UNIVERSITA' DEGLI STUDI DI
NAPOLI FEDERICO II

Scuola Politecnica e delle Scienze di Base
Corso di Laurea in Ingegneria Informatica

Elaborato finale in **Calcolatori Elettronici I**

Architetture di calcolo eterogenee per l'accelerazione del Bitcoin Mining

Anno Accademico 2015/2016

Candidato:

Dario d'Andrea

matr. N46001947

Ai miei genitori, a tutta la
mia famiglia e agli amici,
perché hanno creduto in me
fin dall’inizio

Indice

Introduzione

Oggigiorno esistono diversi e innovativi sistemi di pagamento utilizzabili nel mercato globale, costruiti su piattaforme come la telefonia mobile e Internet. Si sta facendo riferimento a forme alternative di pagamento basate su valuta legale, che sono state sviluppate di recente e continuano a crescere; ne sono un esempio *PayPal*, *Apple Pay*, *Google Wallet* ed altre.

Oltre a questi sistemi di pagamento basati su valuta legale, stanno avendo un crescente interesse a livello mondiale quei sistemi basati su valuta digitale (*digital currency*) che consentono un più rapido, flessibile e innovativo metodo di pagamento per beni e servizi. Una moneta digitale che si distingue dalle altre nell'essere una delle più conosciute ed utilizzate valute digitali al mondo è *Bitcoin*. Per essere più specifici Bitcoin è una criptovaluta (*criptocurrency*) ovvero una particolare tipologia di ciò che è generalmente conosciuto come valuta digitale. Bitcoin è una criptovaluta unica, considerata essere la prima nel suo genere e così come altre create successivamente, utilizza la potenza di Internet per gestire le sue transazioni. A differenza della maggior parte delle valute tradizionali, Bitcoin non fa uso di un ente centrale: utilizza un database distribuito (*Blockchain*) tra i nodi della rete, che tiene traccia delle transazioni, e sfrutta la crittografia per gestire gli aspetti funzionali come la generazione di nuova moneta e l'attribuzione di proprietà dei bitcoin.

Quest'elaborato, nel primo capitolo, si propone di illustrare le caratteristiche del sistema

Bitcoin analizzandone il funzionamento e descrivendolo in tutti i suoi aspetti. Successivamente nel secondo capitolo verranno introdotte e descritte nel dettaglio le piattaforme di calcolo eterogenee GPU, FPGA e ASIC. Tali architetture sono state utilizzate nel corso degli anni come hardware di supporto al sistema Bitcoin, in particolare nella storia della valuta si è passati dall'utilizzare semplici general-purpose CPU, a architetture GPU e FPGA, per finire oggi con sistemi ASIC-based altamente specializzati. Proprio per questo il terzo e ultimo capitolo è volto ad esaminare nel dettaglio l'evoluzione dell'hardware utilizzato nella rete Bitcoin descrivendo come e perché i sistemi eterogenei possono essere applicati al problema del *Bitcoin mining* migliorando le performance e l'efficienza energetica.

Capitolo 1: Bitcoin

Bitcoin, spesso abbreviato con BTC o ₿, è al tempo stesso un software distribuito, una rete decentralizzata, un protocollo ed una valuta che utilizza in un sistema peer-to-peer (p2p) la rete Internet per verificare e gestire le transazioni. Invece di affidarsi su fidate terze parti, come banche o istituzioni finanziarie, la tecnologia Bitcoin usa prove crittografiche nel suo software per gestire transazioni, mantenere i conti e verificare la validità dei pagamenti.

Convenzionalmente con la notazione "Bitcoin" (iniziale maiuscola) ci si riferisce alla rete e alla tecnologia, invece con "bitcoin" ci si riferisce all'unità della moneta.

Questo capitolo si pone l'obiettivo di analizzare in dettaglio il sistema Bitcoin e descriverlo nel suo funzionamento.

1.1 Digital Currency come Alternative Currency

Con il termine *alternative currency* (valuta alternativa) si intende una qualsiasi forma di moneta o di titolo di credito utilizzata per lo scambio di beni e servizi tra i membri di una comunità e collocata al di fuori dei circuiti monetari ufficiali, vigenti legalmente all'interno di un stato.

In accordo con la classificazione di Hileman (2014) si distinguono due forme di valuta alternativa: tangibile e digitale. La valuta digitale (*digital currency*) è un mezzo di

scambio basato su Internet, diverso da quella fisica (come banconote o monete), che permette transazioni istantanee e trasferimenti di proprietà senza confini.

A loro volta le valute digitali si dividono in valute digitali centralizzate (*centralized digital currency*) e valute digitali distribuite e/o decentralizzate (*distributed decentralized digital currency*), la cui differenza sta nella presenza o meno di un entità centrale che diriga l'intero sistema. Per essere più specifici un sottoinsieme delle valute digitali viene chiamato criprovaluta (*cryptocurrency*), in cui è incluso Bitcoin.

1.1.1 Cryptocurrency

Una criptovaluta (*cryptocurrency*) è un mezzo di scambio ed una valuta digitale decentralizzata che utilizza la crittografia per convalidare le transazioni e creare nuova moneta. Permette di effettuare pagamenti online in maniera sicura attraverso l'uso di algoritmi crittografici. Le implementazioni esistenti di criptovalute sono basate sistemi di tipo *peer-to-peer* (p2p) su reti i cui nodi sono computer di utenti collocati in tutto il mondo. Fanno spesso uso di uno schema *proof-of-work*, per evitare pagamenti digitali fraudolenti. Sui diversi nodi vengono eseguiti appositi programmi che permettono di gestire conti e transazioni. Non c'è un'autorità centrale o alcuna forma di gestione di tipo centralizzato che supervisiona il tutto, di conseguenza le transazioni e l'emissione delle criptomonete avvengono collettivamente all'interno della rete.

1.2 Nascita e controllo decentralizzato

Nel 2008 Satoshi Nakamoto pubblicò un articolo scientifico sul Web, intitolato "*Bitcoin: A Peer-to-Peer Electronic Cash System*", in cui viene analizzato il sistema si pagamento elettronico peer-to-peer *Bitcoin*. Nonostante i molti sforzi fatti per identificare Satoshi, la sua identità rimane ignota al pubblico non sapendo nemmeno se Satoshi sia un singolo individuo o un gruppo di più persone.

La criptovaluta inventata da Nakamoto viene eseguita utilizzando un software open-source, rilasciato nel Gennaio del 2009, che può essere scaricato da chiunque. Il sistema esegue su una rete peer-to-peer decentralizzata che è anche totalmente distribuita.

Non a caso la nascita di questa moneta affonda le proprie radici nel periodo più difficile della crisi economico-finanziaria, quando la fiducia nelle banche e negli organi centrali era ai minimi termini. Bitcoin è una moneta digitale che si può inviare attraverso Internet tramite trasferimenti di denaro che non si basano sulla fiducia in terze parti. I nodi, o computer terminali, sono connessi gli uni con gli altri e, in virtù del protocollo p2p, si possono inviare direttamente bitcoin da persona a persona senza ricorrere a mediatori, come banche o istituzioni finanziare (disintermediazione), questo significa che le commissioni sono molto inferiori. In definitiva tale moneta può essere definita come la prima forma di pagamento trustless.

Le principali caratteristiche su cui si basa il sistema per avere una criptovaluta distribuita di successo sono le seguenti:

- *Open-source-software*: chiunque può verificare il codice e i possibili cambiamenti da adottare nella rete.
- *Decentralized*: è essenziale che non sia controllato da una singola entità.
- *Peer-to-peer*: tutti i nodi sono paritari, gli utenti comunicano direttamente.
- *Global*: la moneta è globale e ciò è un punto positivo per l'integrazione finanziaria.
- *Fast*: le transazioni sono veloci e il tempo di conferma è breve.
- *Reliability*: non ci sono rischi di accordi e non ripudiabilità.
- *Secure*: sicurezza attraverso prove di identità con crittografia.
- *Sophisticated and flexible*: il sistema è in grado di supportare tutti i tipi di risorse, strumenti finanziari e mercati.
- *Automated*: gli algoritmi di esecuzione per pagamenti possono essere facilmente aggiornati automaticamente.
- *Scalable*: il sistema può essere usato da milioni di utenti.

