دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)

دانشکدهٔ مهندسی کامپیوتر و فنآوری اطلاعات

مبانی امنیت اطلاعات

(ترم بهمن ۹۸)

CryptoCurrency

نستوه طاهری جوان

nastooh@aut.ac.ir

رمز-ارز

- ✓ خصوصیات رمز-ارزها
  - ارز (پول) مجازی هستند.
  - تاریخچهٔ آنها را می توان به ای-کش در ابتدای دههٔ ۸۰ میلادی نسبت داد.
  - عموما به صورت توزیع شده مدیریت می شود.
  - عموما مبتنی بر فناوری بلاک-چین هستند. (الگوریتم های رمزنگاری نقش اساسی در رمز ارزها دارند)
  - عموماً ارزهای بدون پشتوانه هستند. (بر خلاف ارزهای عادی که دولت ها پشتوانه هایی مانند طلا برای آنها در نظر می گیرند.)
  - عموماً بانک های مرکزی کشورها قدرتی برای کنترل بر روی آنها ندارند.
  - عموماً باید به مرور زمان (هر یک به روشی) استخراج شوند.
  - عموماً مقدار (تعداد) نهایی آنها به صورت عددی محدود است.
    - اما نرخ تبدیل انها به ارزهای دیگر (مانند دلار) متغییر است.

nastooh@aut.ac.ir

Bit-Coin

- ✓ خصوصیات بیت کوین
  - در سال ۲۰۰۹ توسط ساتوشی ناکاموتو!!! ابداع شد. (هویت ناشناس)
  - در واقع نوعی پول بی پشتوانه است.
  - کاملا غیر-متمرکز کار می کند.
  - مبتنی بر بلاک-چین است.
  - هیچ کشوری بیت-کوین را به عنوان پول به رسمیت نمی شناسد.
    - آیا بیت کوین پول است؟ یا کالا؟

nastooh@aut.ac.ir

Bit-Coin

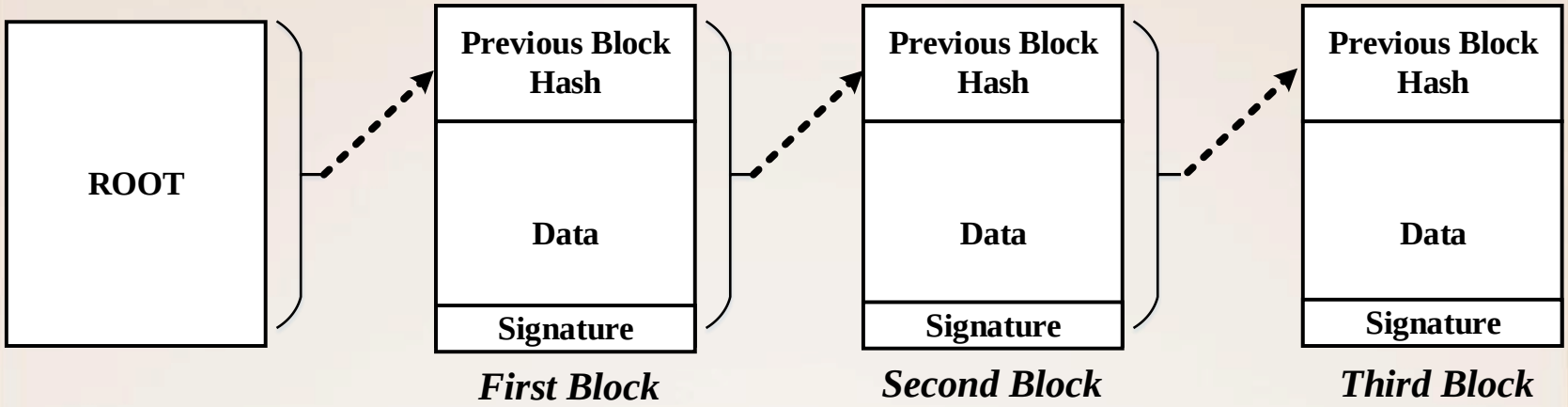
- ✓ جزئیات بیت کوین
  - برای درک ابتدایی از عملکرد فنی بیت کوین، باید ابتدا با مفاهیم زیر آشنا بود
    - رمزنگاری کلید عمومی (نامتفارن)
    - توابع در هم ساز
    - امضای دیجیتال
    - **بلاک چین**

Bit-Coin

- مقدمه ای بر بلاک چین
  - یک سیستم توزیع شده برای ثبت و نگهداری داده ها
  - اصالت سنجی داده ها به سادگی قابل انجام است.
  - دستکاری و خرابکاری در داده ها تقریبا غیرممکن است.
  - هیچ مدیریت متمرکزی ندارد.
  - داده ها در قالب تعدادی بلاک متوالی ذخیره می شوند.
  - هر بلاک، بلاک بعدی را تائید می کند.

