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: سوهيلة عبلاش Souhila Abellache الفوج: 01

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).

الحل:

1.1 حساب الحد الأدنى لعدد القفزات:

Hops=log(d)=Ln(n)/Ln(d)

بما ان : n=50000 d=6 فان

Hops=(10.8198) / (1.7918)=**6.04**

اذن عدد القفزات الازمة لتغطية الشبكة هي ≈ 6 قفزات.

2.1 حساب الزمن النظري للوصول إلى 95% من العقد:

زمن الانتشار:

T=h . latency

(ms)480= 6 . 80 = T

اذن زمن الانتشار T=480ms أي الزمن النظري يساوي0.48 ثانية

3.1 إذا أصبحD=10

Hops=Ln(50000)/ Ln(10)

Hops=4.69 ≈ 5

الفائدة:

- تخفيض عدد القفزات من 6 إلى 5 .
- انتشار أسرع.

الثمن:

- زيادة الاتصالات
- زيادة الحمل الشبكي.
- النطاق الترددي أعلى Bandwidth .10 رسائل بدل 8 لكل عقدة.

4.1 الفرق بين 5000 و50000 عقدة (D=6)

لـ 5000:

Hops=Ln(5000)/Ln(6) اذن **Hops=4.75≈5**

لـ50000:

Hops=Ln(50000) /Ln(6) اذن **Hops≈6**.

الفرق: hops1=5-6 أي الفرق قفزة واحدة فقط

ملاحظة : زيادة حجم الشبكة 10 مرات رفعت القفزات بقفزة واحدة فقط، وهذا ما ياكد قابلية التوسع.Gossip

اذ يبيّن النمو اللوغاريتمي لعدد القفزات أن بروتوكول Gossip يتمتع بقابلية توسع عالية، إذ إن زيادة عدد العقد بشكل كبير لا تؤدي إلى زيادة مماثلة في زمن الانتشار، وهو ما يجعله مناسباً لشبكات البلوكشين اللامركزية واسعة النطاق.

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 إلى Gossip؟ (0.75 ن)
2.4 هل يبقى Gossip مفضّلاً إذا كانت التغطية الكاملة مطلوبة خلال 200 مللي ثانية؟ علّل. (0.5 ن)

الحل:

2.1 حساب العدد الإجمالي للرسائل في كل بروتوكول :

N=3000

Flood : 3000 .40=120000

Gossip : 3000 . 6=18000

2.2 حجم البيانات :

500 KB لكل رسالة

Flood : 120000 . 500KB=60,000,000 KB

≈60 GB

Gossip : 18000 . 500KB=9,000,000 KB

≈9 GB

2.3 نسبة التوفير :

Saving= [(60-9) / (60)] .100 = 85

اذن نسبة التوفير = 85%

2.4 هل Gossip مفضل خلال 200ms :

لا Gossip ليس مفضل لأن:

6. 80=480ms أكبر من 200 ms

إذا التغطية الكاملة خلال 200 ms مطلوبة، Floodأقرب.

ملاحظة: يحقق Gossip خفضاً كبيراً في استهلاك الموارد، حيث يعتمد على الانتشار التدريجي عبر عدة قنوات و بما ان زمن كمون 80ms لكل قفزة فان تغطية جميع العقد يتطلب عدة قفزات أي زمن اجمالي يفوق 200 ms ما ينعكس اقتصادياً على تقليل تكلفة البنية التحتية الشبكية لذلك لا يمكنه تحقيق تغطية كاملة ضمن هذا القيد الزمني.

وعليه: يكون بروتكول أكثر ملاءمة لأنه يحقق انتشارا أسرع رغم استهلاكه الأكبر لعرض النطاق الترددي Flood

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)

الحل.

3.1 حساب حجم المرشح m بالبتات ثم بالكيلوبايت :

$M=-(20000.Ln(0.005))/(Ln(2))^2$ $m=-(n.Ln(p)/(Ln\ (2))^2$

m=220750 bits اي **m≈ 27.59 KB**

3.2 حساب عدد دوال الهاش المثلى k

$k=(m/n).Ln(2)$

$k=(220750/20000).Ln(2)$

k=7.64 أي **≈8 دوال هاش**

3.3 حساب التأثير على عدد الأخطاء إذا تضاعف n إلى40000:

P=(1-e-kn/m)k

عندما P=0.00 , n=20000 و عندما n=40000 اصبح p=12%

نستنتج ان: مع نفس m: معدل الأخطاء يرتفع بشكل كبير. تقريبًا يتجاوز 5% بدل 0.5% أي ان دقة المرشح تنخفض بوضوح.

3.4 الدور الذي يؤديه هذا المرشح (filtre) في تقليل عاصفة البث (Broadcast Storm)

- تحسين كفاءة الشبكة و تقليل Broadcast Storm.

- يقلل عدد الرسائل المتداولة في الشبكة.
- كشف وحذف الرسائل المكررة.

ملاحظة:

يعد Filter آلية وقائية تقلل الازدواجية دون تخزين كامل لسجل الرسائل، مما يحسن كفاءة الذاكرة والزمن معاً.