1.3 Come funziona Bitcoin

Per una persona comune bitcoin è una valuta digitale creata e mantenuta elettronicamente. Esistono diversi modi per entrare in possesso bitcoin:

- nei punti di *exchange*, ovvero cambiavalute dove si possono comprare e vendere BTC

con Euro, Dollari e altre valute;

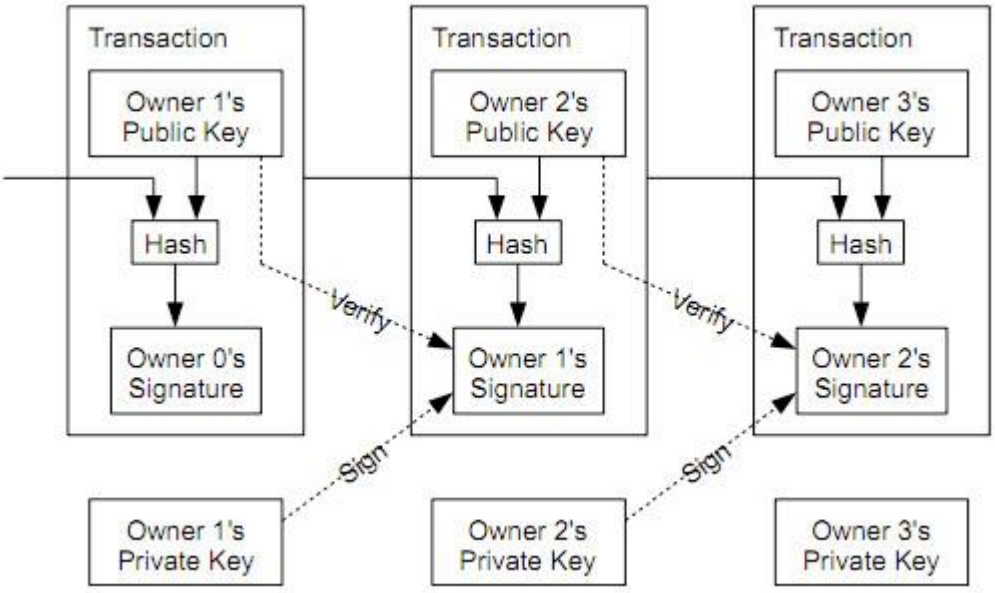
- ottenerli da qualcuno che ne è già in possesso attraverso l'erogazione di beni o servizi;
- attraverso l'attività di mining, che verrà analizzata nei paragrafi successivi.

Trasferire bitcoin è facile quanto mandare un e-mail e si può acquistare qualsiasi cosa con i BTC a partire da beni o servizi e altro ancora. I bitcoin sono mandati e ricevuti usando applicazioni mobile, software su computer o service provider che forniscono un portafoglio digitale (*bitcoin wallet*). Vengono poi mantenuti nel portafoglio digitale dell'utente registrato a cui sono associate due chiavi, una pubblica e una privata. La chiave pubblica, chiamata anche indirizzo Bitcoin, è specie di conto bancario ed è costituita da una sequenza alfanumerica di caratteri, generalmente 34, che inizia sempre con il numero 1 o 3, della forma ad esempio 1Ei8bbsfgLW5hfNbP8b3uiWycnef45ot46, dove l'utente può inviare e ricevere pagamenti. Dato che la generazione delle chiavi richiede costi e tempi di calcolo ridotti, occorre precisare che ogni utente può ottenere un numero indefinito di indirizzi Bitcoin senza alcun limite. Il problema dell'*autenticazione*, in assenza di un server centrale, è quindi risolto con questa coppia di chiavi. Il messaggio che viene inviato al momento di un pagamento conterrà la quantità di denaro da trasferire e la chiave pubblica del destinatario. Tale messaggio verrà firmato digitalmente con la chiave privata del mittente prima di essere inviato. Infine il destinatario verificando la firma avrà la prova crittografica del mittente, del destinatario e della quantità di denaro trasferita. La chiave privata viene quindi utilizzata per fare in modo che il pagamento sia autorizzato unicamente dal reale proprietario della moneta.

1.4 Transazioni

Per gestire il bilancio degli account utente non vengono memorizzati il numero di bitcoin posseduti da ciascuno, ma la procedura risulta più complessa e sicura sfruttando la cosiddetta *transaction chain* (catena di transazioni). Ogni moneta digitale è rappresentata da una catena di transazioni che si incrementa progressivamente al passaggio di proprietario in proprietario. Riprendendo quanto detto precedentemente sui trasferimenti di moneta, l'utente che vuole effettuare il pagamento più precisamente firmerà l'hash della

transazione precedente e della chiave pubblica del destinatario, attaccando il tutto alla fine della catena come mostrato in figura. Infine il destinatario del pagamento può controllare i vari passaggi di proprietà della moneta verificando le firme delle transazioni.



Nonostante questo meccanismo risulti adeguato per un sistema decentralizzato e distribuito, non è ancora in grado, per come è stato descritto fino adesso, di risolvere il cosiddetto problema del *double-spending*, ovvero il fatto che la moneta digitale possa essere spesa più di una volta illecitamente. Infatti per quanto detto finora chi riceve la moneta non è in grado di determinare se uno dei precedenti proprietari non abbia già utilizzato tale moneta per altri pagamenti.

Data l'assenza di una entità centrale, la soluzione proposta dal sistema Bitcoin, per fare in modo che ogni utente possa controllare che la moneta non sia stata già spesa, è che tutti siano a conoscenza di tutte le transazioni che avvengono nel sistema. In tal modo è possibile accorgersi se la moneta è già stata inviata a qualcun altro e quindi non accettarla. Così, invece di un registro dei saldi i nodi Bitcoin tengono traccia di una lista gigante di transazioni. Possedere bitcoin vuol dire che ci sono transazioni in questo elenco che puntano al proprio nome e che non sono state utilizzate come input in altre operazioni. Un'interessante conseguenza di questa struttura è che per capire il proprio saldo occorre scorrere ogni transazione dall'inizio e sommare tutti gli input non spesi.

1.5 Blockchain

Nel precedente paragrafo è stato analizzato il modo in cui vengono controllate le transazioni nel sistema Bitcoin, ma non si è discusso di come gestire il loro ordine. Tenendo conto della vastità della rete e considerando che le transazioni passano da un nodo all'altro, non c'è sicurezza che l'ordine con cui si ricevono sia lo stesso in cui sono state create. Sarebbe poco sicuro affidarsi al timestamp perché risulta banale modificare a proprio vantaggio data e ora della creazione della transazione. Deve esistere un modo per cui l'intera rete debba concordare sull'ordine delle transazioni.

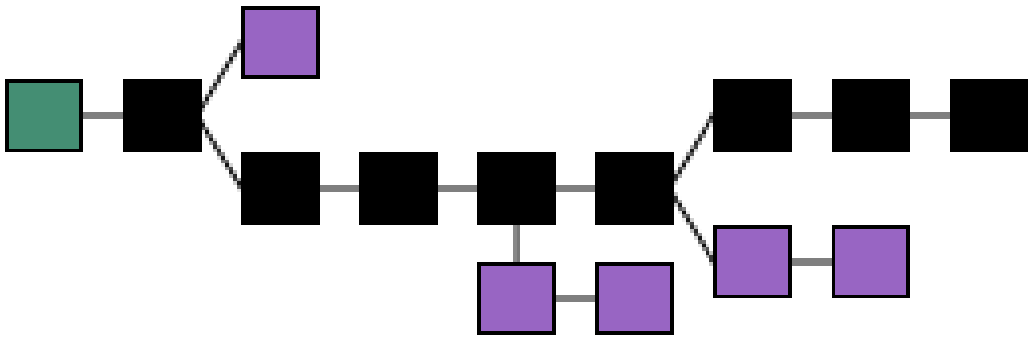
La soluzione adottata dal sistema si basa sul fatto che le transazioni sono organizzate in blocchi collegati tra loro, ognuno al precedente e al successivo, andando quindi a formare una catena chiamata *Blockchain*. Si noti che questa è diversa dalla catena delle transazioni discussa in precedenza; il Blockchain è usato per ordinare le transazioni, mentre la catena delle transazioni tiene traccia dei cambiamenti di proprietà della moneta. Le transazioni all'interno di uno stesso blocco sono considerate essere avvenute nello stesso momento, quelle non ancora in un blocco vengono dette non confermate. Ogni nodo può quindi raggruppare più transazioni all'interno di un blocco e trasmetterle al resto della rete suggerendo quale dovrebbe essere il blocco successivo.

In questo modo sembrerebbe che il problema dell'ordine venga spostato dalla singola transazione a un blocco di transazioni (non ci si può basare sull'ordine di arrivo dei blocchi), ma non è così. Bitcoin utilizza un sistema *proof-of-work*, difficile e costoso da produrre ma facile da verificare, nella forma di un problema matematico in cui la prima persona che risolve il problema trasmette al resto della rete il blocco e il suo gruppo di transazioni viene accettato come prossimo nella catena. Nello specifico ogni blocco è costituito, oltre che dalle transazioni, da un header dove si trovano il *target value* (la risposta al problema matematico), un numero chiamato *nonce* ed un riferimento al blocco precedente. Si utilizza una funzione di hash crittografico applicata al blocco tramite l'algoritmo SHA-256. L'operazione viene ripetuta cambiando il nonce finché non si ottiene un valore di hash che sia inferiore al target value. È intuibile il valore del target value è inversamente proporzionale alla difficoltà di generare un blocco, diminuendo il

target value è più difficile risolvere il problema matematico. La rete bitcoin cambia automaticamente la difficoltà dei problemi matematici in base a quanto velocemente vengono risolti. Il valore del nonce, come già detto, viene modificato partendo da "0" e incrementato per ogni tentativo di trovare l'hash giusto, finché non si ottiene un valore hash che inizi con un determinato numero di zeri (ovvero sia inferiore del target value). Si noti che l'output della funzione di hash è totalmente imprevedibile quindi l'unico modo per trovare un particole valore di output è fare prove casuali, così come si farebbe per indovinare la combinazione di un lucchetto.

