GPU Implementation in Bitcoin Mining

Introduction to Bitcoins:
Bitcoin is one of the first implementations of a concept called ”crypto-currency”. Based on this concept, bitcoin is designed around the idea of a new form of money that uses cryptography to control its creation and transactions, rather than relying on central authorities.

Bitcoin (BTC) is an online commodity that is based on an open-source, peer-to-peer encryption protocol first described in 2009. Bitcoin creation and transfer is accomplished on an Internet-based network and is not managed by any central authority. The creation of new bitcoins is automated and may be accomplished by servers, called bitcoin miners that confirm bitcoin creation by adding codes to a decentralized log, which is updated and archived periodically.

Bitcoin is accepted in trade by various merchants and individuals in many parts of the world.

New bitcoins are generated by the network through the process of ”mining”. In a process that is similar to a continuous raffle draw, mining nodes on the network are awarded bitcoins each time they find the solution to a certain mathematical problem (and thereby create a new block). Creating a block is a proof of work with a difficulty that varies with the overall strength of the network. The reward for solving a block is automatically adjusted so that roughly every four years of operation of the Bitcoin network, half the amount of bitcoins created in the prior 4 years are created.

As the amount of processing power directed at mining changes, the difficulty of creating new bitcoins changes. This difficulty factor is calculated every 2016 blocks and is based upon the time taken to generate the previous 2016 blocks

Bitcoin Mining :
Mining is the process of using your computer’s processing power to process transactions for the Bitcoin network.
By allowing our computer to do a certain amount of cryptographic work ,we are rewarded with some Bitcoin.
In detail ,it is the process of adding transaction records to Bitcoin’s public ledger of past transactions. This ledger of past transactions is called the block chain as it is a chain of blocks. The block chain serves to confirm transactions to the rest of the network as having taken place. Bitcoin nodes use the block chain to distinguish legitimate Bitcoin transactions from at-

tempts to respend coins that have already been spent elsewhere.
Mining is intentionally designed to be resource-intensive and difficult so that the number of blocks found each day by miners remains steady. Individual blocks must contain a proof of work to be considered valid. This proof of work is verified by other Bitcoin nodes each time they receive a block.
The mining process or proof-of-work process involves scanning for a value that when hashed with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required, but can always be verified by executing a single hash.
For the bitcoin timestamp network, it implements the mining process or "proof-of-work" by incrementing a nonce in the record or "block" until a value is found that gives the block's hash the required zero bits. Once the hashing effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later records or "blocks" are chained after it, the work to change the block would include redoing all the blocks after it.
The bitcoin specification starts with a timestamp. A timestamp server works by taking a SHA256 hash function of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.

Difficulty:
The Computationally-Difficult Problem:
Mining a block is difficult because the SHA-256 hash of a block's header must be lower than or equal to the target in order for the block to be accepted by the network. This problem can be simplified for explanation purposes: The hash of a block must start with a certain number of zeros. The probability of calculating a hash that starts with many zeros is very low, therefore many attempts must be made.

Reward:
When a block is discovered, the discoverer may award themselves a certain number of bitcoins, which is agreed-upon by everyone in the network. Currently this bounty is 25 bitcoins; this value will halve every 210,000 blocks.

GPU IMPLEMENTATION in Mining Bitcoins:
By using GPUs (Graphics Processing Units) we can get a significant increase in computational power over conventional CPUs in mining bitcoins.
In the beginning, mining with a CPU was the only way to mine bitcoins. This eventually gave way to mining on graphics cards (GPU) due to the fact that the massively parrallel nature of some GPUs allowed for a 50x to

100x increase in minging power while using less power usage per megahash compared to a CPU.

Why a GPU is prefered over CPU for Bitcoin Mining?
A CPU core can execute 4 32-bit instructions per clock (using a 128-bit SSE instruction) or 8 via AVX (256-Bit), whereas a GPU like the Tesla c2050 can execute a 1.15 ghz clock rate (using its 448 CUDA cores).
A CPU is designed primarily to be an executive and make decisions, as directed by the software. For example, if you type a document and save it, it is the CPU's job to turn your document into the appropriate file type and direct the hard disk to write it as a file. CPU's can also do all kinds of math, as inside every CPU is one or more "Arithmetic/Logic Units" (ALU's). CPU's are also highly capable of following instructions of the "if this, do that, otherwise do something else". A large bulk of the structures inside a CPU are concerned with making sure that the CPU is ready to deal with having to switch to a different task on a moment's notice when needed.
CPU's also have to deal with quite a few other things which add complexity, including enforcing privilege levels and the boundaries between user programs and the operating system and creating the illusion of "virtual memory" to programs.
A GPU is very different.
Hash processing is a lot of repetitive work, since it is constantly being told to do the same thing to large groups data blocks . In order to make this run efficiency, GPUs are far heavier on the ability to do repetitive work, than the ability to rapidly switch tasks.
GPU's have large numbers of ALU's, more so than CPU's. As a result, they can do large amounts of bulky mathematical labor in a greater quantity than CPU's.

Conclusion:
We have used the Nvidia Tesla c2050 which has shown a significant performance in mining bitcoins.This particular card has 448 "Stream Processors", which can be thought of as 448 execution units that can be trained to do the same repetitive task, just so long as they don't have to make any decisions that interrupts their flow. Those execution units are contained in blocks.
Since ALU's are what do all the work of Bitcoin mining, the number of available ALU's has a direct effect on the hash output.Trying a single SHA256 hash in the context of Bitcoin mining requires around 1,000 simple mathematical steps that must be performed entirely by ALU's.
Thus, GPU's can mine Bitcoins so much faster than CPU's. Bitcoin mining requires no decision making - it is repetitive mathematical work for a computer. The only decision making that must be made in Bitcoin mining is, "do I have a valid block" or "do I not". That's an excellent workload to run on a GPU.