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: بلال ميلودي الفوج: 1

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

السياق:

شبكة بلوكشين تضم N = 50.000 عقدة، كل عقدة متصلة بـ D = 6 أقران. زمن الكمون المتوسط بين العقد: 80 مللي ثانية.

التمرين 1 - انتشار Gossip (2.5 نقطة)

1.1 احسب الحد الأدنى لعدد القفزات (hops) اللازمة لتغطية الشبكة باستخدام (Hops ≈ logD(N: (0.5 ن)

1.2 ما هو الزمن النظري للوصول إلى 95% من العقد؟ (0.5 ن)

1.3 إذا أصبح D = 10، أعد حساب عدد القفزات (hops). ما الفائدة وما الثمن؟ (0.75 ن)

1.4 ما الفرق في عدد القفزات بين شبكة بـ 5.000 عقدة وأخرى بـ 50.000 عقدة (D=6)؟ علّق على النتيجة. (0.75 ن)

حل التمرين 1 :

1- حساب الحد الأدنى لعدد القفزات (hops) :

القانون: $Hops \simeq \log_d (N)$

التعويض: $\log_6 (5000) = \frac{ln(5000)}{ln(6)}$

النتيجة: قفزات $\frac{10.819}{1.791} \simeq 6.03$

إذن، الحد الأدنى لعدد القفزات اللازمة لتغطية الشبكة هو 6 قفزات تقريباً (أو 7 لتغطية 100%).

2- الزمن النظري للوصول إلى 95% من العقد:

بما أن 6 قفزات تغطي الغالبية العظمى (أكثر من 95%)، فإن الزمن يُحسب بضرب عدد القفزات في زمن الكمون.

العملية: 6*80=480 ملي ثانية

3- إعادة الحساب إذا أصبح D = 10

عدد القفزات الجديد:

قفزات $\log_{10}(5000) \simeq 4.69$ (اي 5 قفزات عمليا)

الفائدة: عدد القفزات وزيادة سرعة انتشار الرسالة في الشبكة (الزمن يصبح80*5=400 مللي ثانية)

الثمن: زيادة استهلاك عرض النطاق الترددي (Bandwidth) وتكرار إرسال الرسائل بشكل أكبر، مما قد يؤدي إلى إرهاق الشبكة.

4- الفرق بين 5000 عقدة و 50000 عقدة:(D=6)

لـ5000عقدة: $\log_6(5000) \simeq 4.75$ (اي 5 قفزات)

لـ 50000 عقدة: رأينا أنها 6 قفزات.

- الفرق: قفزة واحدة فقط.
- التعليق: هذا يوضح قوة "قابلية التوسع اللوغاريتمية" لبروتوكول .Gossip رغم تضاعف حجم الشبكة 10 مرات، زاد عدد القفزات (وبالتالي زمن النشر) بخطوة واحدة فقط، مما يجعله مثالياً للشبكات الضخمة.

التمرين 2 - مقارنة Gossip مقابل Flood (2.5 نقطة)

شبكة بـ 3.000 عقدة. متوسط الاتصالات: 40 لكل عقدة (Flood) و6 .(Gossip) حجم الرسالة: 500 كيلوبايت. النطاق الترددي لكل عقدة: 50 ميغابت/ثانية.

2.1 احسب العدد الإجمالي للرسائل في كل بروتوكول. (0.5 ن)

2.2 احسب إجمالي البيانات المنقولة (بالغيغابايت -Gigabytes) لكل بروتوكول. (0.75 ن)

2.3 ما نسبة التوفير في عرض النطاق الترددي عند التحول من Flood إلىGossip ؟ (0.75 ن)

2.4 هل يبقى Gossip مفضّلاً إذا كانت التغطية الكاملة مطلوبة خلال 200 مللي ثانية؟ علّل. (0.5 ن)

حل التمرين 2:

1- العدد الاجمالي للرسائل:

بروتوكولflood : 3000*40=120000

بروتوكولgossip : 3000*6=18000

2- اجمالي البيانات المنقولة بالغيغابايت :

(ملاحظة: سنعتمد الحساب العشري المبسط 1gb=1000000kb لتسهيل, وحجم الرسالة 500kb=0.5mb

بروتوكولflood : 20000*0.5mb=60000mb =60gb

بروتوكولgossip : 18000*0.5mb=9000mb=9gb

3- نسبة التوفير في عرض النطاق الترددي :

العملية: $\frac{(120000-18000)}{120000} * 100$

النسبة: $\frac{102000}{120000}*100=85\%$ توفير عند استخدامgossip.