Regolando la difficoltà in base alla potenza di calcolo dei nodi della rete si fa in modo che sono necessari in media 10 minuti perché qualcuno trovi una soluzione, rendendo quindi l'intervallo di generazione dei blocchi pressoché regolare. Se la potenza della rete aumenta è sufficiente aumentare la difficoltà del problema matematico.

La casualità del problema matematico distribuisce efficacemente su tutta la rete la possibilità di trovare una soluzione rendendo grossomodo improbabile che due persone trovino contemporaneamente la soluzione. Può capitare, però, che due blocchi vengano generati contemporaneamente a partire dallo stesso blocco genitore. Ciò implica una biforcazione in due rami della catena che si allungano indipendentemente l'uno dall'altro.



Il singolo nodo continua dal blocco ricevuto per primo che potrebbe essere diverso da quello ricevuto da altri nodi, in ogni caso la regola dice che bisogna accettare blocchi sul ramo più lungo possibile. Alla fine il ramo sui cui si concentra la potenza di calcolo maggiore cresce più velocemente dell'altro, finché i nodi di minoranza che avevano allungato l'altro ramo lo abbandonano e continuano la costruzione dei blocchi su quello principale.

Attualmente la dimensione del Blockchain è di circa 14 GB e tende a crescere linearmente all'aumentare delle transazioni, per questo si stanno facendo studi per comprimerla.

1.6 Bitcoin Mining

L'attività di verificare transazioni e aggiungere blocchi al blockchain è chiamata *mining* (letteralmente significa estrazione), e viene svolta da nodi speciali che prendono il nome di *miners* (minatori). I miners permetto di garantire la sicurezza del sistema Bitcoin svolgendo i calcoli computazionali molto complessi precedentemente descritti, più miners significa una rete più sicura. Per il lavoro svolto, che implica consumo di risorse di calcolo ed energia elettrica, i miners vengono ricompensati attraverso nuova moneta. Questo non rappresenta solo una forma di incentivo, ma anche un'altra modalità di emissione della valuta. La ricompensa che viene data per ogni blocco di transazioni generato diminuisce col passare del tempo. Per essere più specifici ogni 4 anni circa viene dimezzata: inizialmente venivano associati 50 BTC ad ogni blocco, nel 2012 c'è stata la prima riduzione a 25 BTC, il prossimo dimezzamento a 12.5 BTC è stato previsto per Ottobre 2016, fino ad arrivare a zero nel 2140. È stato previsto di arrivare a una cifra di circa 21 milioni di monete in circolazione.

Una volta terminata la ricompensa per i blocchi, i miners riceveranno incentivi sotto forma di *fee*, ovvero una tariffa che il mittente dovrà pagare per trasferire denaro. Oggi già esistono queste commissioni per le transazioni, ma sono facoltative per gli utenti che desiderano velocizzare le transazioni. I miners processano quindi con maggiore priorità le transazioni con contengono una fee. Ad ogni modo le commissioni avranno un ruolo di primo piano in futuro in quanto rappresenteranno l'unica forma di incentivo possibile. L'invio di denaro non sarà gratuito, ma rimarrà sempre più conveniente rispetto alle attuali commissioni con carta di credito.

In accordo con il paper scritto da Nakamoto nel 2008 il protocollo da seguire è il seguente:

1. Le nuove transazioni sono inviate in broadcast a tutti i nodi.
2. Ogni nodo raccoglie le nuove transazioni in blocchi.
3. Ogni minatore lavora per trovare un proof-of-work valido per il proprio blocco.

4. Quando un minatore trova un proof-of-work valido, invia il blocco in broadcast a tutti gli altri nodi.

5. I nodi accettano il nuovo blocco solo se contiene transazioni valide e non incluse in altri blocchi precedentemente.

6. I nodi dimostrano di accettare il nuovo blocco come valido utilizzandone l'hash nel calcolo del proof-of-work del blocco successivo della catena.

Data la complessità attuale dell'attività di mininig, la maggioranza dei minatori non lavora più in solitario, ma si uniscono tra loro per formare le *mining pool*. In tal modo risulta più semplice ottenere i risultati sperati perché la potenza computazionale aumenta. In seguito poi la ricompensa verrà divisa tra i partecipanti in funzione del lavoro svolto, si noti però che dal punto di vista della rete una mining pool è considerata come un unico nodo.

1.7 Irreversibità e anonimato

Le transazioni sono per loro natura irreversibili, questo significa che una volta incluse nel blockchain non possono essere annullate. L'unico modo per ritornare in possesso della propria moneta è farsi rimandare indietro i bitcoin dal destinatario. Questo risulta molto sicuro e affidabile per un commerciante che utilizza Bitcoin e lo tiene al sicuro da chargeback disonesti.

Bitcoin è una moneta anonima, o per meglio dire pseudo anonima: nonostante il database sia pubblico e condiviso da tutti, questo non fornisce alcun legame tra gli indirizzi delle transazioni è l'identità dei corrispettivi proprietari. Attraverso il blockchain è possibile però risalire a ritroso la catena e venire a conoscenza dell'identità di quegli utenti che hanno acquistato BTC attraverso valute tradizionali presso i punti di exchange, i quali per legge sono obbligati a verificare l'identità dei propri clienti.

1.4 Secure Hash Algorithm

Per *Secure Hash Algorithm* (SHA) si intende una famiglia di cinque funzioni di hash crittografiche sviluppate dalla National Security Agency (NSA) negli USA che attualmente rappresentano lo standard federale dal governo.

Essendo un algoritmo di hash, lo SHA produce un *message digest*, (impronta del messaggio), di lunghezza fissa partendo da un messaggio di lunghezza variabile. L'algoritmo di hash risulta sicuro perché la funzione non è reversibile (non è possibile risalire al messaggio originale a partire dall'output) e non deve mai essere possibile ottenere lo stesso digest a partire da due messaggi diversi. I cinque algoritmi della famiglia sono chiamati SHA-1, SHA-224, SHA-256, SHA-384 e SHA-512; gli ultimi quattro vengono spesso indicati con il termine SHA-2. Lo SHA-1 produce un digest del messaggio di 160 bit, mentre gli altri producono digest più grandi di lunghezza in bit pari al numero indicato nella loro nome, ad esempio SHA-256 produce un digest di 256 bit.

Come già detto precedentemente, l'algoritmo crittografico utilizzato nel Bitcoin mining è lo SHA-256 che verrà descritto dettagliatamente nel paragrafo successivo.

1.4.1 SHA-256

Lo SHA-256 opera in modo simile allo SHA-1. Il messaggio M a cui bisogna applicare la funzione di hash deve essere inizialmente preprocessato prima che inizi il loop principale con la funzione di compressione. Gli step che si susseguono sono i seguenti:

Preprocessing

1. *Pad the message*: bisogna "imbottire" il messaggio M affinché la lunghezza finale del messaggio risulti congruente a 448 modulo 512, così facendo la lunghezza l del messaggio M più l'imbottitura è pari ad un numero 64 bit più piccolo di un multiplo di 512 bit. Per costruire l'imbottitura bisogna concatenare il bit "1" alla fine del messaggio M seguito da k zeri tali che $l+1+k = 448 \bmod 512$. A ciò bisogna poi aggiungere un blocco di 64 bit pari al numero l scritto in binario. Ad esempio il messaggio "abc" (8-bit ASCII) ha lunghezza 24, sarà quindi seguito da 448-(24+1)=423 bit zero e dalla sua lunghezza per diventare 512 bit

$$01100001\ 01100010\ 01100011\ 1\ \underbrace{00\cdots0}_{423}\ \underbrace{00\cdots011000}_{64}.$$

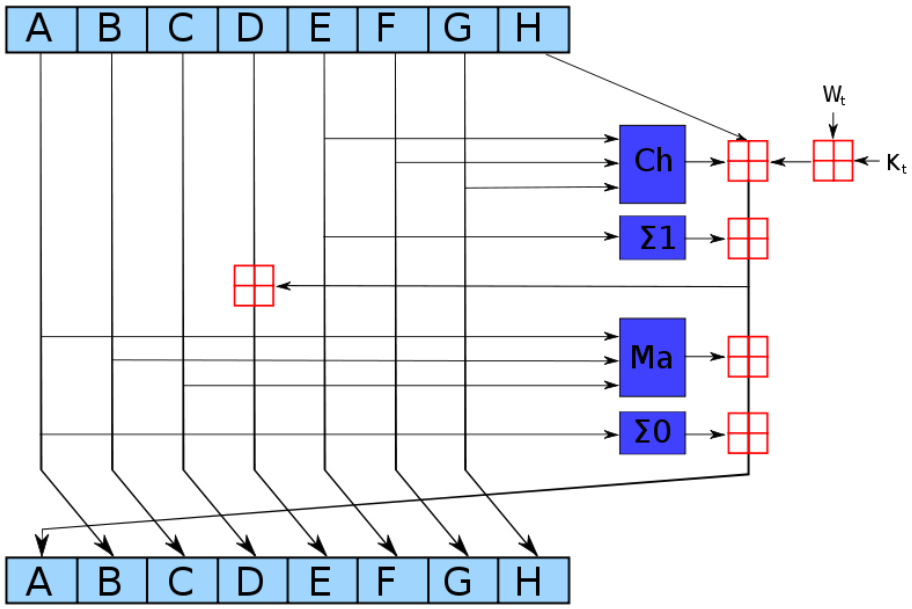
2. *Parse the message*: dividi il messaggio M in blocchi da 512 bit $M^{(1)},M^{(2)},M^{(3)},M^{(1)},\ldots,M^{(N)}$. I primi 32bit di ogni blocco saranno denotati con $M_0^{(i)}$, i successivi con $M_1^{(i)}$, e così via fino ad $M_{15}^{(i)}$.

