Bitcoin Mining.

In bitcoin, miners need to validate every transaction and to reach a consensus on which blocks to include in the block chain. To be a bitcoin miner, you need to join to the bitcoin network and to connect to other nodes of the network. At this point, there are sis tasks to perform by a miner: (i) listen for transactions, (ii) maintain the block chain and listen for new blocks, (iii) assemble a candidate block, (iv) find a nonce that makes your block valid, (v) hope that this block is accepted, and (vi) obtain a profit. In this process it's important to determine the mining difficulty (that changes around every two weeks. Each miner independently computes the difficulty and only accepts blocks that meet the difficulty that they computed, that helps to arrive to a consensus. Hardware used to mine bitcoins needs to solve SHA-256 hash functions, and in that way, there are different kinds of mining: (i) CPU mining, (ii) GPU mining, (iii) FPGA (Field Programmable Gate Arrays) mining, and (iv) ASIC (Application-Specific Integrated Circuits) mining. One of the consequences of the bitcoin mining is the energy consumption of the mining data centers. Energy is consumed in different moment into this process: (i) embodied energy, that is, when the mining equipment is manufactured, (ii) electricity during the mining, and (iii) cooling the mining equipment.

Sometimes, a group of miners joint and form a mining pool in which no matter who find the block, the pool manager will receive the rewards and distribute it to all the participants. There are different forms in which this benefits can be distributed: (i) mining shares, in which miners can prove probabilistically how much work they are doing, (ii) pay-per-share, in which the manager pays a flat fee for every share above a concrete difficulty for the block in which the pool is working, (iii) proportional, in which the reward depends on whether or not the pool founds a valid value (there is no flat fee), and (iv) pool hopping, in which there are two different pools and miners might be incentivized to switch between pools.

There are different incentives and strategies to mining bitcoins, in which it is important to consider: (i) which transactions needs to be included, (ii) which bloc to mine on, (iii) choosing between blocks at the same heights, and (iv) find the best moment to announce new blocks. Miners need to be aware about different deviations (attacks) to the default behavior, for example: (i) forking attacks, that are used to perform a double spend, (ii) forking attack with bribery, in which is possible to bribe the people to work on your behalf, (iii) temporary block-withholding attack. In which a new block is not announced, but the miner can continue working over this block, (iv) blacklisting and punitive forking, in which a miner blacklists transactions from another miner, and (v) feather-forking, in which a miner announces that he refuses to mine an any chain that has certain transactions.

Finally, solving bitcoin puzzles are the basic task of bitcoin miners, in which these puzzles are hash-preimage puzzles, the goal of miners is to find the preimages for a partially specified hash output.