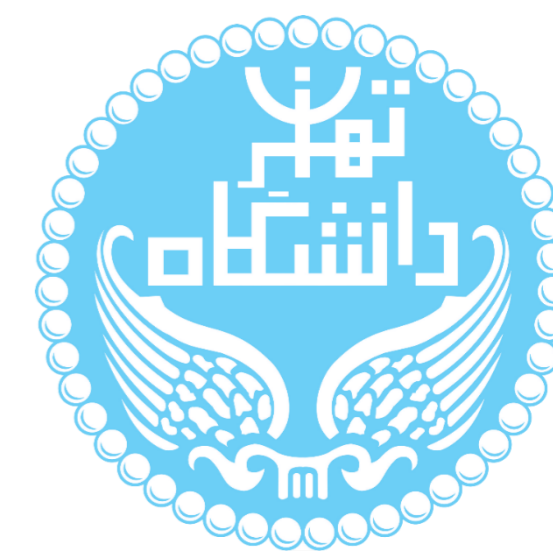


استفاده از پردازنده‌های نهفته برای استخراج ارز رمزی

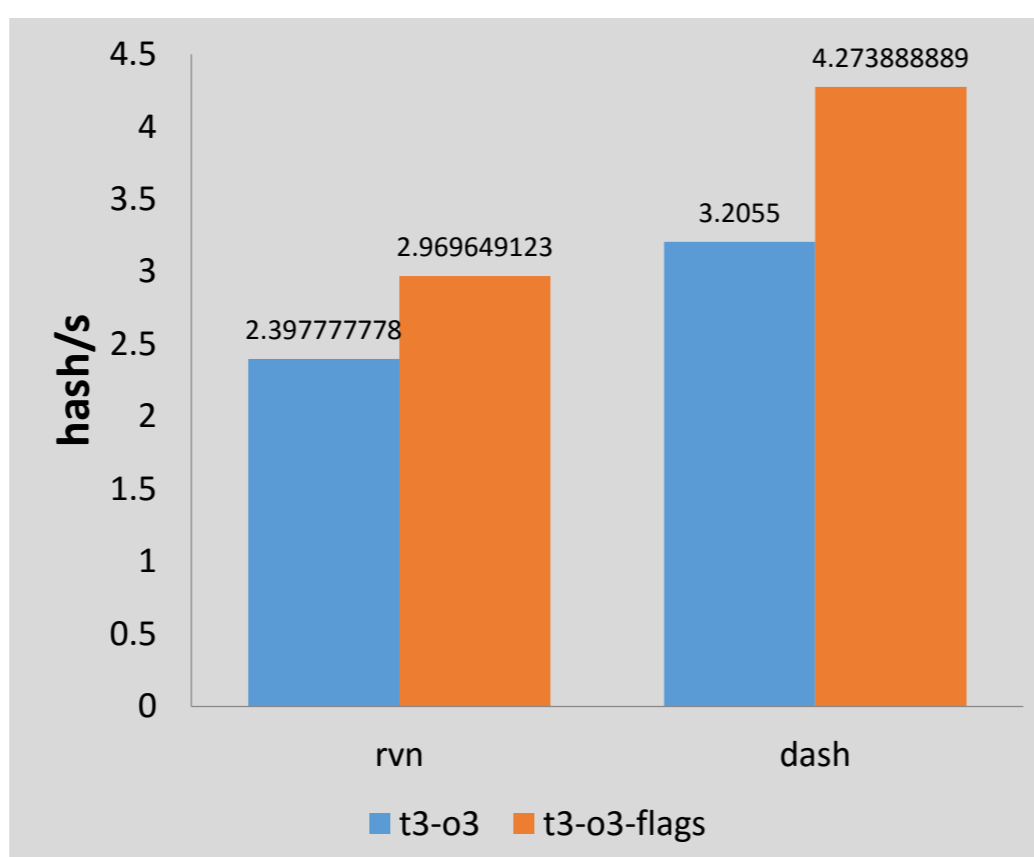
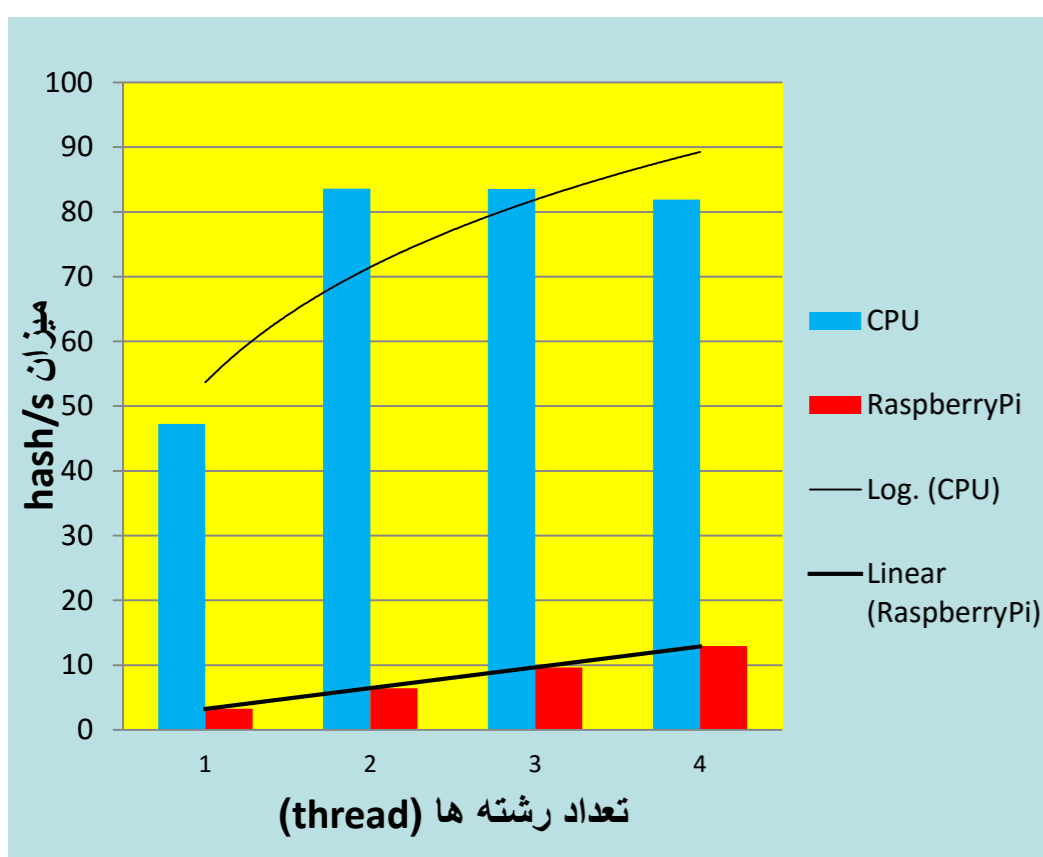


دانشجو: سیده مریم قاسمی
 استاد راهنما: دکتر مهدی کمال
 دانشکده مهندسی برق و کامپیوتر، دانشگاه تهران



