

DATE / /

/ مختصر ملخصه /

/ تاریخ نویس / مکالمه / این صفحه را در

SUBJECT:

مسئلہ اول: (سونہ فریض کرو) کوڈ دیکھ بھائیں نہیں
 (header) میں کیا کوئی خودداری ہے؟

(1814 گز 965) (4) June Version ①

Previous Block Hash: پہلے بلاک کا ہش ②
 جس سے آتی ہے (Proof of Merkle Tree) ③
 = difficulty ④
 نوٹ: میں کوئی خودداری نہیں کر رہا ہوں گے ⑤
 { timestamp ⑤
 nonce ⑥

= 1 جولائی، 2009ء، 14:51:01 : 01430 یہ بلاک
 کوئی خودداری نہیں کر رہا ہے، اس کا ہش

Block Hash:

0000000094f739836057b246cdec3a532bba8b5f7b903a →
 → 530d3a29bc422c45eb

: مسئلہ ۲

Maximum Size of blocks = 1MB

Minimum size of Transactions = 250 bytes

Block Creation Rate = 1 block/min

] → Max Tx = 4000

$$\text{Throughput} \left(\frac{\text{Tx}}{\text{sec}} \right) = \frac{4000 \text{ Tx}}{\text{block}} \times \frac{1 \text{ block}}{10 \text{ min}} \times \frac{1 \text{ min}}{60 \text{ sec}}$$

$$= \frac{40}{6} \approx 6-7 \text{ Tx/sec}$$

✓ Bitcoin Address)

سوال سوم:

حکیم احمد علی یعنی میرزا سبز نعمانی را در این قسمت آدرس اسپریت برای بیت کوین و دیگر اینواع دیگر داریم.

$$\text{ذکر: } \text{Bitcoin Address} = \text{Hash}(\text{Hash}(\text{publickey})) \quad \checkmark$$

سوال چهارم:

۱) خریدار باز هم گذاشته است که این تکسٹ ۲۰۰۰ تا ۳۰۰۰ سنت دارای است اما این دستور اخراج این مقدار نمی تواند.

۲) احتمال ایجاد شواره فورک (forked transaction).

۳) احتمال ایجاد یک معامله مغایم شواره فورک (longest chain fork).

سوال پنجم:

۴) بجزیئیات کوین به این طلاق در کیف رانگر است یا اینکه ۱۰٪ داده

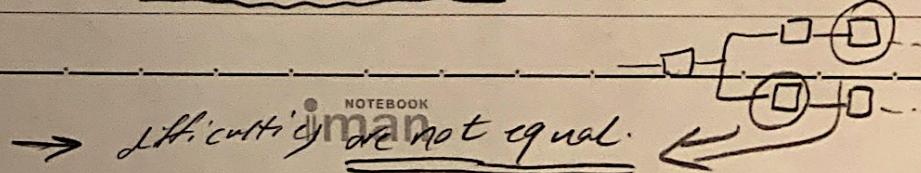
برگردانه نموده (شواره فورک) است که این تکسٹ دوباره است، در اصل سمتی برگردانه را نمی بینیم.

پیشنهاد:

$$\text{Difficulty}_{n+1} = \text{Difficulty}_n \times \frac{2016 \times 10}{\text{current 2016 blocks' time}}$$

$\underbrace{\text{time to mine current 2016 blocks.}}$

۵) از این نظر طبقه بندی کارهای دیگر برای مانع های
ادغام شدن تأثیر این نکته داشت. \rightarrow
شواره فورک داخل یک chain می باشد.

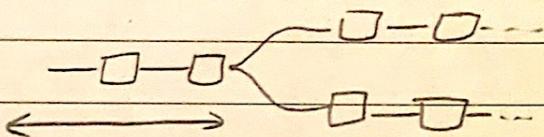


سؤال سیم: بعین اس و بعین چیز fork چونشود و دو حالت درد:

1. در این حالت fork \leftarrow soft fork ①
که اگر خوب باشد، اگر خوب نباشد رفع نمایند.

2. در این حالت fork \leftarrow hard fork ②
که اجماع ترسیم و تغییر میکنند.