3. *Setting the registers with the initial hash value*: impostare i registri *a,b,c,d,e,f,g,h* con i valori iniziali di hash $H_1,H_{2,\ldots,}H_8$ già prestabiliti e indicati in seguito (sono ottenuti dalla parte frazionaria delle radici quadrate dei primi 8 numeri primi).

$$H_1^{(0)} = \texttt{6a09e667}$$
$$H_2^{(0)} = \texttt{bb67ae85}$$
$$H_3^{(0)} = \texttt{3c6ef372}$$
$$H_4^{(0)} = \texttt{a54ff53a}$$
$$H_5^{(0)} = \texttt{510e527f}$$
$$H_6^{(0)} = \texttt{9b05688c}$$
$$H_7^{(0)} = \texttt{1f83d9ab}$$
$$H_8^{(0)} = \texttt{5be0cd19}$$

Main Loop: Hash computation

1. *Apply the SHA-256 compression function*: si applica l'algoritmo a partire dai registri *a,b,c,d,e,f,g,h* e dai valori *W* e *K* come mostrato in figura



In cui le operazioni fatte sono:

Majority function (*Maj*) *box*: vale 1 se e solo se la maggioranza degli input vale 1, altrimenti vale 0 (si analizza singolarmente ogni bit in posizione i-esima dei valori di input).

Shift (*S*): denota una rotazione dei bit a sinistra si *n* posti.

Red box: (il quadrato rosso in figura) indica l'addizione modulo 32.

Choose (*Ch*) *box*: sceglie l'output in base al valore del primo input *e*. Se i bit i-esimo di *e* vale 1 allora l'output corrisponde al bit i-esimo di *f*, altrimenti a quello di *g*.

Input W: determinato dai valori dei dati di input all'algoritmo.

Input K: costante definita ad ogni ciclo.

2. *Compute the hash value*: si aggiornano i valori di hash intermedi nei registri *a,b,c,d,e,f,g,h* e si ripete tale ciclo 64 volte fino ad avere i valori di hash finali del messaggio *M*.

$$
\begin{aligned}
Ch(x,y,z) &= (x \wedge y) \oplus (\neg x \wedge z) \\
Maj(x,y,z) &= (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z) \\
\Sigma_0(x) &= S^2(x) \oplus S^{13}(x) \oplus S^{22}(x) \\
\Sigma_1(x) &= S^6(x) \oplus S^{11}(x) \oplus S^{25}(x)
\end{aligned}
$$

Come si può vedere dal diagramma solo i registri *a* ed *e* sono cambiati ad ogni ciclo, gli altri valori passano praticamente inalterati. Accade però che il vecchio valore di *a* diventa il nuovo valore di *b*, il vecchio valore di *b* diventa il nuovo valore di *c* e così via. Per questo nonostante dopo un singolo ciclo dello SHA-256 i dati non cambiano radicalmente, dopo 64 cicli verranno totalmente modificati.

Capitolo 2: Architetture di calcolo eterogenee

2.1 Panoramica sulle architetture di calcolo eterogenee

Il seguente capitolo si pone l'obbiettivo di esaminare le soluzioni architetturali che permettono di conseguire elevate prestazioni di calcolo ed energetiche, richieste oggi in ambito industriale tanto da far sorgere il termine *High Performance Computing* (HPC). A tal fine risulta indispensabile ricorrere ad architetture di tipo parallelo.

Verranno analizzate le schede grafiche impiegati nel calcolo general-purpose *Graphics Processing Unit* (GPU), per poi passare ai *Field-Programmable Gate Array* (FPGA) e terminare con gli *Application-Specific Integrated Circuit* (ASIC). Tali architetture si differenziano sostanzialmente per il trade-off che mostrano tra efficienza e flessibilità. Se le architetture di tipo GPU forniscono una grande flessibilità, offrono di contro performance minori ed elevati costi energetici. A queste si contrappongono gli ASIC che seppur offrono elevata efficienza, sono progettati per una specifica applicazione e quindi non riadattabili. Le architetture FPGA si pongono in una posizione intermedia tra le due precedenti fornendo prestazioni migliori delle GPU ed al tempo stesso una grande flessibilità.

Si è scelto di analizzare tali architetture perché rappresentano la tecnologia di base per il processo del Bitcoin mining (si rimanda al prossimo capitolo per una chiarificazione al riguardo).

2.2 GPU

2.2.1 Cenni storici

Le *Graphics Processing Unit* (GPU) sono state sviluppate agli inizi degli anni '80 come unità di elaborazione specializzate nella rappresentazione grafica, per permettere l'accelerazione nel disegno di figure geometriche 2-D. L'industria dei videogiochi ha rivestito un ruolo chiave nel loro sviluppo iniziale, perché stava diventando sempre più necessario l'uso di acceleratori grafici. Si può dunque constatare che il rendering grafico bidimensionale costituisce il punto di partenza per lo sviluppo di GPU che si è successivamente consolidato negli anni '90 con applicazioni che fanno uso di grafica tridimensionale.

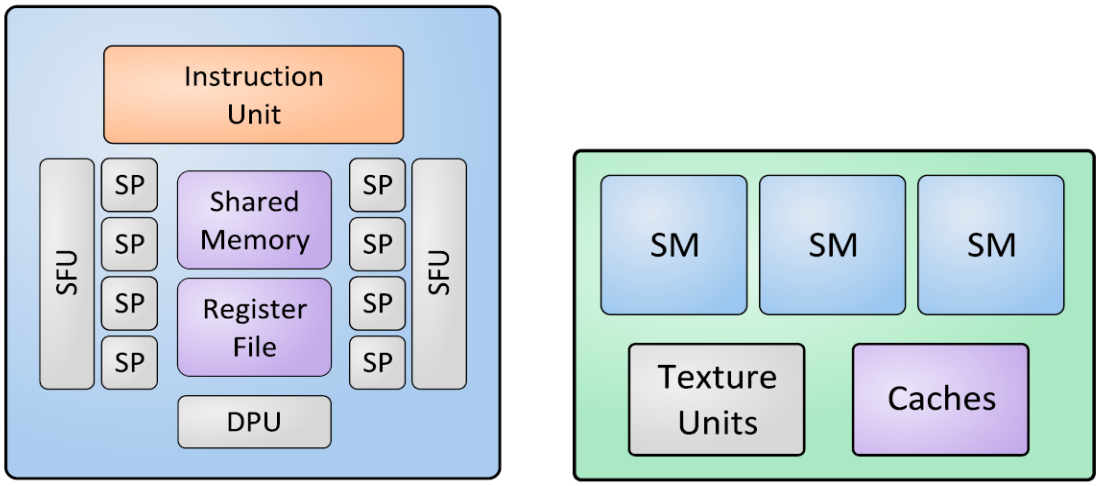
Le GPU sono state maggiormente utilizzate come co-processori grafici che consentono di sgravare le CPU dall'oneroso compito delle elaborazioni grafiche, poco adatto alle caratteristiche di queste unità di elaborazione.

Successivamente il trend è cambiato, le GPU sono state impiegate anche come unità di elaborazione generiche che vengono chiamate GPGPU, ovvero di *General Purpose computing on Grapichs Processor Unit*. Questo perché le GPU, anche se nate per alti fini, risultano particolarmente adatte al calcolo parallelo per programmi scritti con lo scopo di eseguire su unità di elaborazione differenti.

2.2.2 Architettura

Le GPU, essendo progettate inizialmente per applicazioni di elaborazione grafica, presentano un architettura predisposta per eseguire software con numero molto alto di thread in parallelo. La maggiore differenza tra le CPU e le GPU sta proprio in questo: se le prime vengono definite architetture di tipo *multi-core*, per indicare la presenza di un numero relativamente ridotto di unità di elaborazione nello stesso chip, con elevata capacità elaborativa (solitamente 4-8 CPU per chip); le GPU sono più propriamente definite come architetture *many-core* o *hundreds-of-core* a causa dell'elevato numero di core sullo stesso chip, in cui ciascun core ha una capacità elaborativa limitata, ma si riescono a fornire prestazioni eccellenti riducendo i consumi ed ottimizzando il throughput complessivo.