Bit-Coin

- ✓ مقدمه ای بر بلاک چین
  - یک بلاک چین بسیار ساده شدهٔ فرضی



- هر کس می تواند به راحتی با چک کردن هش بلاک ها، صحت زنجیره را بررسی کند.
- هر بلاک، با این روش صحت و دست نخوردگی بلاک های قبلی را تایید می کند.
- نفوذگر برای تغییر در داده ی یک بلاک باید تمام بلاکهای بعدی را دستکاری کند.

nastooh@aut.ac.ir

Bit-Coin

- ✓ اصول حاکم بر بیت کوین
  - در بیت کوین، عملاً بلاک ها باید ساخته شوند. چگونه؟
    - برای ایجاد هر بلاک محاسبات خاصی صورت می گیرد.

  - محاسبات لازم برای ساخت یک بلاک به بیان ساده از جنس زیر است:

پیدا کردن یک دادهٔ ورودی برای یک الگوریتم هَش به صورتی که خروجی هَش فرمت خاصی داشته باشد.

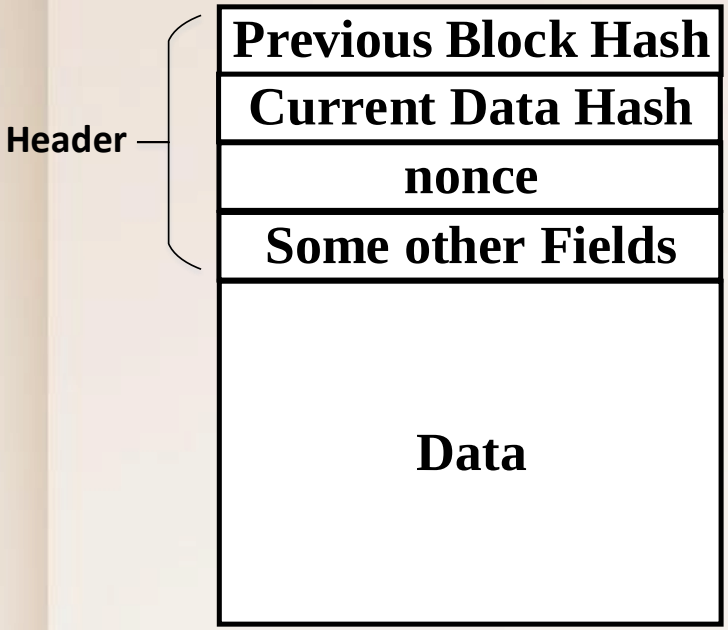
مثلاً خروجی هَش باید به تعداد مشخصی صفر ختم شود!

بلاک چین هایی که در آنها برای ساخت یک بلاک، حجم زیادی محاسبات نیاز است، اصطلاحاً مبتنی بر اثبات کار هستند.

nastooh@aut.ac.ir

Bit-Coin

- ✓ اصول حاکم بر بیت کوین
  - فرمت **ساده شدهٔ** هر بلاک در بیت کوین



نکات اولیه:

- محتوای فیلد دادهٔ بلاک جاری هنگام ساخت بلاک فیکس است.
  این داده حاوی چیست؟؟؟
- هَش دادهٔ بلاک جاری نیس فیکس است.
- هَش بلاک قبل، هنگام ساختن بلاک جاری فیکس است.
- مقادیر فیلدهای دیگر هنگام ساخت بلاک جاری فیکس است.
- فیلدهایی مانند تایم، یا ورژن و ...
- مقدار فیلد nonce باید حدس زده شود.

بگونه ای که مقدار عددی هَش کل بلاک، از یک حد آستانه کوچکتر باشد.

برای این منظور باید مقدار فیلد nonce را با سعی و خطا حدس زد... بارها و بارها...

nastooh@aut.ac.ir

Bit-Coin

✓ اصول حاکم بر بیت کوین

نکات تکمیلی:

- فرض کنیم بلاک nام، ساخته شده است، حال برای ساخت بلاک n+1ام، در واقع یک مسابقهٔ جهانی برقرار است.