4- هل يبقى Gossip مفضلا لتغطية كاملة خلال 200 مللي ثانية

التعليل: لا، قد لا يكون مفضلاً إذا كان الزمن الحرج هو الأهم. في Gossip يتطلب الأمر حوالي 4 إلى 5 قفزات لتغطية 3000 عقدة، وإذا افترضنا أن كل قفزة تأخذ وقتاً، فقد يتجاوز 200 مللي ثانية. بينما Flood يغطي الشبكة في قفزة واحدة أو اثنتين، مما يحقق سرعة أكبر على حساب التكلفة المرتفعة للبيانات (60 غيغابايت). الاختيار يعتمد على سعة النطاق الترددي للشبكة؛ إذا كانت تتحمل 60 GB بدون اختناق، فـ Flood أسرع، وإلا سيحدث تأخير .

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

3.1 احسب حجم المرشح m بالبتات ثم بالكيلوبايت (n=20.000، p=0.005). (0.75 ن)

3.2 احسب عدد دوال الهاش المثلى k. (0.5 ن)

3.3 إذا تضاعف عدد الرسائل إلى 40.000 (أي n = 40.000) مع نفس الحجم m، ما التأثير على معدل الأخطاء؟ (0.75 ن)

3.4 ما الدور الذي يؤديه هذا المرشح (**filtre**) في تقليل عاصفة البث(Broadcast Storm) ؟ (0.5 ن)

حل التمرين 3:

1- حساب حجم المرشحm :

القانون: $m=-\frac{n*ln(p)}{(\mathbf{ln(2)})^2}$

التعويض: $m=-\frac{20000*ln(0.005)}{0.4804}$

النتيجة بالبتات: $-\frac{20000*ln(0.005)}{0.4804}$ 220.566bit

النتيجة بالكيلوبايت : 26.92 kb ≃ (220566/8)/1024

2- حساب عدد الدوال الهاش المثلى k :

القانون: $k=\frac{m}{n}*\ln(2)$

التعويض : $k=\frac{220566}{20000} * 0.693$

النتيجة: 11.02*0.693≃7.64 ناخد 8 دوال هاش

3- تأثير تضاعف عدد الرسائل إلى 40000 مع نفس الحجمm :

عند تضاعف n وبقاء m ثابتاً ،سيمتلئ المرشح بسرعة (تصبح معظم البتات 1)

•التأثير :سيرتفع معدل الأخطاء(الإيجابيات الزائفة p) بشكل كبير جداً ،مما يؤدي إلى تجاهل الشبكة لرسائل جديدة ومهمة ظناً منها أنها استقبلتها سابقاً.

4- دور المرشح في تقليل عاصفة البث:

يقوم المرشح بتخزين بصمات الرسائل التي استقبلتها العقدة مسبقاً بطريقة موفرة جداً للذاكرة .قبل أن تعيد العقدة بث أي رسالة ،تفحصها في المرشح؛ إذا كانت الرسالة موجودة ،يتم إسقاطها ولا يعاد بثها ،مما يمنع التكرار اللانهائي ويقضي على عاصفة البث.

التمرين 4 - الفيضان الاحتمالي (2.5 نقطة)

شبكة بـ 12.000 عقدة تعاني من عاصفة بث. يُقترح الفيضان الاحتمالي بحيث كل عقدة تعيد الإرسال باحتمال p،وكل عقدة متصلة بـ 30 جاراً.