در صورت رخداد fork در این ۲ مسیر از ممکنی ۱. بقیه شرکهای درینه ایجاد نمایند.



shared History

سؤال ششم:

۱. خریدار چیز را که میخواهد Miner چیزی را باید ترجیح بخواهند تا آنها را تسلیم کنند
که اینها را اگر سپاه نهادند میتوانند اینها را از خریدار جدا نمایند.

۲. به این درسته fork چیزی را که میخواهد Miner ترجیح دهد اینها را باید ترجیح دهند
و بقیه میخواهند سافر، لیکن دلخواه داشتند خود را برداشته.

۱. این حالت نه تنها برای این مورد است، بلکه دنبالهای زیادی
داریم که زنجیرهای مختلف ترجیح دارند و ناگزیر هستند که در آن موارد
UTXO را در میان اینها تقسیم کنند.

سؤال هفتم: با این نظر نهادن Probing Space را ترسیم داد:

۱. اینها را در حالتی که همان ترجیحات را داشته باشند
۲. محدوده از این ترجیحات را در حالتی که نداشته باشند

بسیاری از این احتمالات ممکن هستند اما این موارد احتمالی بودند و موقتاً این را ترسیم کردند.

سول غر :

سؤال دهم: لیے نہیں اتنے کارروائیاں داد سے سچم خیریں

- private key $(\phi \leftarrow (\text{choose } p, l \text{ in random})$ ①
 public key ϕ is elliptic curve, which is private key ϕ . ②

$$\text{publicKey} = \text{privateKey} \times \text{Generator}$$

- redundant in checksum is not useful unless it is checked at least twice ①

سُؤال یازدهم :

$\text{Private} \times \text{Generator} = \text{public}$ $\xrightarrow{\text{because of elliptic curve multiplication}}$ \rightarrow hard to find pr key through pub key.

$$\text{Hash}(\text{Hash}(\text{public key})) = \text{Bitcoin Address}$$

• جعل العثور على مفتاح خصوصي من الصعب جداً very hard to find public key through Bitcoin Address.

سوال ۱۱: ساخت اداسن private key را آن آدرس یعنی چهل رایج بگرد:

~~public key = private key Generator~~
elliptic curve

Bitcoin Address = Hash(Hash(public key)) added checkSum.

۱۱۰ مانند این قسم کیسے اور اسیں چیز بولتے ہیں دست اور کھلکھل کر

: ~~incorrect~~ checkSum : 15 clear

١) سُجْنَتْ خَادِمَةً، أَرْسَلَتْهُ (جَاءَهُ)

لِهِ مُسْرِفٌ مُّلْكٌ ①

• \Rightarrow human readability is it. (P)

جزئیات از این آذیت سیکلوں، public را بخواهد، حسنه دارم:

Bitcoin Address = Hash(Hash(publickey))

و دارای یک Hash می باشد و ممکن است از آن برای این داده ها استفاده شود.

شبکه‌ی peer to peer میان این دو طبقهٔ شبکه‌ی محدود و غیرمحدود است. در شبکه‌ی محدود، میزبانی که می‌خواهد ترانسیس برای دیگر میزبانان انجام داد، باید خود را میزبانی معرفت کند. در شبکه‌ی غیرمحدود، میزبانی که می‌خواهد ترانسیس برای دیگر میزبانان انجام داد، باید میزبانی را که می‌خواهد ترانسیس برایش انجام داد، شناسد. میزبانی که می‌خواهد ترانسیس برای دیگر میزبانان انجام داد، باید میزبانی را که می‌خواهد ترانسیس برایش انجام داد، شناسد.