Analizzando in dettaglio l'architettura di una GPU si nota che è costituita da unità chiamate *Thread Processing Cluster* (TPC), che contengono altre unità dette *Streaming Multiprocessor* (SM), le quali a loro volta racchiudono le unità di elaborazione fondamentali denominate *Streaming Processor* (SP).



Nella figura di destra viene mostrato lo schema di un Thread Processing Cluster costituito da 3 SM, con memorie cache condivise tra gli elementi del TPC e memorie dedicate alla gestione di texture.

Sulla sinistra della stessa figura è rappresentato uno Streaming Multiprocessor che contiene 8 processori scalari (SP) che eseguono istruzioni logico/matematiche in virgola mobile e fissa, una memoria condivisa, alcuni registri, 2 unità per funzioni speciali (SFU) per l'esecuzione di funzioni speciali come funzioni trascendenti e matematiche in singola precisione (seno, coseno, ecc.), ed infine un'unita di doppia precisione (DPU) per operazioni in virgola mobile a 64 bit in doppia precisione.

Lo Streaming Multiprocessor gestisce una insieme di thread che raggruppa in unità denominate *warp*. I thread di un warp eseguono lo stesso insieme di istruzioni in maniera indipendente, richiedendo però, che l'esecuzione sia in qualche modo sincronizzata. Se ad esempio uno dei thread dovesse eseguire, a causa di un salto condizionato, un'istruzione diversa da una attualmente in esecuzione sugli altri, questo dovrà aspettare che tutti i thread del warp arrivino allo stesso punto dell'esecuzione. Questa forma di sincronizzazione forzata (*lockstepped*) è affidata ad un componente chiamato *warp scheduler* che disabilita i thread che non si trovano in linea col percorso.

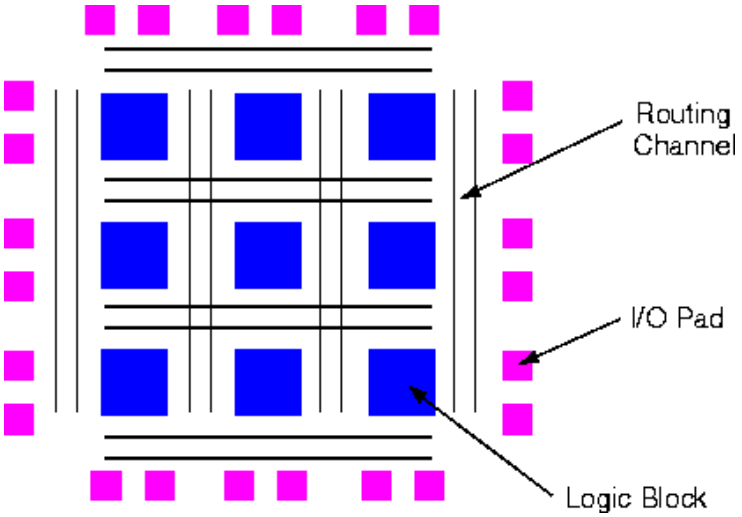
2.3 FPGA

2.3.1 Che cos'è un FPGA

Un *Field Programmable Gate Array* (FPGA) può essere definito come un circuito integrato le cui funzionalità sono programmabili via software. Questa tipologia di dispositivi sono costituiti da un gran numero di porte che permettono di realizzare funzioni logiche molto complesse. Nell'elettronica generale hanno pian piano rivestito un ruolo di primaria importanza soprattutto in campo industriale e nella ricerca. Il primo circuito FPGA risale a metà degli anni '80, costituito da un numero di porte logiche relativamente ridotto rispetto a quelli attuali e di dimensioni complessivamente maggiori. Poi con l'avanzare della tecnologia il numero di porte è aumentato, passando da poche migliaia a qualche milione, e le dimensioni sono diminuite, dando prova di un elevata scalabilità.

2.3.2 Architettura

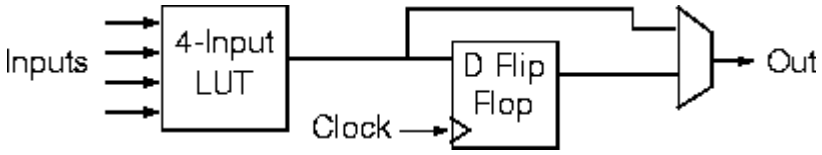
L'architettura di una scheda FPGA si può schematizzare come una matrice di blocchi logici configurabili, chiamati *Configurable Logic Blocks* CLB, con interconnessioni programmabili che sono dei canali di instradamento. Alle estremità della matrice sono presenti i blocchi di ingresso/uscita, *Input Output Block* IOB, collegati ai canali di instradamento attraverso transistor programmabili. Lo scopo dei CLB è quello di



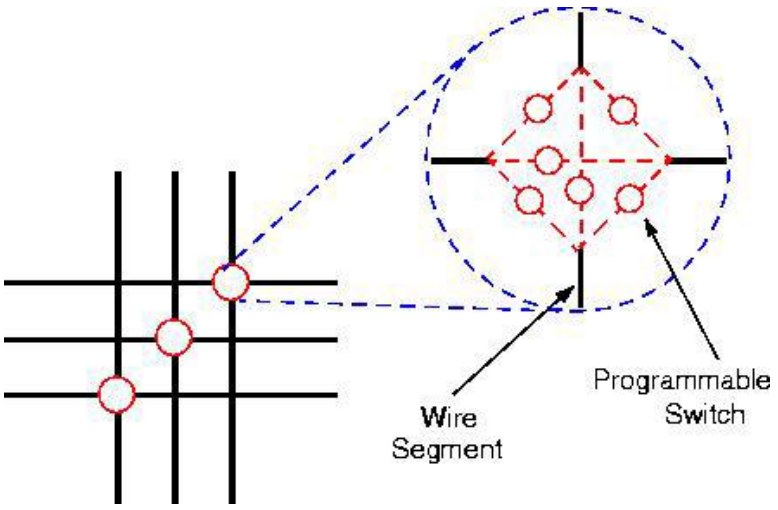
realizzare funzioni logiche, mentre gli IOB si occupano dell'interfacciamento del circuito da e verso l'esterno del FPGA. Nella matrice ci sono anche altre tipologie di componenti tra cui il DCM (*Digital Clock Manager*), che genera il segnale di clock, ed altre risorse di memoria distribuita e di calcolo, come le ALU (*Arithmetic Logic Unit*). Ogni risorsa ha un

compito ben preciso da portare a termine per garantire il corretto funzionamento del chip.

I blocchi logici sono composti generalmente da due o quattro *logic cell* (celle logiche), che eseguono le operazioni logico/booleane. Ogni cella logica è a sua volta costituita da una o più *Look Up Table* (LUT) programmabili che realizzano le funzioni booleane generalizzate. Le LUT hanno anche una piccola porzione di memoria programmata per creare le dipendenze tra la logica di uscita e quella di entrata, ovvero una tabella di verità. Sono costituite da una memoria SRAM da 16 bit e da un multiplexer a 4 ingressi: dopo averle programmate sono in grado di generare qualsiasi funzione logica a quattro ingressi. Avendo più LUT in un CLB connesse da una rete locale di interconnessioni si raggiunge una velocità superiore rispetto a quella tra blocchi logici distinti. Ogni LUT ha una unica uscita, che può essere memorizzata all'interno di un flip flop, in modo da preservarne il valore oltre il singolo ciclo di clock e per riutilizzarlo all'interno di una logica implementativa successiva.



I canali di instradamento corrono lungo i differenti blocchi logici e sono utilizzati per mettere in comunicazione le risorse del dispositivo. Questi canali sono controllati dagli *Switch Block*, ovvero un blocchi di interruzione che ne permettono la programmazione. Le interconnessioni permettono quindi di programmare un enorme numero di logiche differenti e, di conseguenza, di realizzare qualsiasi tipo di funzionalità.



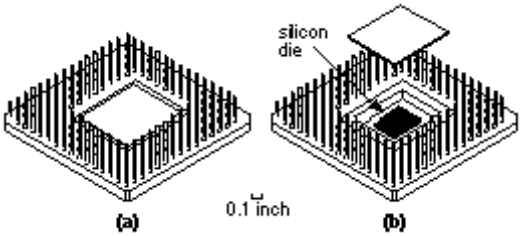
2.4 ASIC

2.4.1 Che cos'è un ASIC

Un *Application Specific Integrated Circuit* (ASIC) viene definito in elettronica digitale come un circuito integrato creato appositamente per risolvere un'applicazione di calcolo ben precisa (*specific purpose*). Realizzare un ASIC significa quindi realizzare un circuito integrato che implementi esattamente un insieme di funzioni logiche prefissate, ossia realizzi un compito specifico rispondendo alle specifiche tecniche che lo descrivono.

I vantaggi che si hanno con i chip ASIC sono molteplici: migliori prestazioni in termini di funzionalità e velocità, aumento dell'affidabilità, diminuzione dei costi di produzione, dimensioni e pesi ridotti, riduzione dei consumi, non riproducibilità e migliore qualità ed impiego di tecnologie avanzate. Da questo ne è derivato un enorme successo ed una grande diffusione nel corso del tempo.