4.1 مع: p = 0.7 كم رسالة متوقعة لكل عقدة؟ ما إجمالي الشبكة؟ قارن مع Flood الكلاسيكي. (0.75 ن)

4.2 احسب نسبة تخفيض الرسائل مقارنة بـ Flood الكلاسيكي. (0.5 ن)

4.3 إذا خُفِّض p إلى 0.2، ما المخاطرة على تغطية الشبكة؟ (0.75 ن)

4.4 اقترح قيمة p مثلى مع تبرير مُسنَد بالأرقام. (0.5 ن)

حل التمرين 4 :

1- p=0.7

رسائل متوقعة لكل عقدة : رسالة 30*0.7=21

اجمالي الشبكة: رسالة 12000*21=252000

المقارنة مع flood الكلاسيكي

12000*30=360000

الاحتمال اقل ب108000رسالة

2- نسبة التخفيض:

$\frac{36000-252000}{360000}$*100=30%

(وهي تكافئ الرياضي 1-p)

3- المخاطر ادا خفضp الى0.2

الرسائل المتوقعة للعقدة ستصبح

رسالة 30*0.2=6

المخاطرة: خطر انقطاع السلسلة وعدم وصول الرسالة إلى جزء كبير من الشبكة (تجزئة الشبكة Network Partition)حيث تفشل الرسالة في تحقيق تغطية كاملة.

4- اقتراح قيمة p مثلى مع التبرير:

القيمة المثلى المقترحة : p=0.3 (او0.35)

التبرير الرقمي عند p=0.3 سترسل كل عقدة الرسالة الى 9=0.3*30جيران, العدد9 يعتبر متوافقاً مع العدد الأمثل لبروتوكول) Gossip الذي يتراوح عادة بين 6 و 10 أقران) لضمان تغطية شبه كاملة. وفي نفس الوقت، سنحقق نسبة تخفيض للرسائل تصل إلى 70% (108,000 رسالة فقط بدلاً من 360,000)، موازنين بذلك بين كفاءة الانتشار وتقليل الضغط على الشبكة.

الجزء ج - قابلية التوسع Sharding: وقنوات الحالة (5 نقاط / 15 دقيقة)

التمرين 5 - حسابات Sharding (2.5 نقطة)

منصة بلوكشين بدون Sharding: 20 TPS. عدد الشرائح المقترحة: 32. و أن TPS النظري لكل شريحة هو 20TPS.

فالمعاملات المطلوبة: 2 مليون/يوم. التكلفة الحالية: 1.80 دولار/معاملة. التكلفة مع Sharding: 0.04 دولار/معاملة.

5.1 احسب إجمالي TPS مع 32 شريحة. هل يكفي لـ 2 مليون معاملة/يوم؟ (0.75 ن)

5.2 ما الحد الأدنى من الشرائح اللازمة لاستيعاب 2 مليون معاملة/يوم؟ (0.5 ن)

5.3 احسب التوفير اليومي لشركة تنجز 50.000 معاملة/يوم. (0.75 ن)

5.4 ما الخطر الأمني الرئيسي لـ Sharding وكيف يُخفَّف؟ (0.5 ن)

حل التمرين 5 :

1- اجمالي TPS مع 32 شريحة وهل تكفي:

اجماليTPSهو: 32*20=640TPS

عدد الثواني في اليوم: ثانية 24*60*60=68400

قدرة الشبكة اليومية: معاملة/اليوم640*86400=55296000

الاستنتاج: نعم, يكفي وزيادة كبيرة جدا (55.2مليون >2مليون)

2- الحد الأدنى من الشرائح لاستيعاب 2 مليون معاملة/يوم:

TPS:$\frac{2000000}{86400}$ ≈23.15

بما ان الشريحة الواحدة تتحمل 20TPS

عدد الشرائح اللازم $\frac{23.15}{20}$ ≈1. 15 نحتاج الى شريحتين (2shards) كحد ادنى

3- حساب التوفير اليومي لشركة تنجز 50000 معاملة/يوم:

التكلفة القديمة: دولار50000*1.80=90000

التكلفة الجديدة: دولار50000*0.04=2000

التوفير اليومي: دولار/يوم90000-2000=88000

4- الخطر الأمني الرئيسي لـ Sharding وكيف يُخفّف:

الخطر: هجوم 1% أو هجوم الشريحة الواحدة بدلاً من السيطرة على 51% من كامل الشبكة ،يحتاج المهاجم فقط للسيطرة على الأغلبية في شريحة واحدة صغيرة لاختراقها وتزوير المعاملات.

