University of Oslo
Blockchain and Distributed Technologies

Name: Sowelu
Surname: Avanzo

Summary of the course materials

Topic 1: Bitcoin

In Curran (2018) and Chumbley and collaborators (Brilliant.org) the basic characteristics of the Merkle Tree, a hash-based data structure are described. This underpins the functioning of blockchains and of several distributed systems, such as Git or IPFS (Curran, 2018). The design of the Bitcoin blockchain is structured in such a way that each block contains a set of transactions, and additional data included in its header that are essential for the functioning of the blockchain. Every transaction SHA-256 hash is a leaf node of a binary Merkle Tree, whose root node is stored in the block header in addition to: the block version number, the previous block hash, the timestamp, the mining difficulty target and the nonce of the block.
This data structure facilitates verification of the integrity and validity of transaction data which in its turn reduces the amount of information sent through the network and processed by the participants. This is achieved by adopting Merkle Proofs, particularly useful in Simple Payment Verification (SPV). SPV refers to the possibility to check the validity of a certain transaction or block by comparing a small subset of hashes, rather than performing a lookup on the entire blockchain.
Moreover, the Bitcoin blockchain design enables the pruning of insessential branches, which further increases the efficiency of verification operations.

The Bitcoin network is maintained through the mining process, described in Chapter 5 of *Bitcoin and Cryptocurrency Technologies* (Narayanan et al. 2016). The actions performed by miners are the following: these listen to new transactions and ensure that those are valid, assemble blocks, find a nonce making the block valid, and communicate the valid block to the network. After the block is accepted by the network, a reward is transferred to the miner's wallet.
Finding the right nonce is part of solving a Proof-of-Work puzzle, whose difficulty is automatically adjusted every 2016 blocks to be maintained constant in relation to the computational power adopted by miners.
Since mining is extremely energy-consuming, it requires specialized hardware to be performed efficiently. The chapter also examines the state of the art in the mining industry and presents the challenges related to the network centralization this process involves.
Furthermore, the authors outline the problems related to the high ecological impact of hardware production, shipping and computations performed to solve the Proof-of-Work puzzle.
In chapter 8 of the book, the authors present alternative puzzles that are intended to solve the centralization and energy consumption issues. In particular, solutions that enable useful computations to be performed during mining (Proof-of-Useful-Work), and virtual mining solutions are being explored, including Proof-of-Stake.