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)

الحل:

4.1 حساب كم رسالة متوقعة لكل عقدة مع: p = 0.7:

لكل عقدة : 30.(0.7)=21

إجمالي الرسائل: 252000=12000.21

Flood الكلاسيكي : 360000=12000.30

المقارنة : 360000>252000

4.2 حساب نسبة تخفيض الرسائل مقارنة بـ Flood الكلاسيكي:

0.3 = 360000/ (360000-252000) أي ان نسبة التخفيض تقدر بـ **30 %**

4.3 حساب المخاطرة على تغطية الشبكة إذا p=0.2

30.0.2=6

اذن : الانتشار في هذه الحالة يصبح ضعيفا أي بعض العقد لن تستقبل الرسالة . ما يجعل خطر انخفاض تغطية الشبكة مرتفع.

4.4 اقتراح قيمة p مثلى مع تبرير مُسنَد بالأرقام:

p=0.6-0.7

تحقق تغطية جيدة مع تخفيض معتبر.اي افضل توازن بين التغطية وتقليل الرسائل.

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 20 TPS.

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)

الحل:

5.1 حساب إجمالي TPS مع 32 شريحة. هل يكفي لـ 2 مليون معاملة/يوم

32. 20=640 TPS

2000000/86400=23.15 TPS

النتيجة: نعم يكفي لان 640 > 23

5.2 حساب الحد الأدنى للشرائح لاستيعاب 2 مليون معاملة في اليوم:

20/23.15 =1.16 اذن نحتاج: **2 shards**

5.3 حساب التوفير اليومي لشركة تنجز 50.000 معاملة في اليوم:

فرق التكلفة: 1.8- 1.76=0.04

لـ50000 معاملة: 50000(1.76)=88000 أي **88 ألف دولار يومياً**

5.4 الخطر الأمني لـ Sharding :

الخطر الأمني الرئيسي في أنظمة الـ Sharding هو Shard takeover attack ما يعرف بهجوم السيطرة على شريحة واحدة . حيث يكفي التحكم في اغلبية المدققين داخل شريحة واحدة فقط. وهذا ما يؤدي الى التلاعب بالمعاملات داخل تلك الشريحة مما يهدد مصداقية النظام.

التخفيف:

- توزيع عشوائي للعقد
- التحقق المتقاطع بين العقدCross-shard validation
- Resharding

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)

الحل:

6.1 حساب التكلفة اليومية دون قناة الحالة (state channels).

500 . (1.5)=750 أي 750 دولار لليوم

6.2 حساب التكلفة الإجمالية بقناة حالة مفتوحة لمدة شهرين (60 يوماً).

داخل القناة: 500.(60).(0.002)=60

فتح وإغلاق: 16 =8*2

المعاملات 0.002*60*500=60

الإجمالي: 16+60 = **76 دولار**

6.3 نسبة التوفير الشهري:

بدون قناة:

45000=(60).750

% 99= 45000/ (76-45000)

6.4 حساب الحد الأدنى لعدد المعاملات/يوم الذي يبرر اقتصادياً فتح القناة :

1.5x=16/60+0.002x أي: **x≈0.18**

نستنتج انه : عملياً معاملة واحدة يومياً تبرر فتح القناة اقتصاديا.

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 30 ،Gossip اتصالاً للـ Flood). (1.25 ن)

7.2 هل الشبكة بحاجة إلى Sharding؟ 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)

الحل:

7.1 اختيار بروتوكول النشر مع تبرير بالحسابات :

القفزات Gossip (D=6) :

Hops=log6(400)=Ln(400)/Ln(6)

Hops=3.33 اذن : **≈4 قفزات**

Flood : 400.30=12000
Gossip : 400.6=2400
12000/2400=5
أي : أقل من 5 ثوان

اذن نستنتج ان Flood مكلف وغير مناسب وعليه فان Gossip يحقق شرط الزمن لـ 400 عقدة .

7.2 هل الشبكة بحاجة إلىSharding :

86400/300000=3.47 TPS

20 TPS كافية . اذن لا حاجة لـ.Sharding

7.3 تصمصم Bloom Filte
n=400 p=0.01
$m=-(n.Ln(p))/(Ln(2))^2$
$m=-(400.Ln(0.01))/(Ln(2))^2$
m≈3834 bits
≈479 bytes

عدد الدوال k : k=m/n.Ln2
k=3840/400*0.693 =6.65 اذن **k≈7**

نسبة التخفيض :
(2400-480)/2400=0.8 أي نسبة تخفيض الرسائل المكررة تقدر **بـ 80%**

7.4 قنوات الحالة
20 بلدية
عدد الأزواج: 10=2/20
كل زوج: 200 معاملة/يوم

***بدون قنوات:**
لكل زوج : 200*(1.5)*30=9000

***بقنوات الحالة:**

16+(200*30*0.002)=16+12=28

التوفير يساوي 8972 أي **≈99%**

اذن التوفير هائل نعم موصى بها.

نستنتج انه قنوات الحالة نوصي بها بقوة لكونها تقلل عدد المعاملات على البلوكشين بنسبة تقارب99% وتخفظ الضغط على الشبكةوتوفر توكيدات شبه فولرية للمعاملات بين البلديات.

ملاحظة :

التصميم الأمثل لشبكة Sonelgaz يعتمد على دمج Gossip للنشر، Bloom Filters لتخفيف البث، PBFT للإجماع، وقنوات الحالة للمعاملات المتكررة، بما يحقق التوازن بين الأمن، الكلفة، وقابلية التوسع.

تعليمات تسليم الإجابة

شكل التسليم:

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

تسمية الملفات: NOM_Prenom_Examen_Blockchain.docx و NOM_Prenom_Examen_Blockchain.pdf

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

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 / .....**