  به این ترتیب که هر کسی که زودتر بر اساس هَش بلاک nام، و محتوای دادهٔ بلاک پیشنهادی خود، مقدار nonce مناسب خود را پیدا کند، برندهٔ مسابقه خواهد شد و بلاک n+1ام را ساخته است.

- پس از کشف بلاک n+1ام توسط برندهٔ خوش شانس، مسابقه ای جدید (بر اساس هَش بلاک n+1) شروع می شود و باز هم باید nonce مناسب حدس زده شود تا بلاک n+2 ساخته شود...

- برندهٔ ساخت هر بلاک، مقداری بیت کوین به عنوان جایزه دریافت می کند!!!
  - در واقع بیت کوین ها در این مرحله ایجاد می شوند.
  - برندهٔ جایزه می تواند بعداً بیت کوین های خود را بفروش برساند.

nastooh@aut.ac.ir

Bit-Coin

✓ اصول حاکم بر بیت کوین

- حساب کاربری در بیت کوین
  - هر حساب کاربری شامل یک جفت کلیدخصوصی-عمومی است که در کیف پول نگهداری می شود.
- عملاً کلید عمومی شما، نشانی شما برای دریافت بیت کوین در تراکنش ها است.
  - کلید عمومی در بیت کوین ۳۳ کاراکتر است.
- کیف پول
  - نرم افزاری که مدیریت تراکنش ها را انجام می دهد.
- واحد خرد بیت کوین، **ساتوشی** نام دارد.
  - هر ساتوشی 0.00000001 بیت کوین است.
  - در حقیقت هر صد میلیون ساتوشی، یک بیت کوین است.

nastooh@aut.ac.ir

Bit-Coin

- ✓ اصول حاکم بر بیت کوین
  - **گره ها**
    - هر کاربر متصل به شبکه بیت‌کوین، یک گره (node) به‌شمار می‌رود.
    - در شبکه بیت‌کوین هر گره باید با چند گره دیگر در ارتباط باشد.
    - به گره هایی که کل بلاک چین بیت کوین را دانلود کرده باشند، اصطلاحا Full node گویند.
      - سایر گره ها اصطلاحاً لایت-نود نامیده می شوند.
    - فول-نودها با نرم افزار bitcoin core که در سایت Github به صورت متن-باز قرار دارد، با یکدیگر در ارتباط هستند.
    - کل بلاک چین بیت کوین، امروز حدود ۲۰۰ گیگابایت حجم دارد.

nastooh@aut.ac.ir

Bit-Coin

✓ اصول حاکم بر بیت کوین

○ نقل و انتقال بیت کوین

- انتقال دهنده (فروشنده) به کمک کلید عمومی (آدرس) گیرنده تراکنش را ایجاد می کند.
- تراکنش ها در جایی به عنوان mempool نگهداری می شوند.
- ماینرها هنگامی که یک بلاک کشف میکنند، تعدادی تراکنش از mempool انتخاب کرده و به عنوان بدنهٔ بلاک خود به کار می برند.
- هر فروشنده مقداری کارمزد برای تراکنش خود انتخاب می کند.
  - ➢ کارمزد می تواند حتی صفر باشد.
- ماینرها سعی می کنند تراکنش هایی را برای بلاک خود انتخاب کنند که کارمزد بیشتری داشته باشد.
- تراکنش های با کارمزد پایین، ممکن است مدت زیادی منتظر بمانند.
- هنگامی که شبکه شلوغ باشد (خرید و فروش زیاد باشد)، مقدار کارمزد بالاتر می رود.
- یادآوری یک: هر بلاک حدود ۴ هزار تراکنش جا دارد.
- یادآوری دو: در روز حدودا ۱۴۴ بلاک کشف می شود.