سوال ۱۶ :

جزءی از تراکنش درونهای Pec می‌باشد که محیر است. جمله این
جزءی از تراکنش ماده‌های تراکنده سیزده ایام و دنیانه Pec Miner
تغییر شرود و بحسب رایاست نیز ماینر ناقص بود. این موقوفه از پسی تغییر نموده است.
بررسی از این امر

سوال ۱۷ :

که ماینر باید ماده‌های تراکنده را در این ده روزه و علاوه بر آن در زمانی مخصوص نیز فراهم نماید.
و زمانی در زمانی خاص تراکنده :

ارزشی دارد: $\left\{ \begin{array}{l} \text{Miner بوقت خود را proof of work بیان کرده است.} \\ \text{درین: تغییر ماینرها این را تضمین نمایند.} \end{array} \right.$

بلک و بلاک‌چین صافی دارند و بازیه همچنان برای خود می‌گذشت.
و ماینرها خود را درین را تضمین نمایند.
و این را دریافت کنند.

سوال ۱۸ : خیرخواسته بیو: mine را بنام، ماینر یادداشت را نمایند که به این

- ① block را درین را نسبت سود.
- ② ماینرها را تضمین نمایند.

زیرا شدید دلالات آفرین است و بین است در جای دیگری بکار رفته نمایند و باید در حدود چیزی خوارد
باشند می‌گذرد و می‌گذرد
کافی همیشگز در این توانان نکنند و آن را تضمین نموده آن بکار مانند است.

(ادله روشیات در مختصر عبار)

سؤال ۱۹: میں اسے میں آتا ہے جو میں دھن دیتا ہو تو دھن بلٹر

کا اور طبقہ سارے ترانزنس کا دھن رکھتا ہے، میں اسے دھن بلٹر کہا جائے دیں
جس کے لئے اس نے میں دھن دیتا ہے اس سے دھن دیتا ہے تو دھن بلٹر کا شکر

بے پریمینیم بیت کوین دھن دیتا ہے، بیول را در ترانزنس کی تاریخ کیلئے دھن بلٹر کی نظر
کے لئے اپنے UTXO کا اسکے زیرِ نظر دھن دیتا ہے، سیکونڈ تاریخ کی نظر دھن دیتا ہے
کہ دھن بلٹر کا شکر کیا ہے اس کی تاریخ کی نظر دھن دیتا ہے

این کا double spending کی وجہ بیان دیجئے جو دھن دیتا ہے بیت کوین
کو زنگوں کا ایجاد کر سکتے ہیں بٹری (fork) کو زنگوں کا ایجاد کر سکتے ہیں
کہ زنگوں کا ایجاد کر سکتے ہیں اور دھن دیتا ہے صورت فیکل اور ترانزنس کو زنگوں کا ایجاد کر سکتے ہیں جو دھن دیتا ہے

مسئلہ ۲: سید بیان حبیبی خان نے دیپوز ۱۷ نوامبر، ۲۰۱۷ء کی تاریخ پر hard fork خواہ دیکھا۔

دھن دیکھا hard fork کا نتیجہ ہے سختی جدید ایجاد کیا گی اور ایک جو ہے hardfork کا نتیجہ ہے سختی جدید ایجاد کیا گی

اسے است. Bitcoin، hard fork کا نتیجہ Bitcoin Cash ہے، نسبت compatible ہے

soft fork کا نتیجہ ہے soft fork کا نتیجہ ہے soft fork کا نتیجہ ہے soft fork کا نتیجہ ہے

soft fork کا نتیجہ ہے soft fork کا نتیجہ ہے soft fork کا نتیجہ ہے soft fork کا نتیجہ ہے

"2015 BIP66 Blockchain fork" ← 2015

/ منع دہندا ہے /

(ادامہ سوتھات و مصادر بعد)

سؤال ۲۳ (عکس ۱۳۱ این پرسش است):

حالات مختلفی که در ترتیب حاصل خواهد شد و این وجود داشت
 fee گیرنده می‌باشد. می‌توانید میزنهای مخصوص آنها را در اینجا نمایش دهید.

fee سبب انتشارها در شبکه است.

now



motivation: 1. Tx's fee

2. reward of block mining (currently 6.25 Bitcion per block)

future



motivation: Tx's fee

سؤال ۲۴ (عکس ۱۳۲ این پرسش است):

خدمات زیرمذکور در بروکر دست داشت و توان برای زیستی miner با توان برای زیستی عکسواره سیمه توکاره سیم. همان‌طور Miner های احتمال سیمه توکاره نسبت به (برای زیستی) عکسواره کمتر است و دست نسبت ایجاد رساندن می‌نمایند. "زیسته" برقرار برای زیسته، "عکسواره" برقرار برای عکسواره، "توکاره" برای توکاره، "صوفا" برای صوفا، "کلین" برای کلین است. می‌توانید اینها را در شبکه نمایش دهید.

