UNIVERSITY OF MOLISE

DEPARTEMENT OF BIOSCIENCE AND TERRITORY

PROJECT PROPOSAL

TODO GPU cryptojacking

Author:
Federico ZAPPONE

Networking security and software security
December 01, 2020

Abstract

Contents

List of Figures

Research topic

Sempre più spesso si sente parlare di moneta digitale e delle così dette criptovalute, da qualche anno infatti sulla bocca di tutti risaltano parole di innovazione e opportunità in seguito all'avvento della nuova tecnologia blockchain basata sulla logica di database distribuito. Proprio grazie a quest'ultima è nata la prima criptovaluta al mondo, più precisamente, il 3 gennaio 2009 veniva alla luce il blocco genesi di Bitcoin composto allora da 50 *BTC* dal valore complessivo che non raggiungeva neppure un dollaro statunitense dato il prezzo iniziale di $0.0008 per Bitcoin. In seguito all'ottimo riscontro in molteplici campi il 6 novembre 2010 un Bitcoin si presentava con un valore di $0,50, in meno di due anni il prezzo era aumentato di 625 volte, e da allora in poco più di sette anni, Bitcoin raggiunse il suo massimo storico di quasi $20.000 ovvero circa 40.000 volte in più. Divenuto un caso più unico che raro, Bitcoin si è posto da apripista a più di 5000 altre criptovalute fino ad essere definito come l'oro del XXI secolo. Questa definizione non è dovuta solo all'incredibile aumento del prezzo di Bitcoin negli ultimi anni ma anche ad una delle caratteristiche chiave che la maggior parte delle criptovalute condivide, ovvero il mining, il processo di "estrazione" delle monete digitali.
Il mining di criptovalute consiste nel creare monete virtuali attraverso la risoluzione di alcune funzioni crittografiche necessarie per la validazione delle transazioni e dei blocchi che compongono una blockchain. Questi calcoli vengono eseguiti dai sistemi informatici dedicati a questo specifico processo, questi sistemi sono divisi in due grandi macro sezioni: quelli che sfruttano la Central Processing Unit e quelli che sfruttano invece la Graphics processing unit. I primi prendono il nome di *ASIC* che sta per *Application Specific Integrated Circuit* ovvero circuiti costruiti per la risoluzione di un calcolo ben specifico ma risultano molto inefficienti su altri tipi di algoritmi. I sistemi basati su GPU sono invece molto più prestanti grazie proprio al fatto che le schede video riescono ad effettuare più calcoli al secondo rispetto alle CPU e quindi risultare più redditizie, d'altro canto risultano essere molto più difficili nella gestione delle temperature e nettamente più costose in termini di assemblaggio e di efficienza energetica. Proprio questi ultimi costi sono quelli di notevole impatto quando si parla di mining, il costo di acquisto delle componenti è infatti nettamente aumentato negli ultimi anni, questo sia a causa delle nuove scoperte tecnologiche sia proprio a causa delle grandi farm di mining sparse per il mondo che acquistano sempre più componenti per ingrandire i propri centri di estrazione. Il costo energetico che questi sistemi comportano ha portato invece le grandi farm a svilupparsi maggiormente nei paesi con costi dell'elettricità più bassi e allo stesso tempo ha reso

molto più impegnativo l'operazione di mining per chi volesse entrarne a far parte.

Related Work

Aims and Objectives

Methodology