nastooh@aut.ac.ir

Bit-Coin

✓ اصول حاکم بر بیت کوین

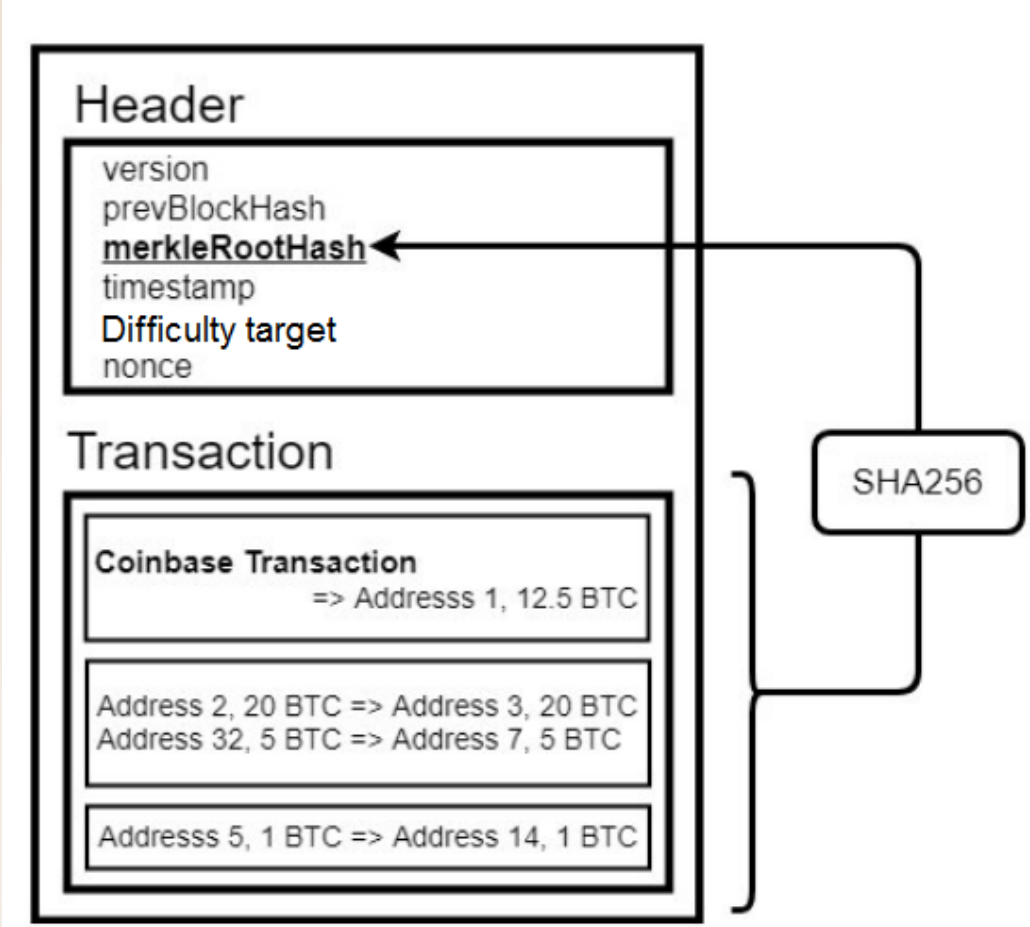
○ ساخت بلاک (ماینینگ)

- اولین بلاک بیت کوین، بلاک جنسیس نام دارد.
- ماینر ابتدا تراکنش های مورد نظرش را انتخاب می کند و بعد شروع به انجام محاسبات می کند.
- هر ماینر ابتدا یک تراکنش ۱۲.۵ بیت کوینی برای خودش، در ابتدای تراکنش ها قرار می دهد.
  - ➢ جایزهٔ کشف بلاک!
- هنگامی که یک ماینر یک بلاک را کشف کرد، آن را برای همسایه های مستقیم خود ارسال می کند.
- هر گره بعد از بررسی صحت بلاک، آن را برای همسایه های خود ارسال می کند.
  - ➢ کشف این بلاک به سرعت در شبکه منتشر می شود، در حد یکی-دو ثانیه.
- بعد از کشف یک بلاک، ماینرها دنبال تراکنش های دیگر از mempool رفته و ساخت یک بلاک جدید را شروع می کنند.