2.4.2 Come è fatto un ASIC



La figura mostra un circuito integrato con un *Pin Grid Array* sulla sinistra e il *silicon di*e, il dado di silicio o chip vero e proprio, sulla destra, la cui dimensione può variare da pochi millimetri a qualche centimetro a seconda della complessità.

Un ASIC è generalmente incapsulato all'interno di un involucro ceramico o plastico, mentre la restante parte è costituita dalle linee che collegano i piedini agli ingressi e uscite del chip. La complessità di un ASIC viene misurata in termini di numero di gate logici o numero di transistors contenuti al suo interno. Generalmente un gate corrisponde a quattro transistors, per cui dal numero di gate si può risalire al numero di transistors presenti in un ASIC.

2.4.3 Tipi di ASIC

Esistono diverse tipologie di ASIC che si distinguono in: *full-custom ASIC, standard-cell based ASIC, gate-array based ASIC*.

Tra i *full-custom ASIC* un esempio che li rappresenta a pieno è il microprocessore. In questa tipologia di ASIC tutte le celle logiche sono completamente personalizzabili ed anche il layout, ovvero la disposizione dei componenti del circuito e la loro interconnessione. I full-custom ASIC sono i più complessi e versatili tipi di circuiti integrati, di conseguenza sono anche i più costosi da produrre e da progettare. In questo caso il progettista non utilizza celle logiche predefinite, ma progetta, alcuni o tutti, i circuiti specifici per il singolo ASIC.

La tecnologie più utilizzate sono però le standard-cell-based e gate-array-based, in cui tutte le celle logiche sono predefinite e quasi tutte le maschere per gli strati sono personalizzabili, rendendo i costi di produzione inferiori e la progettazione facilitata.

Le *standard-cell-based ASIC* (CBIC, pronunciato "sea-bick") usano celle logiche predefinite (AND, OR, multiplexer, flip-flop) note come celle standard (SC). Le SC sono disposte in righe e costituiscono le cosiddette *standard-cell areas*. Il progettista ASIC definisce dove piazzare le SC all'interno del IC e le sue interconnessioni. Le SC possono essere piazzate ovunque nel silicio, quindi le maschere sono personalizzate ed uniche in ogni progetto. Il vantaggio dei CBIC è che il progettista risparmia tempo e denaro riducendo i rischi, mentre gli svantaggi sono il tempo e il costo di progettare le nuove SC.

Nei *gate-array-based ASIC* (abbreviati GA) i transistor sono invece predefiniti nel wafer del silicio. Tali transistor sono combinati in modo da formare il *base array*; il più piccolo elemento che viene replicato per formare l'array base è chiamato *base cell* (cella base o primitiva). Nei GA la costituzione della cella base è la stessa per ogni cella logica e solo gli strati di livello più alto, che caratterizzano l'interconnessione tra transistor, sono definiti dai progettisti attraverso maschere personalizzate. Il progettista deve quindi scegliere tra una libreria di celle logiche già prefabbricate chiamate *macros*. Il costo di fabbricazione è di conseguenza inferiore rispetto ad una SC o un full-custom ASIC come anche il costo di progettazione. Uno degli svantaggi è però questa struttura predefinita e meno flessibile.

Capitolo 3: Bitcoin Mining Technology

3.1 L'evoluzione dell'hardware per il Bitcoin Mining

Come già detto precedentemente il sistema Bitcoin fa uso dei miners per memorizzare e inviare in broadcast il blockchain e verificare le nuove transazioni.

A causa della popolarità della moneta bitcoin e della competitività che si è venuta a creare per il mining, nel corso degli anni sono state utilizzate differenti tecnologie hardware al fine di migliorare le performance e l'efficienza energetica. La velocità delle operazioni viene misurata in hashrate (h/s hash generati al secondo, con i multipli kH/s, MH/s, GH/s, TH/s) che riguardano il calcolo della funzione di hash SHA-256 eseguita più volte.

Dal 2009 ad oggi i miners hanno sperimentato essenzialmente quattro tipologie di hardware differenti (CPU, GPU, FPGA e ASIC) che si sono susseguite e hanno aumentato progressivamente la potenza computazionale del sistema.

3.2 CPU mining

Quando tutto è iniziato chiunque (anche persone che non ne sapevano niente al riguardo) usavano le CPU per l'attività del mining. Era l'unico modo conosciuto per farlo ed era sufficiente utilizzare la CPU general-purpose del proprio personal computer per ottenere i risultati sperati. Oggigiorno anche dopo anni sarebbe probabilmente impossibile ottenere anche un semplice bitcoin, dato che la difficoltà è aumentata e continua ad aumentare rapidamente. Sulle general-purpose CPU la potenza computazionale varia in un range tra i 2-20 MH/s a seconda della potenza della CPU, oggi risulta inadeguata e per questo il mining con CPU è stato abbandonato completamente. Utilizzando ad esempio una CPU di fascia alta, che permette un throughput di 20 MHz, attualmente ci vorrebbero 139,461 anni per trovare un blocco valido.

3.3 GPU mining



Una volta che le CPU sono risultate essere poco efficienti per l'attività di mining, i miners hanno iniziato a usare le GPU che si sono rivelate essere più adatte per la rete Bitcoin. All'inizio il mining attraverso le GPU era risultato essere più redditizio in termini di "bitcoins mined", portando un incremento nell'efficienza, rispetto a quanto avveniva con le CPU.

Il cambiamento al GPU mining è iniziato nel Luglio del 2010 quando il primo OpenCL miner è stato scritto e utilizzato. Nel Settembre dello stesso anno anche il primo open-source GPU miner basato su CUDA è stato rilasciato.

Risulta particolarmente interessante che le architetture di schede grafiche AMD si sono rivelate essere molto più efficienti rispetto al principale competitor dell'NVIDIA.

I vantaggi che le GPU hanno apportato riguardano sostanzialmente: *high parallelism* e *high throughput*. Tipicamente "multiple hash calculation" sono eseguite simultaneamente

sfruttando il parallelismo offerto dalle GPU. Molti miners hanno modificato alcuni parametri dell'hardware, come il voltaggio e la frequenza di clock della RAM video e del GPU core allo scopo di ottenere un throughput più alto (overclocked) riducendo il costo di funzionamento di ogni singola GPU e aumentando l'efficienza.

Allo scopo di aumentare ulteriormente i profitti i miners erano soliti collocare più GPU sulla stessa motherboard, fornendo hashrate più alti. Tuttavia ogni GPU aggiunta implica un aumento risorse sprecate perché ogni unità elaborativa include hard-drive, RAM e processori inutilizzati. Inoltre dispositivi aggiuntivi comportano una maggiore necessità di potenza energetica e raffreddamento. La potenza di consumo di ogni GPU era di circa 200W in media.

Per concludere vengono sintetizzati vantaggi e svantaggi del mining attraverso le GPU

3.3.1 Vantaggi

Facilmente disponibili e installabili: è possibile ordinare e comprare GPU on-line o in negozi di elettronica.

Parallel ALU: sono progettate per lavorare in parallelo e hanno numerose ALU perfettamente adeguate a svolgere quest'attività.

Bit-specific instruction: supportano operazioni bit a bit particolarmente utili per lo SHA-256.

Controllabili da un unica CPU: molte GPU possono essere facilmente controllate da un unica CPU su un unica motherboard.

Overclock: si possono sovraccaricare superando i parametri massimi di progettazione. Questo è un rischio che si è soliti prendere per il bitcoin mining anche se si introducono degli errori nel processo. Quello che conta è il *goodput = throughput x success rate* (quanto velocemente si trovano i blocchi x quanto spesso il calcolo presenta errori).

3.3.1 Svantaggi

Poor utilization of hardware: le GPU hanno molto altro hardware progettato per la grafica che veniva totalmente inutilizzato nel Bitcoin mining.

Poor cooling: non vengono progettate per essere eseguite insieme in uno spazio piccolo

l'une vicino alle altre, per questo mostravano problematiche di raffreddamento.

Large power draw: era richiesta molta energia elettrica per il loro utilizzo.

Few boards to hold multiple GPU: si doveva comprare una scheda grande molto costosa o costruire la propria scheda per ospitare più GPU.

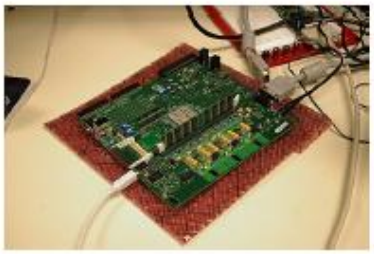
Le performance che si riuscivano ad ottenere su una buona scheda grafica erano di circa 200MHz. Alla difficoltà attuale mettendo insieme 100 schede grafiche di buon livello sarebbero necessari 173 anni per trovare un blocco, per tale motivo anche queste sono state abbandonate.

Nell'immagine che segue si può notare il trend che si era sviluppato dove si cercava di avere più GPU possibili all'interno di una stessa stanza.

