ایرادات رایج سوالات تئوری

سوال اول

راه حل مطلوب:

اگر که تعداد بیت‌های خروجی n بیت باشد، اندازه فضای حالت خروجی $N = 2^n$ می‌شود.

احتمال آنکه m عمل هش کردن تلاقی با یک‌دیگر نداشته باشند، به صورت زیر است:

$$(\frac{N-0}{N})(\frac{N-1}{N})(\frac{N-2}{N})\dots(\frac{N-(m-1)}{N})$$

توضیح رابطه: جمله اول حاکی از احتمال نشستن هش اول در فضای حالت بدون تلاقی است. این هش می‌توان هر جا از فضای حالت بنشیند. هش دوم فقط در جای هش اول نمی‌تواند بنشیند، هش سوم در جای هش اول و دوم، همین‌طر تا هش m که در m-1 جای قبلی نمی‌تواند بنشیند.

عبارت بالا را به صورت زیر می‌توان نوشت.

$$(1-\frac{0}{N})(1-\frac{1}{N})(1-\frac{2}{N})\dots(1-\frac{m-1}{N})$$

احتمال مطلوب ما یعنی رخ دادن پیش‌آمد تلاقی به صورت زیر است:

$$p = 1-(1-\frac{0}{N})(1-\frac{1}{N})(1-\frac{2}{N})\dots(1-\frac{m-1}{N})$$

طبق سری تیلور می‌دانیم $e^x \approx 1+x$ پس می‌توان رابطه بالا را به صورت زیر نوشت.

$$p \approx 1-e^{-\frac{0}{N}}e^{-\frac{1}{N}}e^{-\frac{2}{N}}\dots e^{-\frac{(}{m}-1)N}$$

پس:

$$p \approx 1-e^{-\frac{0+1\dots(m-1)}{N}} = 1-e^{-\frac{m(m-1)}{2N}}$$

دوباره طبق سری تیلور:

$$p \approx 1-(1-\frac{m(m-1)}{2N}) = \frac{m(m-1)}{2N} \approx \frac{m^2}{2N}$$

پس اگر این مقدار مساوی 0.5 بخواهد باشد:

$$\frac{m^2}{2N} = \frac{1}{2} \rightarrow m^2 \approx N \rightarrow m \approx \sqrt{N} \rightarrow m \approx 2^{\frac{n}{2}}$$

استناد به خود مسئله یا پارادوکس روز تولد برای حل این سوال منطقا نمره‌ای ندارد.

سوال دوم

تراکنش‌ها در بلاک‌چین ذخیره می‌شوند. اینگونه نیست که ذخیره نشوند. در segwit بخشی از داده‌ها در بلاک‌چین ذخیره نمی‌شود و نه در مکانیزم اصلی بیت‌کوین.
هش داده‌های تراکنش که حاوی scriptSig چه در ورودی و چه در خروجی که خود شامل امضای تراکنش می‌باشد امضا می‌شود.
کاربر هش تراکنش را امضا می‌کند در scriptSig.
بعد از به دست آوردن هش نامبرده تازه در مرحله mine کردن بحث merkle tree مطرح می‌شود.
تحت هیچ عنوان کلید خصوصی در بلاک‌چین قرار نمی‌گیرد. در این صورت همه چیز به هم می‌ریزد.

سوال چهارم

عدم بیان امکان اینکه الگوریتم false positive بدهد منجر به کسر ۲۵ نمره از این سوال می‌شود.

سوال پنجم

در شش مورد کاربرد دارد که بیان ۳ تا از آن‌ها الزامی بوده است.

1. -در فرآیند استخراج (استفاده از Ethash
2. در ایجاد ساختار داده Patricia Merkle Tree
3. در ساختار داده (serialize Simple) SSZ که البته این ساختار در زنجیره Chain Beacon کاربرد دارد.
4. - در امضا و اعتبارسنجی قراردادهاي هوشمند و تراکنش‌ها در شبکه اتریوم

5. در ساخت آدرس که ۱۶۰ بیت سمت راست از کلید عمومی است که ابتدا توسط ECDSA رمزنگاري شده است و سپس توسط hash Keccak، هش آن محاسبه شده است.
6. استفاده از هش در ساختار block: استفاده از هش block قبلي در ساخت block جدید، در فیلد root_state که هش ریشه object state است، در فیلد root_block_beacon از فیلد data از فیلد attestations از فیلد body که هش ریشه block Beacon است و در بخشهاي ديگري در ساختار يك block