nastooh@aut.ac.ir

Bit-Coin

- ✓ اصول حاکم بر بیت کوین
  - فرمت بلاک



nastooh@aut.ac.ir

Bit-Coin

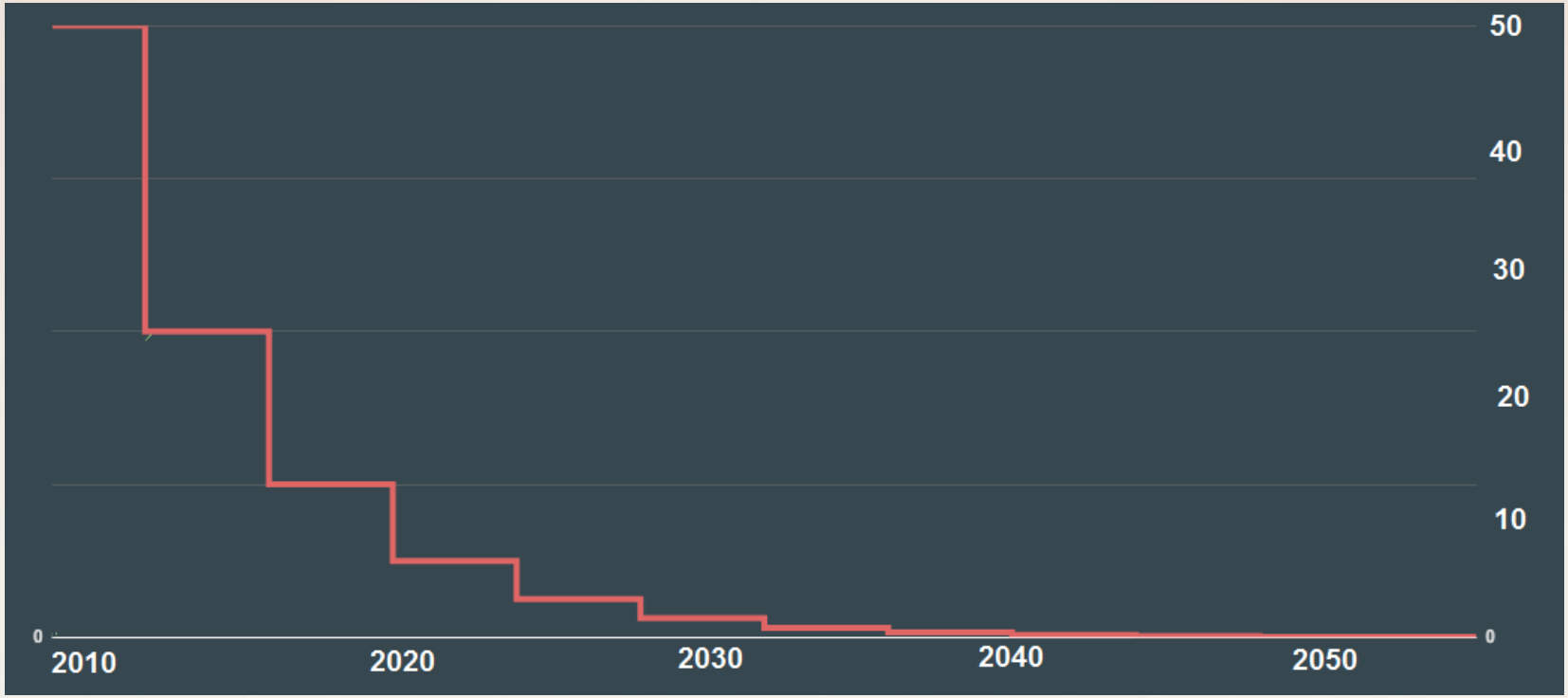
- ✓ اصول حاکم بر بیت کوین
  - **جایزهٔ ساختن بلاک**
    - پاداش کشف بلاک به حساب ماینر ریخته می شود.
      - در قالب یک تراکنش در ابتدای یک بلاک که به CoinBase معروف است.
    - هر ۲۱۰ هزار بلاک، پاداش نصف می شود. (حدود ۴ سالی یک بار)
    - این جایزه بین سال‌های ۲۰۰۹ تا ۲۰۱۲، تعداد ۵۰ بیت‌کوین برای هر بلوک بود.
    - بین ۲۰۱۲ تا ۲۰۱۶ به ۲۵ بیت‌کوین رسید.
    - از سال ۲۰۱۶ به مقدار ۱۲.۵ بیت کوین کاهش پیدا کرد.
    - در ماه می سال ۲۰۲۰ (اواسط اردیبهشت ۹۹) به مقدار ۶.۲۵ کاهش یافت.

nastooh@aut.ac.ir

Bit-Coin

- ✓ اصول حاکم بر بیت کوین
  - جایزهٔ ساختن بلاک

نمودار کاهش جایزهٔ کشف بلاک در طول زمان



nastooh@aut.ac.ir

Bit-Coin

- ✓ اصول حاکم بر بیت کوین
  - **سختی کشف یک بلاک جدید (سختی انجام کار)**

- هر ۲۰۱۶ بلاک یک بار، سختی کار بر اساس میانگین سرعت کشف بلاک های اخیر، تنظیم می شود. (حدود ۲ هفته یک بار)
- هدف این است که کشف هر بلاک همواره بطور میانگین ۱۰ دقیقه طول بکشد.
- با افزایش قدرت محاسباتی ماشین ها، در کنار افزایش تعداد ماینرها، کشف بلاک ها سریعتر رخ می دهد.
- افزایش سختی با تنظیم مجدد حد آستانهٔ عددی مقدار هَش بلاک انجام می شود.
  - ➢ هر بار این آستانه کاهش پیدا می کند و هش باید از یک آستانه کوچکتر شود.