3.4 FPGA mining

Sebbene la transizione tra GPU e FPGA non è stata così spettacolare come quella tra CPU e GPU in termini di efficienza, ha segnato l'era dell'hardware specializzato per il Bitcoin mining, dato che l'FPGA è un circuito integrato che può essere adattato al bisogno dell'utente dopo la fabbricazione. Questa è stato anche il periodo della forte commercializzazione dell'hardware Bitcoin.

Il più grande cambiamento riscontrato è stata una riduzione nel consumo della potenza energetica di cinque volte inferiore rispetto alle GPU dando un 30% di miglioramento nell'efficienza del mining a parità di energia spesa.



Schede FPGA per il mining sono apparse nel Giugno del 2011 programmate in Veriolog, l'hardware design language utilizzato per programmare FPGA. Nonostante non ci sono stati grandi vantaggi intermini di efficienza, questi chip forniscono un netto miglioramento nelle operazioni bit a bit utili per l'algoritmo SHA-256. Furono creati diversi progetti open-source che potevano essere utilizzati per differenti tipi di FPGA. Un altro punto a favore delle FPGA era la possibilità di poter creare tante unità parallele per l'hash calulation, quante potevano entrarne sulla scheda. Tali unità sono totalmente indipendenti l'une dalle altre e ognuna richiede quindi il proprio tempo di calcolo. È necessario combinare più chip insieme per ottenere performance migliori.

Si possono schematizzare vantaggi e svantaggi dell'FPGA come segue.

3.4.1 Vantaggi

Higher performance then GPU: si hanno performance maggiori delle GPU in particolare per le operazioni bit a bit.

Better cooling: rispetto alle GPU si comportano meglio per quanto riguarda il raffreddamento quando unite insieme e controllate da un unità centrale.

Extensive customisation, optimisation: personalizzabili e riconfigurabili a piacere dell'utente per differenti scopi.

Quello a cui si è andato in contro è stato simile a quello che era avvenuto per le GPU, ovvero unire più FPGA per ottenere risultati più prestanti.

3.4.2 Svantaggi

Power-hungry: sono ancora causa di grandi consumi per quanto riguarda la potenza energetica.

Poor optimization of 32-bit adds: bassa ottimizzazione per l'addizione a 32-bit utile per lo SHA-256.

Fewer hobbyists with sufficient expertise: è più difficile comprare FPGA e meno persone sapevano come programmarle (erano necessarie competenze più specifiche).

More expensive then GPU: erano più costose delle GPU.

Marginal performance/cost advantage over GPUs: incremento dei costi e performance, ma i vantaggi erano in fin dei conti marginali.

L'FPGA è stato solamente per pochi mesi la soluzione migliore per il bitcoin mining. Utilizzando 100 schede a 1000MHz FPGA in modo adeguato si impiegava in ogni caso all'incirca 25 anni per trovare un blocco valido.

3.5 ASIC mining

L'ultima tecnologia adottata per il Bitcoin mining (almeno fino ad ora) è quella degli ASIC (*Application-Specific Integrated Circuit*). I chip ASIC, a differenza delle GPU e CPU, vengono fabbricati con l'unico scopo del Bitcoin mining, non possono essere usati per nessun altro fine. Questo ha diminuito notevolmente il costo del mining, in particolare per quanto riguarda il consumo di energia elettrica. Il bisogno di performance più alte ed efficienza energetica ha spinto i bitcoin miners ad adottare questa soluzione.

Né GPU né FPGA possono essere paragonate ai dispositivi ASIC. I primi chip di questa tecnologia iniziarono ad apparire in rete agli inizi del 2013 ed al giorno d'oggi dominano completamente il mercato. La specializzazione dell'hardware è diventata l'unica possibile forma esistente per l'industria del cryptocurrency mining e attualmente non c'è niente che

possa rimpiazzare gli ASIC.

Questi chip progettati e fabbricati con il solo scopo del Bitcoin mining sono facilmente disponibili on-line, il numero di venditori è incrementato sensibilmente negli ultimi due anni. Le schede si differenziano per grandezza, prestanza, costo, potenza necessaria, efficienza, etc. Ciò che sta diventando problematico è quanto velocemente vengano spedite al compratore, c'è un'enorme richiesta e vengono preordinate prima che siano ancora disponibili, senza che si abbia alcuna garanzia sulla data di consegna. Anche pagandole prima ci sono lamentele per i tempi di consegna poiché, nonostante i prezzi a cui sono state pagate, si rischia di avere un hardware ormai già superato a causa del troppo ritardo.

Le principali caratteristiche degli ASIC sono le seguenti:

Special purpose: progettate esclusivamente per il Bitcoin mining.

Designed to be run constantly for life: progettate appositamente per essere eseguite costantemente per tutto il loro ciclo di vita.

Require significant expertise, long lead-times: competenze non banali nella fabbricazione e lunga esecuzione.

Perhaps the fastest chip development ever: hanno prestazioni che attualmente non possono essere conseguite in altro modo.

3.5.1 Caso di studio: TerraMiner IV

Prima spedizione Gennaio 2014

Hashrate: 2 TH/s

Costo: US$ 6,000

Sono ancora necessari 14 mesi per cercare un nuovo blocco valido.

3.5.2 Dinamiche di mercato

La maggior parte delle schede diventano obsolete in 3-6 mesi e la maggior parte dei profitti viene fatta nelle prime 6 settimane. Per questo se vengono consegnate anche con una settimana di ritardo significa aver perso un sesto del profitto ottimo. Questo è sostanzialmente il motivo per cui le aziende richiedono preordini, data la grande competizione che si ha per avere le schede ASIC prima di tutti. Esistono anche problemi di speculazione perché alcune aziende che fabbricano schede ASIC, le eseguono per alcune settimane prima di spedirle ai consumatori. La dinamica di mercato sta ormai diventando alquanto complicata. Nonostante queste problematiche il prezzo dei bitcoin si sta alzando progressivamente ed è per questo che risulta in ogni caso è conveniente l'attività di mining.

3.5.2 Professional mining centers

Oggi siamo ufficialmente nell'era di centri professionali per il bitcoin mining. I dettagli di come sono organizzati questi centri non sono particolarmente chiari, perché le aziende che si occupano del mining non vogliono diffondere precisamente il loro modo di lavorare. In ogni caso questo è sicuramente un fenomeno che si sta diffondendo in tutto il mondo.

Un esempio di mining center è quello raffigurato dell'immagine seguente che mostra un centro nella Repubblica di Georgia.

Le caratteristiche essenziali che un luogo deve avere per essere adatto ad ospitare un centro di bitcoin mining sono:

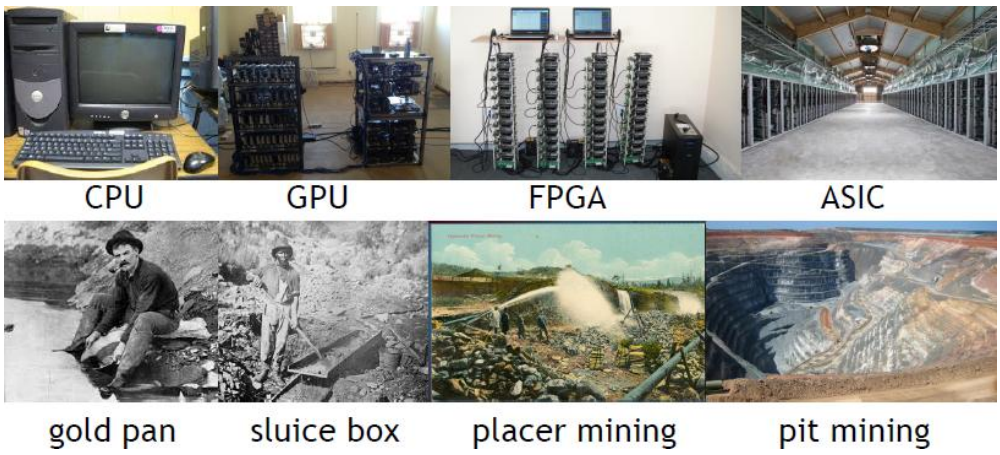
Cheap power: elettricità a basso costo;

Good network: buona connessione Internet per trovare soluzioni più velocemente;

Cool climate: un tempo relativamente freddo per non spendere troppo in impianti di raffreddamento.

3.5.3 Analogia con il gold mining e riflessioni

Nel pensare all'evoluzione del Bitcoin mining si può fare un parallelismo interessante con il gold mining (estrazione dell'oro). L'evoluzione per il bitcoin è partita dalle CPU che possono essere paragonata alle singole persone che andavano a cercare l'oro con semplici pentole. Fino ad arrivare alle ASIC che ricordano le grandi miniere d'oro sicuramente oggi più adatte e remunerative.



Così come è avvenuto per l'oro anche per il bitcoin mining la possibilità per piccoli gruppi o singoli individui di entrare nel mercato in maniera redditizia sta diminuendo e nello stesso tempo si sta avendo un consolidamento delle grandi industrie. La domanda che ci si pone è quindi se piccoli miners possono stare ancora restare in gioco? Gli ASIC violano lo spirito originale del Bitcoin? Sarebbe stato meglio senza gli ASIC che con questi grandi centri per il mining vanno contro la visione originale di Satoshi Nakamoto che era quella di avere ogni singolo individuo della rete a fare mining sul proprio computer?

