كلية العلوم الاقتصادية والتجارية وعلوم التسيير

ماستر 1 – الاقتصاد الرقمي

الاسم :صارة	الفوج : 1
	اللقب : الشيخ

الاجابة على امتحان الاعمال الموجهة

الجزء أ – بروتوكول Gossip وقياس الانتشار

التمرين الاول

1) حساب الحد الأدنى لعدد القفزات

لدينا

N = 50000, D = 6

Hops = log(N) = log(50000) = ln(50000)/ ln(6)

ln(50000) ≈ 10.8198, ln(6) ≈ 1.7918

1.7918/ 10.8198 ≈6.04

النتيجة: قفزات 6

2) حساب الزمن النظري للوصول إلى 95% من العقد

زمن الكمون بين عقدتين = 80 ميلي ثانية.

T = Hops x Latence

T=6x80 = 480 ms. النتيجة : (0.48 ثانية)

3) إعادة الحساب عندما D = 10

Hops = log10(50000) =ln(50000)/ ln(10)

ln(50000) ≈ 10.8198, ln(10) ≈ 2.3026

5 2.3026/10.8198 ≈ 4.70

النتيجة : قفزات 5

الفائدة : تقليل زمن الانتشار إلى 1004 = 08 × 5 ميلي ثانية، أي انتشار أسرع للمعلومات.

الثمن : زيادة عدد الاتصالات لكل عقدة من 6 إلى 10 مما يزيد من:

- استهلاك الذاكرة .
- عرض الحزام المستخدم.

تعقيد إدارة الأقران .

4) مقارنة شبكة بـ 5.000 عقدة وشبكة بـ 50.000

N ل 0005

Hops = log6(5000) =ln(5000)/ ln(6) ≈ 8.5172 / 1.7918≈4.7.

:00005 ل N 6 = Hops

الفرق5 - 6 فقط قفزة إضافية1

التعليق : بالرغم من زيادة حجم الشبكة بعشرة أضعاف)من 5.000 إلى 50.000 عقدة، فإن عدد القفزات اللازمة لانتشار المعلومات لم يزد إلا بقفزة واحدة فقط. هذا يدل على أن بروتوكول Gossip يتمتع بقابلية توسع أسية مما يجعله مناسبًا ،(Scalabilité exponentielle(للشبكات كبيرة الحجم مثل البلوكتشين

التمرين الثاني:

مقارنة Gossip مقابل Flood

معطيات المسألة: عدد العقد N 0003

Flood : متوسط الاتصالات لكل عقدة DFlood = 40

. Gossip : متوسط الاتصالات لكل عقدة DGossip = 6

Mb4 Mo 5.0 = KO 005 = M نحول عادة للـ)حجم الرسالة (bits

النطاق الترددي لكل عقدة: Mbps 05 = B

1. حساب العدد الإجمالي للرسائل في كل بروتوكول

Flood إغراق

كل عقدة ترسل الرسالة إلى جميع جيرانها)بافتراض أن كل عقدة ترسلها مرة واحدة فقط في سياق نظري للانتشار الاولي

في الـ الكلاسيكي على شبكة غير شجرية، عدد الرسائل التقريبي

Nb_messagesFlood ≈ NX DFlood

لأن كل عقدة ترسل الرسالة إلى D جار، مع إهمال الاستقبالات المكررة في حساب بسيط

Nb_messages Flood = 3000 × 40

= 120000رسالة

Gossip

كل عقدة ترسل الرسالة إلى DGossip جيران فقط.

Nb_messages Gossip =N× DGossip =3000 x 6

=18000رسالة

النتيجة :

Flood: 120000. Gossip : 18000

.2 حساب إجمالي البيانات المنقولة)بالغيغابايت(لكل بروتوكول

حجم الرسالة

bits 8 x 4201 × 005 = KB 005

Mb 1.4≈ bits 000 690

Donnéesprotocole = Nb_messages × Taille_mess

Flood

DonnéesFlood= 120 000 × 500 KB

=60 000 000 KB

=60 000 MB

=60 GB

Gossip

DonnéesGossip = 18000 × 500 KB

=9 000 000 KB

= 9.000 MB

=9 GB

النتيجة

Flood: 60 GB Gossip: 9 GB

3. نسبة التوفير في عرض النطاق الترددي عند التحول من Flood إلى Gossip

النسبة المئوية للتوفير

Économie= DonnéesFlood – DonnéesGossip/Données Flood ×100

Économie=60-9/60 ×100 =51/60 ×100 =85%

النتيجة التردد النطاق عرض في توفير% 85

4. هل يبقى Gossip خلال مطلوبة الكاملة التغطية إذا كانت مفضًلا 200 ميلي ثانية ؟ علل