سؤال ۲۵ (عکس ۱۳۳ این پرسش است):

در سیستم account based هر کاره که انجام داده شود، می‌داند و موجودی آن بر اساس تراکنش هایم و زیاد نمود. این account base یعنی etherium در این سیستم، UTXO است. آنچه در سیستم UTXO است، اینکه اینها را در هر تراکنش تبدیل نمی‌کنند بلکه ایجاد نموده هر کس اینها را داشته باشد که با آدرس UTXO مطابق داشته باشد. این اینها را در تراکنش اضافی نمایند. که توجه کنید هر UTXO باید آدرس داشته باشد.

ستولن ٢٧ (عادي + ١٣٦ من مرسى اسماوة) :

از ایجاد این دارم هر 10 دسته ای از مکانیزم های ایجاد شده در نهاد اداری به نام آن تعریف و 10 دسته های مکانیزم های ایجاد شده در نهاد اداری به نام آن تعریف شد.

$$P\{ \text{rej.} = 10 \text{ (yearly)} \} = 1 - e^{-1} \approx 63\%$$

$$f_{\zeta}(k; \lambda) = \frac{\lambda^k e^{-\lambda}}{k!}$$

سؤال ٢٨ (مقدمة في علم الاجتماع) :

با توجه به اینکه آن بیداری که نیاز است باید مانند آن باشد و میتواند جزو برآور بود رئیس (من) باش
نمایش نمود و خوشحال شوند باشد و میتوانند طبق آن نسبت نسبت بزرگ تر داشته باشند و میتوانند
برآور نمایش نمود و خوشحال شوند باشند و میتوانند طبق آن نسبت نسبت بزرگ تر داشته باشند و میتوانند
برآور نمایش نمود و خوشحال شوند باشند و میتوانند طبق آن نسبت نسبت بزرگ تر داشته باشند و میتوانند

- (۱) آنچه عیوب از اینهاست روش سنجشی است که بازه‌ی افراد تسبیم شوند و
با توجه به آنچه در میان افراد تسبیم شده بروز نمایندگی داشتند.

نحوه ترتیب بینیم که: X به این متریال تعریف شده است
 X به عنوان عارز بر دست آورده باشد و از این

مسئلہ ۲۹ (معادل بی ۱۷ اسے پرستک آئندھی) :

چنانچه در رایج Δ لعنت و هر روز سنه هزاری بهترین خود هم ایشان را ترسیل نمیکنند، خانواده داشت که ندو ببار این متفاهه باشد آن باید که عزیزی همچو ما تولید نموده است ما نظریه دین و بنی رسیلم به صورت درست مسخه ای و متفاهه ای را درین طبقه قرار نمایند و طبق آن میباشد دستور.

سؤال ۳: میز سینه (MemPool)

میز سینه (Memory Pool) MemPool
در این میز سینه اینها درون ماینینگ دارند.
در این میز سینه اینها خود را خود میزند و هر کسی میتواند اینها را بخواهد.
برای میز سینه
Mining Pool

~~~

: (Bitcoin Script)

ScriptSig میز سینه است که درون آن اینها را خواهند داشت.

ScriptSig <'0kapi'>

note: Hash('0kapi') = 0xeb271cbcc1190d0b0e6212903e29f22e5 ~  
~78ff69b

b. میز سینه را باز کنید و درون آن از نوع password است.  
که درون آن ScriptSig است.

c. درون آن از نوع pass است و خود را در آن آنها با خود دارند.  
که درون آن ScriptSig است و درون آن از نوع pass است.  
که درون آن از نوع pass است و خود را در آن آنها با خود دارند.  
که درون آن از نوع pass است و خود را در آن آنها با خود دارند.