•التخفيف :يتم التخفيف عن طريق" التعيين العشوائي والدوري (Random Sampling/Shuffling) " للعقد والمدققين بين الشرائح المختلفة بشكل مستمر ،مما يمنع المهاجمين من التركيز على شريحة محددة.

التمرين 6 - قنوات الحالة (State Channels) (2.5 نقطة)

شركة تنجز 500 معاملة/يوم بين طرفين ثابتين (على سبيل المثال شركتان، حسابان، عميلان أي دون تغيير المستلم). و أن تكلفة المعاملة :on-chain 1.50 دولار.

تكلفة فتح/إغلاق قناة الحالة: 8 دولار لكل عملية (أي، إذا قمت بفتح حساب في يوم واحد وإغلاقه في يوم آخر، فإنك تدفع 2 × 8 = 16 دولارا كرسوم ثابتة (خارج رسوم المعاملات خارج السلسلة). تكلفة المعاملة داخل القناة: 0.002 دولار.

6.1 احسب التكلفة اليومية دون قناة الحالة (state channels). (0.5 ن)

6.2 احسب التكلفة الإجمالية بقناة حالة مفتوحة لمدة شهرين (60 يوماً). (0.75 ن)

6.3 ما نسبة التوفير الشهري؟ (0.5 ن)

6.4 ما الحد الأدنى لعدد المعاملات/يوم الذي يبرر اقتصادياً فتح القناة؟ (0.75 ن)

حل التمرين 6 :

1- التكافة اليومية دون قناة الحالة:

دولار/يوم750=1.50*500

2- التكلفة الاجماية بقناة حالة مفتوحة لمدة شهرين:

رسوم فتح واغلاق(ثابتة): دولار16=8*2

تكلفة المعاملات:

دولار60=0.002*30000=0.002*60*500

التكلفة الاجمالية: دولار76=60+16

3- نسبة التوفير الشهري:

(سنحسب على أساس 60 يوماً للحصول على النسبة الإجمالية ،وهي تعكس النسبة الشهرية لأن التكاليف تتناسب طردياً باستثناء الرسوم الثابتة الضئيلة)

التكلفة بدون قناة (60يوم):

دولار45000=60*750

التوفير المالي: دولار44924=76-45000

النسبة: $\frac{44924}{45000}$*100≈99.83%

4- الحد الأدنى لعدد المعاملات/يوم الذي يبرر اقتصادياً فتح القناة:

لإيجاد نقطة التعادل لدورة فتح وإغلاق قناة ليوم واحد:

تكلفة السلسلة الأساسية = تكلفة القناة

الحد الأدنى هو 11 معاملة)بين نفس الطرفين) لتبرير تكلفة الفتح والإغلاق.

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

التمرين 7 - تصميم شبكة بلوكشين لـ Sonelgaz

السيناريو:

أنتم مستشارون لدى شركة الكهرباء (Sonelgaz) تريد إطلاق شبكة بلوكشين لتتبع استهلاك العدادات الذكية في 400 بلدية. المتطلبات:

- 400 عقدة (بلديات)
- 300.000 معاملة/يوم
- زمن التأكيد أقل من > 5 ثوان
- ميزانية: 200.000 دولار/سنة

7.1 اختاروا بروتوكول النشر مع تبرير بالحسابات(D=6 للـ Gossip، 30 اتصالاً للـ Flood). (1.25 ن)

7.2 هل الشبكة بحاجة إلىSharding ؟ برّروا بحساب TPS. (1 ن)

7.3 صمموا مرشح بلوم (filtre de Bloom) مناسب لمكافحة عاصفة البث مع p = 0.01 و n = 400. (1 ن)

7.4 في حال وجود 20 بلدية تتبادل معاملات متكررة (200 معاملة/يوم لكل زوج)، هل توصون بقنوات الحالة؟ احسبوا التوفير. (1.25 ن)

حل التمرين 7 :

1- اختيار بروتوكول النشر مع التبرير بالحسابات:

نجتاج لحسابTPS اولا:

300000/86400≈3.47TPS

بروتوكولgossip (D=6) :

عدد القفزات: $\log_6(400)$≈3.34 (اي 4 قفزات)

ب4قفزات فقط سيتم التاكد بالتاكيد في اقل من 5 ثوان .