زمن انتشار Gossip في التمرين 1 كان

TGossip = Hops × Latence

مع N = 0003، D= 6

Hops = log(3000) =ln(3000) /ln(6)≈8.006 /1.7918≈4.4

Tgossip = 5 × 80 ms = 400 ms

هذا يفوق 200 مللي ثانية المطلوب

الـ إرسال إلى جميع الجيران مباشرة قد يصل إلى) حسب قطر الشبكة (أي : تغطية كاملة في قفزتين أو3

Tflood ≈3× 80 = 240 ms

ولا يزال أكبر قليًلا من 200 مللي ثانية، لكنه أقرب

الإجابة

لا بروتوكول Gossip لا يبقى مفضًلا في هذه الحالة لأن زمن انتشاره النظري يبلغ حوالي 400 ملي ثانية)5(قفزات × 80 ملي ثانية، وهو ضعف 200 ملي ثانية المطلوبة. في المقابل، بروتوكول Flood ينتشر بشكل أسرع)عادة في قفزتين أو ثلاث بفضل كثافة الاتصالات العالية، مما يجعله أكثر ملاءمة عندما تكون السرعة هي الأولوية القصوى، على الرغم من استهلاكه الأعلى العرض النطاق الترددي.

الجزء ب – عاصفة البث وتقنيات التخفيف

التمرين الثالث

1. حساب حجم المرشح m بالبتات ثم بالكيلوبايت

الصيغة:

m= -nx ln(p) / (ln(2))²

ln(p) = ln(0.005) ≈ -5.2983

ln(2) ≈ 0.6931, (ln(2))² ≈ 0.48045

m= 20.000 x (-5.2983) /0.48045 =105.966 / 0.48045 ≈220.5

بالكيلوبايت

220.540 ÷ 8 = 27.567≈0.027

2 .حساب عدد دوال الهاش المثلى k

الصيغة

$K=m/n \times \ln(2)$

$m/n = 220.540 / 20.000 \approx 11.027$

$k \approx 11.027 \times 0.6931 \approx 7.648 \approx 8$ هاش دوال

.3 إذا تضاعف إلى 40.000 مع نفس m، ما تأثير على معدل الأخطاء؟

عند ثبات m وزيادة n ، يزداد معدل الإيجابيات الزائفة p

حسب العلاقة $P \approx (1-e-kn/m)\ k$

تأثير ملحوظ بشكل الزائفة الإيجابيات معدل يزداد على وجه التحديد، سيرتفع من 5 % إلى حوالي 0.5%

4. ما الدور الذي يؤدي هذا المرشح في تقليل عاصفة البث ؟

يسمح مرشح بلوم للعقدة بتذكر الرسائل التي سبق استلامها وتجنب إعادة بثها عند استلامها مرة أخرى مما يقلل عدد الرسائل المكررة في الشبكة ويخفف ظاهرة عاصفة البث.

التمرين الرابع

.1 حساب عدد الرسائل

- عدد العقد = 12000
- عدد الجيران لكل عقدة = 30
- احتمال الإرسال $p=0.7$

عدد الرسائل المتوقعة لكل عقدة: $30 \times 0.7 = 21$ رسالة

إجمالي الرسائل في الشبكة: $12000 \times 21 = 252000$ رسالة

في ال Flood

$12000 \times 30 = 360000$ رسالة

2. احسب نسبة تخفيض الرسائل مقارنة بـ Flood الكلاسيكي

التخفيض نسبة = TotalFlood - Totalprob /TotalFlood × 100

= 360.000-252.000/ 360.000 × 100

= 108.000 /360.000 × 100

30%=

3. إذا خفض إلى 0.2 ، ما المخاطرة على تغطية الشبكة ؟

عند p=0.2

عدد الرسائل لكل عقدة: 30 × 0.2 = 6

الخطر

- الرسالة تنتشر بشكل ضعيف
- احتمال كبير أن لا تصل لكل العقد
- قد "تموت" الرسالة مبكرًا)عدم تغطية الشبكة بالكامل(

4. اقتراح قيمى مثلى مع تبرير مسند بالأرقام P

اختيار مناسب يكون بين 0.5 و 0.7

مثلًا عند p الرسائل لكل عقدة: 30×0.6=18

إجمالي الرسائل. 12000×18=216000

نسبة التخفيض. 360000-216000/ 360000 =%40

النتيجة

P الكبير ⇒ تغطية جيدة لكن رسائل كثيرة

P الصغير ⇒ رسائل قليلة لكن خطر فقدان التغطية

أفضل توازن: بين 0.5 و 0.7

التمرين الخامس

حساب الإجمالي TPS

TPS = 32 × 20 = 640 TPSالإجمالي

عدد المعاملات في اليوم

640 × 86400 = 55,296,000 معاملة / يوم

النتيجة : نعم، أكثر بكثير من 2 مليون – يكفي وبفارق كبير

الحد الأدنى من الشرائح

نحول المطلوب إلى TPS 2,000,000 ÷86400 ≈ 23.15 TPS

عدد الشرائح 23.1520 ≈ 1.16

نأخذ العدد الصحيح الأعلى → 2 شرائح

حساب التوفير اليومي

عدد المعاملات = 50,000 / يوم

التكلفة القديمة 50000 × 1.80 = 90,000 دولار

مع التكلفة Sharding. 50000 × 0.04 = 2,000 دولار

التوفير:

90,000 – 2,000 = 88,000 دولاريوميًا

التوفير = 88,000 دولار / يوم

الخطر الأمني الرئيس

المشكلة: هجوم على شريحة واحدة (Shard takeover)

إذا كانت شريحة ضعيفة يمكن اختراقها بسهولة

الحل:

- توزيع عشوائي للعقد بين الشرائح
- تغيير دوري (reshuffling)
- استخدام آليات تحقق قوية

التمرين السادس

1. التكلفة اليومية بدون قناة الحالة

كل المعاملات تتم على blockchain

500 × 1.50=750

إذن: دولار يوميًا 750

2. التكلفة الإجمالية لمدة شهرين)60(يومًا(مع قناة الحالة

تكلفة فتح وغلق القناة : دولار 16

تكلفة المعاملات داخل القناة خلال 60 يوم

500 × 60 = 30000

تكلفتها : 30000 × 0.002=60

إذن التكلفة الإجمالية 16+60=76

دولار خلال 60 يوم 76

3. نسبة التوفير الشهري

أولا نحسب تكلفة شهرين بدون قناة. 750 x 60 =4500

التوفير: 45000-76 = 44924

نسبة التوفير:

44924/ 45000 × 100 ≈ 99.83%

4. الحد الأدنى لعدد المعاملات اليومية الذي يبرر فتح قناة

نفترض عدد المعاملات اليومية = x

تكلفة بدون قناة لمدة 60 يوم 60(1.5x) = 90x

تكلفة مع قناة: 16 + 60(0.002x)

16 + 0.12x

حتى تكون القناة مجدية 90x = 16 + 0.12x

90x – 0.12x = 16

89.88x = 16

X = 16/89.88

X 16 89.88 ≈ 0.18

$x \approx 0.18$

بما أن عدد المعاملات يجب أن يكون عددًا صحيحًا: اذن معاملة يوميًا 1

أي ابتداء من معاملة واحدة يوميًا يصبح فتح قناة الحالة اقتصاديا

الجزء د – تمرين تركيبي تصميم بنية بلوكشين

التمرين السابع

1) اختيار بروتوكول النشر

المطلوب مقارنة بين: Flood و(Gossip (D=6

1) Flood

في Flood كل عقدة ترسل الرسالة إلى جميع العقد الأخرى:

$N(N-1)$ $400(399) = 159600$

عدد الرسائل كبير جدًا - استهلاك مرتفع للشبكة.

ب) Gossip (D=6)

كل عقدة ترسل فقط إلى 6 عقد $400\times6=2400$

عدد الرسائل أقل بكثير.

المقارنة : $159600 \gg 2400$

إذن: نختار Gossip لأنه أقل تكلفة ويحقق انتشارًا أسرع دون ضغط كبير على الشبكة.

2) هل تحتاج الشبكة إلى Sharding؟

نحسب TPS: عدد الثواني في اليوم

$60\times60\times24=86400$

TPS: $300000/86400 \approx 3.47$

هذا معدل منخفض جدا اذن:

لا تحتاج إلى لأن الشبكة تستطيع معالجة هذا الحجم بسهولة Sharding.

3) تصميم Bloom Filter

نستخدم صيغة حجم مرشح بلوم $m= -n \ln(p) /(\ln 2)2$

حيث $p = 0.01$ $\eta = 400$

$m= -400 \ln(0.01)/ (0.693)2 \approx 3837$

اذن $M\approx 3837$ bits

عدد دوال الهاش $K= m/n \ln 2$

$k=3837/400\times0.693 \approx 7$

$K\approx7$

النتيجة: نستخدم Bloom Filter بحجم 3837 bits و 7 دوال hash

4) هل نوصي بقنوات الحالة؟

لدينا 20 بلدية

200 معاملة / يوم لكل زوج .

إجمالي المعاملات: $20\times200=4000$

بما أن المعاملات متكررة بين نفس الأطراف، فإن استخدام قنوات الحالة (State Channels) مناسب لأنه يقلل عدد المعاملات على السلسلة ويخفض الرسوم.

نعم، نوصي بقنوات الحالة لأنها تحقق توفيرًا كبيرًا