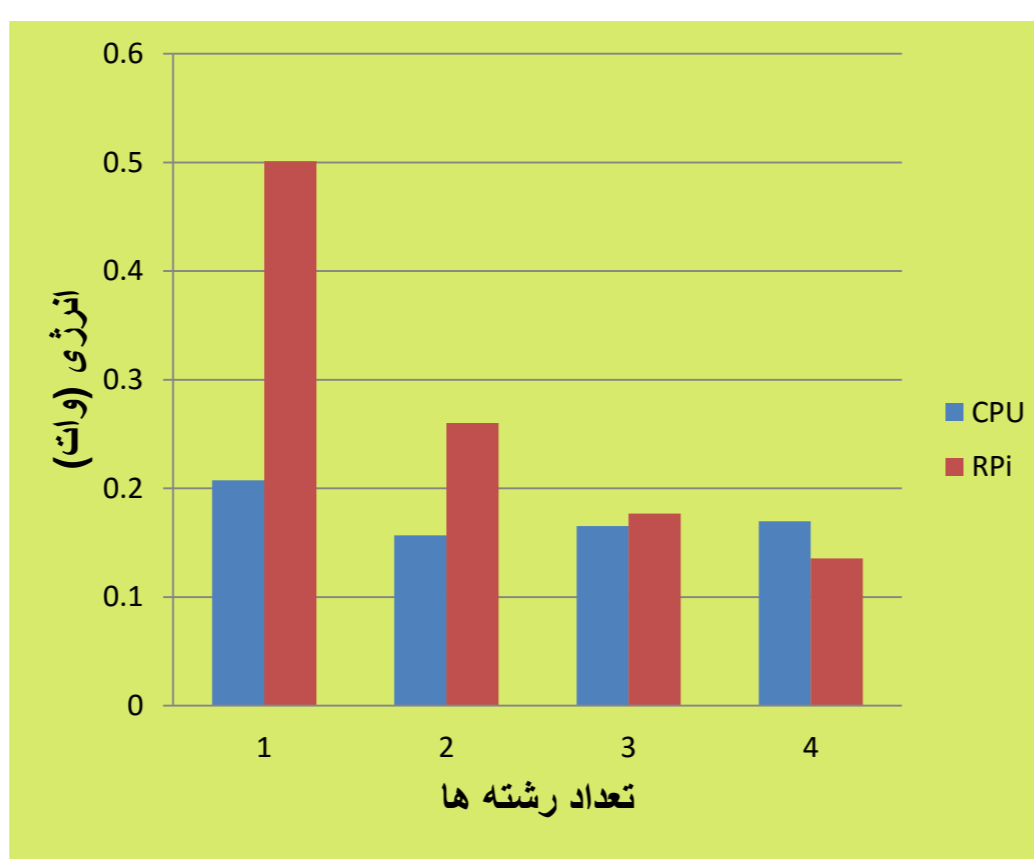
نتایج

در ادامه دستاوردها و نتایج به دست آمده را در قالب نمودارهایی ارائه می دهیم.



شکل (۵) مقایسه تاثیر افزایش تعداد threadها در پردازنده‌ی رزبری پای و پردازنده‌ی رایانه

شکل (۴) تاثیر اعمال flagها در میزان هش بر ثانیه (به ازای هر thread) بر روی دو ارز رمزی