- امروز حدودا چند ده میلیون تِرا هَش در ثانیه در کل شبکه انجام می شود.

nastooh@aut.ac.ir

Bit-Coin

- ✓ اصول حاکم بر بیت کوین
  - **درآمد ماینرها**
    - ماینرها دو درآمد دارند:
      1. جایزه کشف بلاک جدید
      2. کارمزدهای تراکنش های جایگذاری شده در بلاک
    - امروزه ماینرها به صورت توزیع شده به استخر ماین متصل می شوند.
      - به صورت توزیع شده کارها را تقسیم می کنند.
      - جایزهٔ احتمالی نیز به نسبت بین اعضا تقسیم می شود.

انجام عملیات ماینینگ به صورت انفرادی عملاً شانس بسیار پایینی برای کشف یک بلاک دارد.

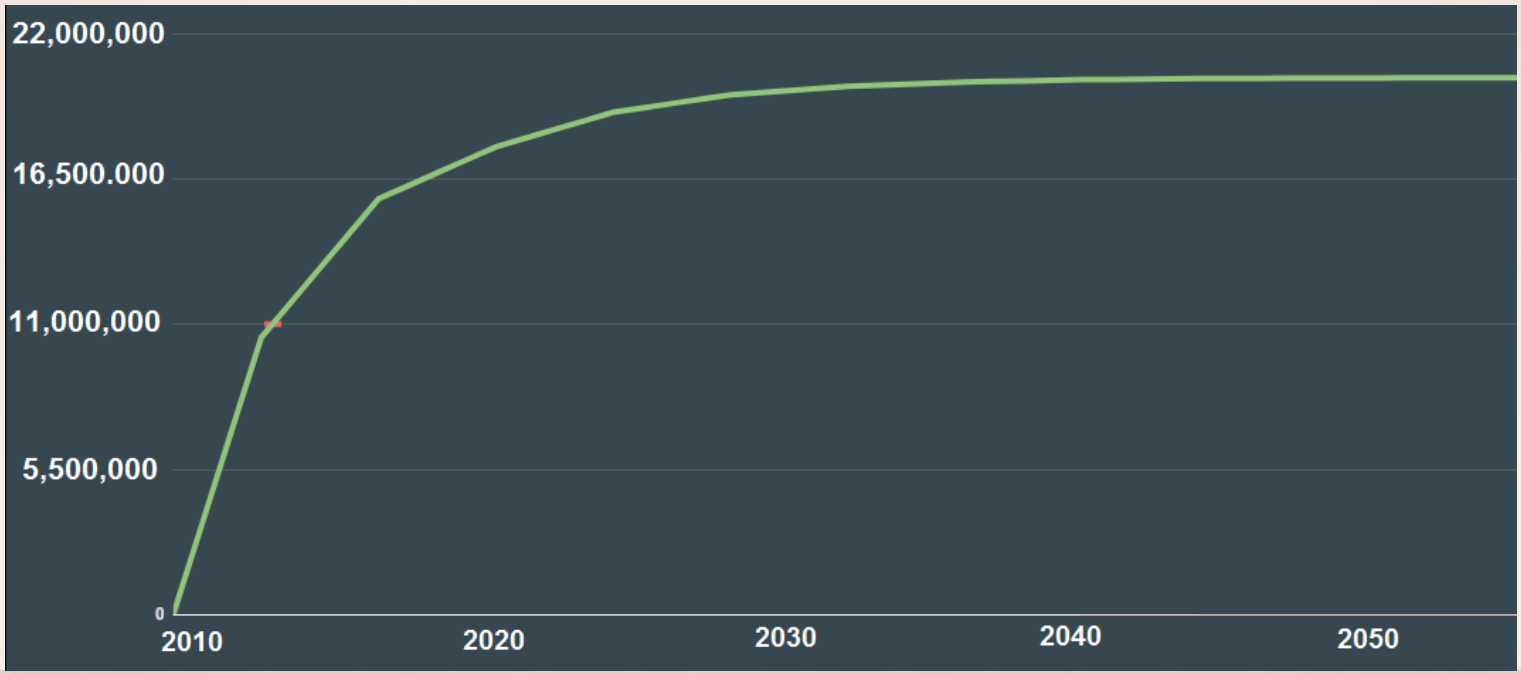
Bit-Coin

- ✓ اصول حاکم بر بیت کوین
  - مزرعهٔ استخراج

Bit-Coin

✓ اصول حاکم بر بیت کوین

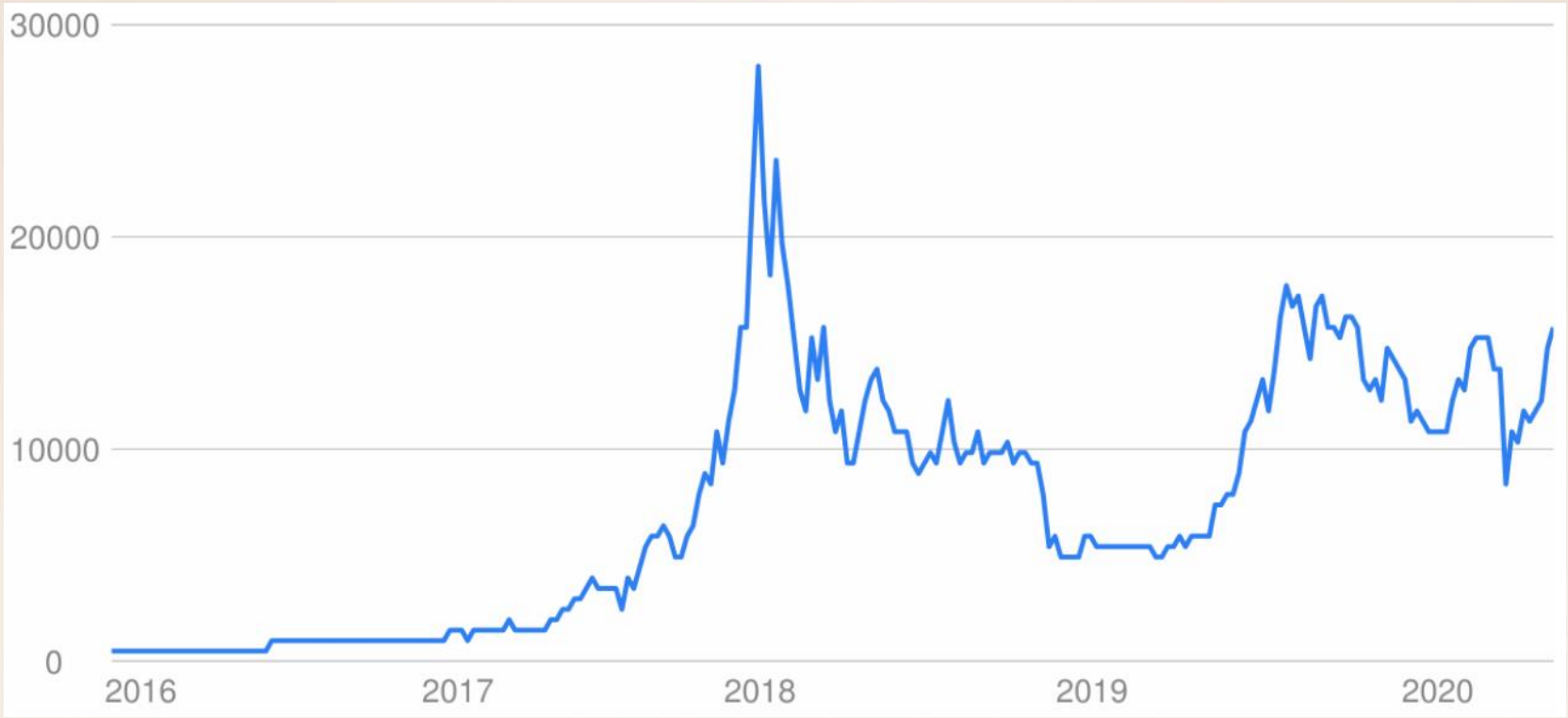
- تعداد نهایی بیت کوین
  - تعداد بلاک های بلاک چین در بیت کوین عملاً محدودیتی ندارد.
  - اما جایزهٔ کشف هر بلاک هر ۴ سال کم خواهد شد.
  - بنابراین تعداد کل بیت کوین های استخراج شده به سمت ۲۱ میلیون میل خواهد کرد.