عدد الرسائل الاجمالي: رسالة للمعاملة 400*60=2400

بروتوكولflood (30اتصالا):

رسالة 400*40=12000

القرار: نختار بروتوكول .Gossip لأنه يحقق شرط الزمن التأكيدي بسهولة (بفضل صغر حجم الشبكة نسبياً - 400 عقدة)، ويقلل من استهلاك النطاق الترددي بشكل هائل مقارنة بـ Flood، مما يساعد في البقاء ضمن حدود الميزانية المتاحة (200,000 دولار/سنة) وتجنب تكاليف البنية التحتية الباهظة.

2- هل الشبكة بحاجة إلىSharding ؟

القرار:لا ،الشبكة ليست بحاجة إلى Sharding مطلقاً.

التبرير بحساب TPS: الشبكة تحتاج إلى معالجة 300,000 معاملة يومياً ،مما يعني TPS≈3.47 فقط .أي بلوكشين كلاسيكي بدون Sharding قادر على معالجة 15 إلى 20 TPS بسهولة (كما رأينا في معطيات التمرين5) تطبيق الـ Sharding سيعقد البنية التحتية ويزيد التكاليف والمخاطر الأمنية دون أي حاجة تقنية لذلك .

3- تصميم مرشح بلوم(filtre bloom) مع p=0.01 و n=400

حسابm :

$$m=-\frac{400*ln(0.01)}{(\ln(2))^2} = -\frac{400*(-4.605)}{0.4804} \approx 3843$$

(اي حوالي 480 بايت)

حسابk :

$$k=\frac{3834}{400}*0.693\approx 9.58*0.693\approx 6.6 : 7hash$$

4- قنوات الحالة لـ 20 بلدية بـ 200 معاملة متكررة/يوم:

التوصية: نعم ،نوصي بشدة باستخدام قنوات الحالة لهذه البلديات ،لأنها معاملات متكررة بكثافة بين أطراف ثابتة .

حساب التوفير المالي (التقريبي بناءً على أسعار التمرين6) :

اجمالي المعاملات :

معاملة/يوم 20*200=4000

التكلفة التقليدية :

دولار/يوم 4000*1.50=6000

(ما يعادل 2.19 مليون دولار سنويا - وهدا سيدمر ميزانية الشركة بالكامل!)

تكلفة قناة الحالة :

دولار/ يوم 4000*0.002=8

التوفير اليومي: يبلغ حوالي 5992 دولار يومياً (مما يضمن بقاء المشروع ناجحاً ضمن الميزانية السنوية 200 ألف دولار).

تعليمات تسليم الإجابة

شكل التسليم:

يجب تقديم ملفَين: ملف Word (docx) يحتوي على إجاباتكم كاملة مع جميع الحسابات والتعليقات، وملف PDFمُنشأ منه عبر « حفظ باسم » أو « تصدير.« PDF

تسمية الملفات NOM_Prenom_Examen_Blockchain.docx : و
NOM_Prenom_Examen_Blockchain.pdf

القناة GitHub3 :	القناة Google Drive2 :	القناة Telegram1 :
1. أنشئوا مستودعاً عاماً باسم: **Examen-Blockchain-Alger3** 2. ارفعوا الملفين بـ.Upload files 3. أرسلوا رابط المستودع في Telegram.	1. أنشئوا مجلداً باسم: **Examen_Blockchain_NOM_Prenom** 2. شاركوا المجلد مع بريد الأستاذ بصلاحية «قارئ». 3. أرسلوا الرابط في مجموعة.Telegram	أرسلوا الملفين مباشرةً في مجموعة Telegram الخاصة بالمقياس. انقروا على أيقونة المرفق ثم اختاروا « ملف » (وليس صورة) ثم أرسلوا الملفين.

تنبيه: كل عمل لم يُرسَل عبر علي الأقل في قانين في آن واحد سيُعتبر غير مكتمل

شبكة التنقيط لتذكير :

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