شکل (۷) نمودار دمای پردازنده در برد رزبری پای به ازای تعداد threadهای پردازشی

شکل (۶) مقایسه انرژی مصرفی در CPU و برد Raspberry Pi

مقدمه / خلاصه

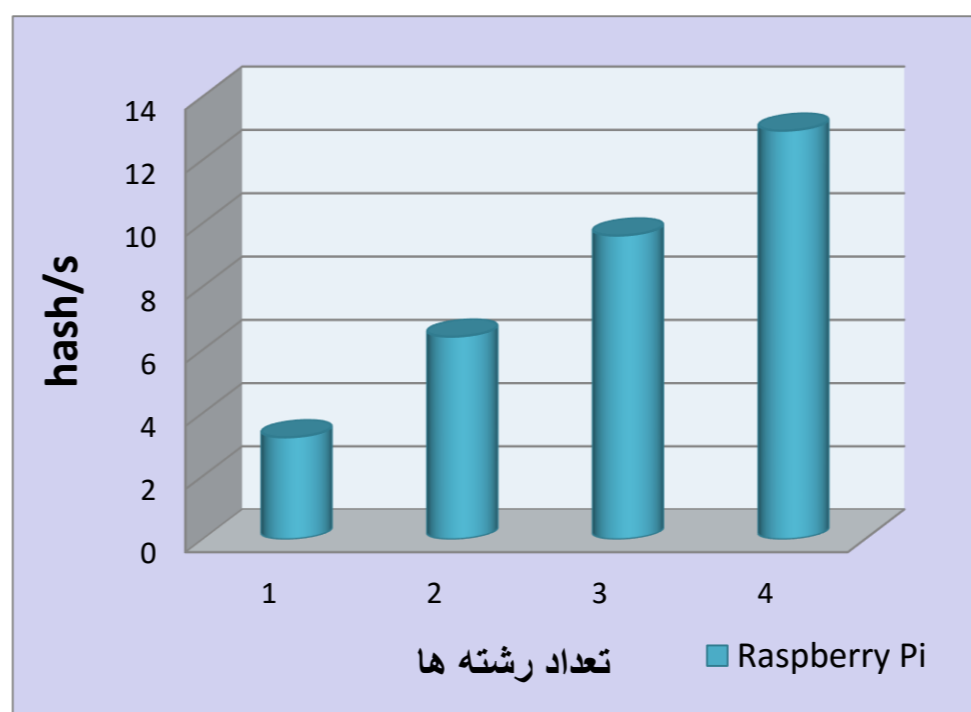
Cryptocurrencyها یا ارزهای رمزی یکی از مفاهیمی است که امروزه بسیار مورد توجه قرار گرفته است. ارزهای رمزنگاری شده نوعی پول دیجیتالی هستند که به گونه‌ای طراحی شده‌اند که ایمنی بالایی داشته و در بیشتر موارد از خود ردپایی برجا نگذارند. واحدهای ارز مجازی از طریق یک فرایند به نام استخراج (mining) تولید می‌شوند که شامل استفاده از قدرت کامپیوتری برای حل مسائل پیچیده ریاضی است که باعث تولید coinها (سکه‌ها) می‌شود.

در این پروژه قصد داریم این فرایند را بر روی پردازنده‌های نهفته (embedded processor) اجرا نموده و ببینیم که آیا استفاده از پردازنده‌های نهفته می‌تواند به عنوان یک راهکار برای به دست آوردن سود یا کارایی بیشتر باشد یا خیر.