nastooh@aut.ac.ir

Bit-Coin

- ✓ اصول حاکم بر بیت کوین
  - نمودار قیمت بیت کوین



nastooh@aut.ac.ir

Bit-Coin

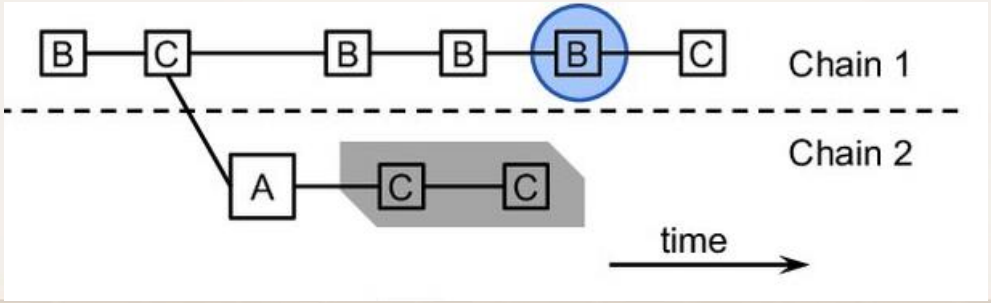
- ✓ اصول حاکم بر بیت کوین
  - **مقیاس پذیری بیت کوین**
    - پروتکل بیت کوین مشکل مقیاس پذیری دارد.
    - در صورتی که نقل و انتقال های بیت کوین زیاد شود، تراکنش ها تلنبار می شوند!
      - سرعت ساخت بلاک ثابت است.
      - تعداد تراکنش های قابل ثبا در بلاک نیز ثابت است.
    - کارمزدها افزایش می یابد.
      - ماینینگ هم روز به روز هزینه ی بیشتری نیاز دارد.

Bit-Coin

✓ اصول حاکم بر بیت کوین

○ همزمانی کشف بلاک

- گاهی دو ماینر تقریبا همزمان یک بلاک ثبت میکنند و برای یک مدت کوتاهی بلاک چین به دو شاخه تقسیم می شود.
  - ➢ یعنی در ادامه هر کدام یکی-دو بلاک اضافه می شود.
- یادآوری: زنجیره اصلی باید یکتا باشد.
  - ➢ بنابراین یکی از رشته تا باید باقی مانده و رشته دیگر حذف شود.
- رشته ای که طولانی تر است باقی می ماند و بلاک های رشتهٔ مقابل باید حذف شوند.
  - ➢ به بلاک های رشتهٔ ضعیف و جدا شده بلاک های **اورفان** (یتیم) گویند.
  - ➢ تراکنش های آن بلاکها باید به کیف پول کاربران برگشت داده شوند.



nastooh@aut.ac.ir

Bit-Coin

✓ اصول حاکم بر بیت کوین

○ حملهٔ احتمالیِ ۵۱ درصد

- اگر روزی، یک تیم بیش از ۵۰ درصد قدرت محاسباتی شبکه را داشته باشد چه می شود؟
  - از نظر احتمالات به ازای هر بلاک، بالاترین شانس ایجاد و کشف آن بلاک را دارد.
  - عملا بلاک های زیادی را کشف می کند.
- تا بحال این حلمه رخ نداده است.
  - قدرت محاسباتی بسیار زیادی نیاز دارد.
- شاید بتواند محدودیت هایی را اعمال کند، مانند:
  - مثلا بر روی انتخاب تراکنش ها
  - اعمال تغییرات و فورک ها
  - برگشت زدن بلاک های اخیرا کشف شده
  - دوبار خرج کردن کوین ها
  - و و و
- البته این حمله موجب ایجاد عدم اطمینان (و مهاجرت کاربران)، خواهد شد و احتمالاً در بلند مدت موجب زیانِ کلی رمز-ارز و درنتیجه زیانِ خود حمله کنندگان خواهد شد!!!

nastooh@aut.ac.ir

Bit-Coin

- ✓ اصول حاکم بر بیت کوین
  - **فورک**
    - ورژن ها و به روزرسانی های مختلف از بیت کوین را فورک گویند.
    - علت ایجاد آپدیت:
      - اصلاحات...
      - موارد امنیتی...
      - اختلاف نظر بین اعضای شبکه...
    - عملا دو نوع فورک وجود دارد، هارک فورد و سافت فورک.
    - معمولا وقتی هاردفورک رخ میدهد، به کاربران اعلام می شود که نقل و انتقال انجام ندهند تا وضعیت نسخه اصلی مشخص شود.
    - فورک ها از پیش مشخص میشوند که از چه شماره بلاکی به بعد اعمال می شوند.

nastooh@aut.ac.ir

پایان

nastooh@aut.ac.ir