Le risposte a queste domande sono abbastanza controverse nella comunità scientifica, perché se da un lato queste idee vanno contro la visione originale del bitcoin, dall'altra

parte sarebbe impossibile oggi pensare di fare mining ancora attraverso le CPU senza utilizzare i chip specializzati.

3.6 Confronto ed efficienza energetica

In questo paragrafo vengono messe a confronto le architetture FPGA e ASIC mostrando quali sono gli aspetti a favore delle une e delle altre, giustificando quindi il motivo per cui attualmente i chip ASIC dominano il mercato. Entrambi sono microchip ma hanno caratteristiche differenti:

FPGA	ASIC
È un circuito integrato le cui funzionalità sono programmabili via software da un progettista	È un circuito integrato creato appositamente per risolvere un applicazione di calcolo ben precisa
Ciclo di progettazione semplice e veloce	Ciclo di progettazione complesso e lungo
Software per la progettazione economico	Software per la progettazione costoso
Costi iniziali bassi, poi costi per unità alti	Costi iniziali alti, poi costi per unità bassi
Occupano molto spazio e dissipano più potenza	Occupano poco spazio e dissipano poca potenza
Frequenze di funzionamento basse	Frequenze di funzionamento alte
È possibile apportare modifiche in qualsiasi momento	Non sono modificabili

Conclusioni

Si è giunti al termine di questa trattazione che si è focalizzata sulla descrizione del sistema Bitcon analizzando in particolare le architetture di calcolo di supporto al suo funzionamento.

Nonostante è un fenomeno ancora in evoluzione, Bitcoin rappresenta il capostipite di una nuova generazione di tecnologie che rivoluzioneranno molti settori. Permette di scambiare moneta elettronica in maniera sicura ed ha mostrato nel suo ciclo di vita una notevole resistenza ad attacchi, scalabilità e flessibilità. Bitcoin mette a disposizione una nuova piattaforma per l'innovazione, sta cambiando la finanza allo stesso modo in cui la rete ha cambiato l'editoria. Proprio per questo risulta difficile inquadrarlo all'interno di confini prestabiliti in aspetti economici, politici e legali. La possibilità di scavalcare le istituzioni finanziarie e l'indipendenza dalle banche centrali hanno generato opinioni contrastanti, alcune positive ed altre hanno addirittura portato alla chiusura di punti di exchange in alcuni paesi.

Indipendentemente dagli sviluppi futuri di successo o meno, Bitcoin, che non è solo una cripto moneta, ma anche un protocollo e una tecnologia, costituisce un'idea rivoluzionaria che offre nuovi stimoli per nuovi scenari. Rappresenta un nuovo paradigma nello sviluppo dei sistemi distribuiti p2p basato sulla crittografia e sulla decentralizzazione. Le occasioni che offre sono innumerevoli e attendono soltanto di essere esplorate.

Per quanto riguarda la tecnologia hardware di supporto al sistema, prima o poi si troverà

sicuramente il modo di migliorala per permettere un attività di mining più veloce ed efficiente. Tuttavia le ricerche fatte in quest'ambito sostengono che non ci sarà un passaggio a una quinta generazione di miners in tempi brevi, perché le prestazioni attuali risultano soddisfacenti e i miglioramenti che porterebbe sarebbero marginali.

Bibliografia

[1] David Lee Kuo Chuen, “Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data”, Academic Press, May 5, 2015, pp. 5-64, URL: https://books.google.it/books?hl=en&lr=&id=RfWcBAAAQBAJ&oi=fnd&pg=PA45&dq=bitcoin+hardware+comparison&ots=2LtMJjB6AA&sig=CIShHrRR30p4FxZUizfndVcJ7tI#v=onepage&q&f=false

[2] Satoshi Nakamoto, “A Peer-to-Peer Electronic Cash System”, 2008, URL: http://bitcoin.org/bitcoin.pdf

[3] Nicolas T. Courtois, Marek Grajek, Rahul Naik, “The Unreasonable Fundamental Incertitudes Behind Bitcoin Mining”, 2014, URL: http://arxiv.org/pdf/1310.7935v3.pdf

[4] Torbjørn Langland, Kristian Klomsten Skordal, “Mining Bitcoins using a Heterogeneous Computer Architecture”, 2015, URL: https://daim.idi.ntnu.no/masteroppgaver/012/12754/masteroppgave.pdf

[5] Samuel Oliveira, Filipe Soares, Guilherme Flach, Marcelo Johann, Ricardo Reis, “Building a Bitcoin Miner on an FPGA”, 2008, URL: http://www.inf.ufrgs.br/sim-emicro/papers2012/sim2012_submission_46.pdf

[6] Bitcoin, URL: https://bitcoin.org/it/, (visitato il 31/08/2016)

[7] Bitcoin wiki, URL: https://en.bitcoin.it/wiki/Main_Page, (visitato il 31/08/2016)

[8] Wikipedia it: Bitcoin, URL: https://it.wikipedia.org/wiki/Bitcoin, (visitato il 31/08/2016)

[9] Wikipedia en: Bitcoin, URL: https://en.wikipedia.org/wiki/Bitcoin, (visitato

il 31/08/2016)

[10] Bitcoin miner, URL: http://bitcoinminer.com/, (visitato il 31/08/2016)

[11] Weusecoin, URL: https://www.weusecoins.com/, (visitato il 31/08/2016)

[12] Bitcoin mining, URL: https://www.bitcoinmining.com/, (visitato il 31/08/2016)

[13] Bitcoin, URL: https://www.bitcoin.com/, (visitato il 31/08/2016)

[14] Bitcoin and Cryptocurrency Technologies - Princeton University Lecture 5 Bitcoin mining, 2015, URL: https://docs.google.com/presentation/d/1fLe3sh9LRnijhAknIU4rb-EfF_bs6LJ1C6hBGq3fj_g/edit#slide=id.p

[15] ImponderableThings (Scott Driscoll's Blog) - How Bitcoin Works Under the Hood, URL: http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html, (visitato il 31/08/2016)

[16] Ken Shirriff's blog - Mining Bitcoin with pencil and paper URL: http://www.righto.com/2014/09/mining-bitcoin-with-pencil-and-paper.html, (visitato il 31/08/2016)

[17] Ken Shirriff's blog - Bitcoin mining the hard way: the algorithms, protocols, and bytes URL: http://www.righto.com/2014/02/bitcoin-mining-hard-way-algorithms.html, (visitato il 31/08/2016)

[18] “Bitcoin: aspetti tecnici, economici e politici di una critto valuta”, 2014 URL: http://amslaurea.unibo.it/7313/1/costa_pierfrancesco_bitcoin.pdf

[19] “Bitcoin, la cripto moneta”, 2014 URL: http://tesi.cab.unipd.it/47076/1/Rossi_Silvia.pdf

[20] Wikipedia Moneta alternativa, URL: https://it.wikipedia.org/wiki/Moneta_alternativa, (visitato il 31/08/2016)

[21] Wikipedia: Criptovaluta, URL: https://it.wikipedia.org/wiki/Criptovaluta, (visitato il 31/08/2016)

[22] Wikipedia: SHA, URL: https://it.wikipedia.org/wiki/Secure_Hash_Algorithm, (visitato il 31/08/2016)

[23] Wikipedia: SHA-256, URL: https://en.wikipedia.org/wiki/SHA-2, (visitato il

31/08/2016)

[24] “Description of the SHA-256, SHA-384, and SHA 512”, URL: http://www.iwar.org.uk/comsec/resources/cipher/sha256-384-512.pdf, pp. 2-9

[25] John D. Owens, Mike Houston, David Luebke, Simon Green, John E. Stone, and James C. Phillips, “GPU Computing”, 2008, URL: http://cs.utsa.edu/~qitian/seminar/Spring11/03_04_11/GPU.pdf

[26] Politecnico di Milano, corso di Architetture Avanzate (dispense), “Architetture dei calcolatori, l’approccio GPU), 2012, URL: http://home.dei.polimi.it/sami/architetture_avanzate/GPU_11.pdf

[27] Introduzione alla progettazione degli ASIC, URL: http://www.salvitti.it/geo/asic/, (visitato il 02/09/2016)

[28] Michael John Sebastian Smith, “Application-Specific Integrated Circuits, Introduction to ASICs”, Addison Wesley, 2004, URL: https://ia801301.us.archive.org/32/items/ApplicationSpecificIntegratedCircuitsAddisonWesleyMichaelJohnSebastianSmith/Application-Specific%20Integrated%20Circuits%20-%20Addison%20Wesley%20Michael%20John%20Sebastian%20Smith.pdf

[29] Wikipedia: Field Programmable Gate Array (FPGA), URL: https://it.wikipedia.org/wiki/Field_Programmable_Gate_Array, (visitato il 02/09/2016)

[30] FPGA Architecture for the Challenge, URL: http://www.eecg.toronto.edu/~vaughn/challenge/fpga_arch.html, (visitato il 02/09/2016)