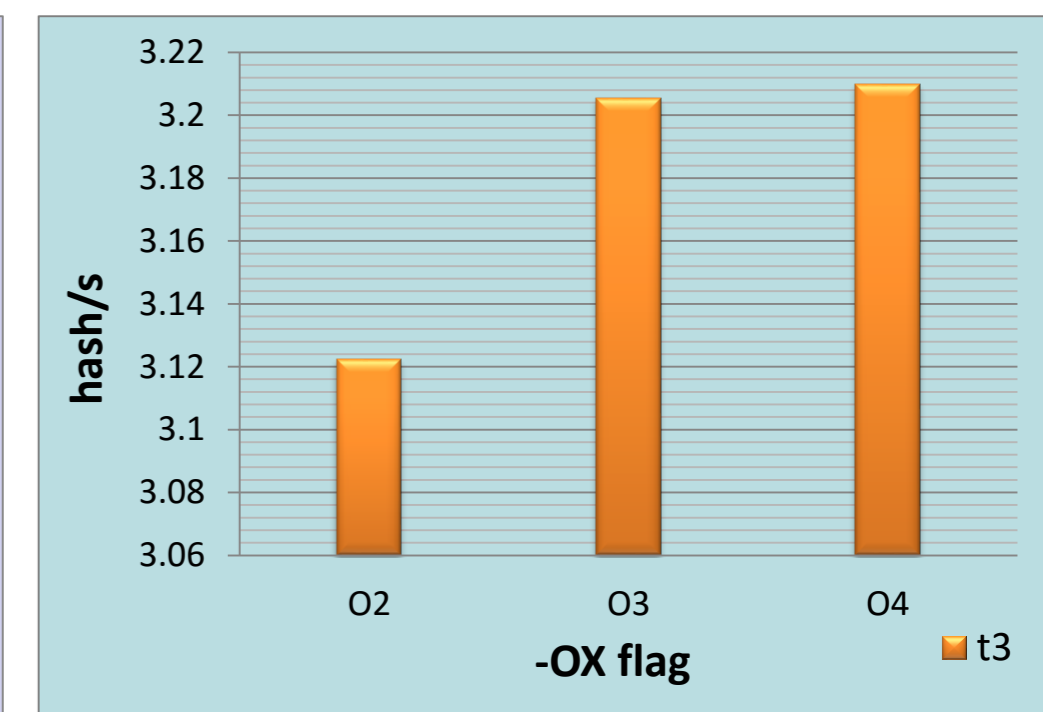
روش / ساختار / مدل پیشنهادی

در این پروژه برای پیاده سازی یک node از شبکه برای استخراج ارزهای رمزی، با استفاده از mining poolها یا استخرهایی برای استخراج، سعی در استخراج ارزهای رمزی نمودیم. همچنین از پردازنده‌ی برد Raspberry Pi 3 model B به عنوان پردازنده‌ی نهفته‌ی خود استفاده نمودیم.

در گام بعد برای افزایش دادن و بهبود میزان هش انجام شده در یک ثانیه توسط پردازنده‌ی