharding 32 شريحة — 640 TPS =يستوعب 2 Mمعاملة/يوم بهامش أمان 27×

5.2 الحد الأدنى من الشرائح لاستيعاب 2 مليون معاملة/يوم

TPS المطلوبة = 2.000.000 / 86.400 = 23,15 TPS

شرائح كحد أدنى 2 → عدد الشرائح = 23,15 / 20 = 1,16

2 شرائح كحد أدنى —بينما 32 شريحة يُعطي هامش أمان ضخماً

5.3 التوفير اليومي لشركة تنجز 50.000 معاملة/يوم

بدون Sharding: 50.000 × 1,80 = 90.000 USD/يوم

يوم/USD 2.000 = 0,04 × 50.000 :Sharding مع

(–97,8%) USD التوفير اليومي: 90.000 – 2.000 = 88.000

يوم أي –97,8% في رسوم المعاملات/USD توفير 88.000

[ن 0.5] وآلية التخفيف Sharding الخطر الأمني الرئيسي لـ 5.4

(1% Attack) هجوم تركيز الموارد :الخطر

من الموارد فقط للسيطرة عليها 1/32يحتاج ← المهاجم يستهدف شريحة واحدة فقط

(Random Reshuffling) إعادة تعيين عشوائية دورية للعقد بين الشرائح :التخفيف

إعادة التعيين العشوائي للعقد يمنع تركيز المهاجم على شريحة واحدة

التمرين 6 - قنوات الحالة

• 16 USD = 2 × USD فتح/إغلاق: 8 • on-chain: 1,50 USD • معاملة/يوم 500 :البيانات
داخل القناة: 0,002 USD

6.1التكلفة اليومية بدون قناة الحالة

يوم/USD التكلفة = 500 × 1,50 = 750

6.2التكلفة الإجمالية بقناة حالة لمدة شهرين (60 يوماً)

(ثابتة لمرة واحدة) USD رسوم الفتح + الإغلاق = 2 × 8 = 16
USD معاملات داخلية: 500 × 60 × 0,002 = 60
يوماً 60 / USD الإجمالي = 16 + 60 = 76
بدون قناة — توفير هائل USD خلال شهرين مقابل 90.000 USD 76

6.3نسبة التوفير الشهري 30يوما

USD بدون قناة (30 يوم) = 750 × 30 = 22.500
USD 46 = 30 + 16 = (0,002 × 30 × 500) + (30 يوم) = 16 مع قناة
التوفير = (22.500 – 46) / 22.500 = 22.454 / 22.500
توفير شهري 99,8% ≈
من تكاليف المعاملات الشهرية 99,8%قنوات الحالة توفر

6.4الحد الأدنى للمعاملات/يوم الذي يُبرر اقتصادياً فتح القناة

تكلفة بدون قناة >شرط الجدوى (لشهر كامل): تكلفة مع قناة

$$16 + (n \times 30 \times 0{,}002) < n \times 30 \times 1{,}50$$
$$16 + 0{,}06 \cdot n < 45 \cdot n$$
$$16 < 44{,}94 \cdot n$$

من 1 معاملة/يوم تُبرر القناة ← $n > 16 / 44{,}94 \approx 0{,}36$

القناة مجدية اقتصادياً من معاملة واحدة/يوم — مربحة جداً عند 500 معاملة/يوم

الجزء د - تمرين تركيبي: تصميم بنية بلوكشين (5 نقاط / 15 دقيقة)

التمرين 7 - تصميم شبكة بلوكشين لـ Sonelgaz

7.1اختيار بروتوكول النشر مع تبرير بالحسابات

— Gossip (D=6):

Hops = $\log_6(400)$ = ln(400)/ln(6) = 5,991/1,792 = 3,34 → 4 قفزات

زمن الانتشار ≈ 4 × 50 ms = 200 ms << حد 5 ثوان ✔

عدد الرسائل = 400 × 6 = 2.400 رسالة

Flood (30 —اتصالاً):

عدد الرسائل = 400 × 30 = 12.000 رسالة (5× أكثر من Gossip)

تعقيد → $O(n^2)$ مُكلف جداً مع 400عقدة

الاختيار 4 ← Gossip (D=6): قفزات، 200ms ، 5 ×أكفأ من Flood

كافٍ وفعّال لـ 400 عقدة • 200ms زمن • 4 قفزات :Gossip (D=6)

7.2هل الشبكة بحاجة إلىSharding ؟ — تبرير بحساب TPS

TPSالمطلوبة = 300.000 / 86.400 ≈ 3,47TPS

بروتوكول Comet FT(المستخدم في شبكات خاصة) يوفر ≤ 1.000TPS

Sharding لا حاجة مطلقاً لـ → 1.000 TPS >> 3,47 TPS

لا حاجة لـ — Shardingيُبسّط البنية ويُخفض التعقيد والتكلفة

7.3تصميم مرشح بلوم مناسب(p = 0,01) ، (n = 400)

الصيغة: $m = -(n \times \ln(p)) / (\ln(2))^2$ • $k = (m/n) \times \ln(2)$

$m = -(400 \times \ln(0,01)) / (0,6931)^2$

$= -(400 \times (-4,605)) / 0,4804$

$= 1.842 / 0,4804$

≈ 3.834 bits ≈ 480 octets < 1 KB !

دوال هاش $k = (3.834 / 400) \times 0,6931 = 9,585 \times 0,6931 \approx 6,64 \rightarrow k = 7$

مرشح بلوم 1 KB >مع 7 دوال هاش يضمن إيجابيات زائفة 1% >

7.4قنوات الحالة لـ 20بلدية (200 معاملة/يوم لكل زوج) — حساب التوفير

نفرض تكلفة ● on-chain = 1,50 USD فتح/إغلاق = 16 ● USD داخل القناة = USD0,002

بدون قناة الحالة (لكل زوج/شهر):

200 × 30 × 1,50 = 9.000 USD/ زوج/شهر

مع قناة الحالة (لكل زوج/شهر):

16 + (200 × 30 × 0,002) = 16 + 12 = 28 USD/ زوج/شهر

التوفير/زوج: 9.000 – 28 = 8.972 USD/شهر(–99,7%)

إذا كانت هناك 10 أزواج رئيسية من البلديات الأكثر تبادلاً:

إجمالي التوفير = 10 × 8.972 ≈ 89.720 USD/شهر

التوصية: نعم، قنوات الحالة مُوصى بها بشدة — توفير ~90K USD/شهر لـ 10 أزواج

شبكة التنقيط لتذكير :

الجزء أ	الجزء ب	الجزء ب	الجزء ج	الجزء د	المجموع / 20
5 /	5 /	5 /	5 /	5 /	20 / .....