برد رزبری پای، سعی کردیم تا از کدهای دستوری و flagهای مخصوص کامپایلر بهره برده که نتایج به دست آمده در جدول‌های زیر نشان دهنده‌ی نحوه‌ی تاثیرگذاری هر یک از عوامل هستند که مورد بررسی قرار گرفته اند.



شکل (۲) نمودار تاثیر تغییر تعداد threadهای اجرایی در میزان هش بر ثانیه



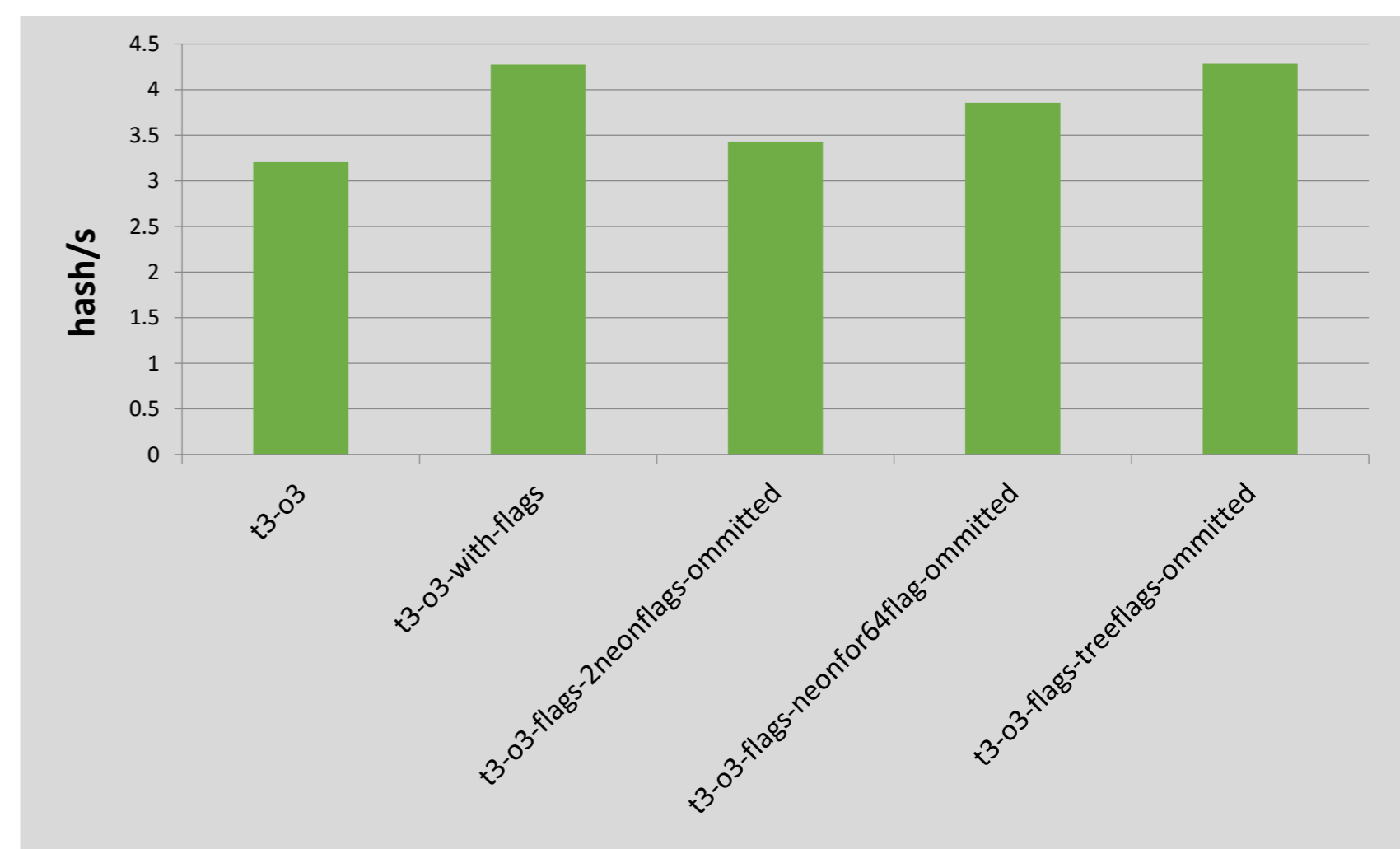
شکل (۱) نمودار بررسی تغییر flag مربوط به optimization بر روی میزان هش بر ثانیه (در هر رشته)

جمع بندی

در این پروژه در گام نخست ما به جستجوی روش‌های استخراج ارزهای رمزی پرداخته و پس از امتحان نمودن روش‌های مختلف و انتخاب نمودن روش مناسب، سعی در بهبود دادن روش به دست آمده نمودیم و عملکرد آن‌ها را بر روی برد Raspberry Pi خود امتحان کردیم. سپس به بررسی تفاوت‌های عملکرد CPU و برد Raspberry Pi بر عواملی چون تغییر تعداد threadهای اجرایی پرداخته و توان و انرژی مصرفی آن‌ها را مشاهده نمودیم و دیدیم که توان مصرفی برد Raspberry Pi به مراتب کمتر از رایانه بوده اما از لحاظ مصرف انرژی رایانه به طور کلی عملکرد بهتری داشته اما به ازای threadهای بالاتر انرژی مصرفی برد Raspberry Pi به مقداری کمتر از رایانه رسیده و بهره‌وری مناسب آن به ازای threadهای بالاتر رخ داد. همچنین تاثیر افزایش دادن تعداد threadها را در افزایش دمای پردازنده‌ی Raspberry Pi مشاهده نمودیم.

کاربرد های صنعتی:

با بررسی نتایج و مقایسه‌های انجام شده در این پروژه می‌توان در صنعت به بخشی از پرسش‌های پیش آمده در زمینه‌ی نحوه‌ی عملکرد و یا میزان کارایی و به صرفه بودن یا نبودن استفاده از پردازنده‌های نهفته (به خصوص برد Raspberry Pi) با توجه به نیازهای پروژه‌های مربوطه، پاسخ داد.



شکل (۳) تاثیر flagهای استفاده شده در میزان هش بر ثانیه (به ازای هر thread)

مراجع اصلی

- [Online]. Available: <https://www.raspberrypi.org>.
- [Online]. Available: <https://github.com/tpruvot/cpuminer-multi>.
- A. Narayanan, J. Bonneau, E. Felten, A. Miller and S. Goldfeder, "Bitcoin and Cryptocurrency Technologies," 9 February 2016. [Online]. Available: https://lopp.net/pdf/princeton_bitcoin_book.pdf. [Accessed 6 February 2018].

در ادامه به مقایسه‌ی استخراج روی پردازنده نهفته و رایانه و ارزیابی نتایج می‌پردازیم. معیار ارزیابی ما ترکیبی از پارامترهای مختلفی چون تعداد hashهاست که در یک زمان مشخص پردازنده توانایی انجام آن را دارد و همچنین توان و انرژی مصرفی پردازنده به ازای این مقدار هش می‌باشد.