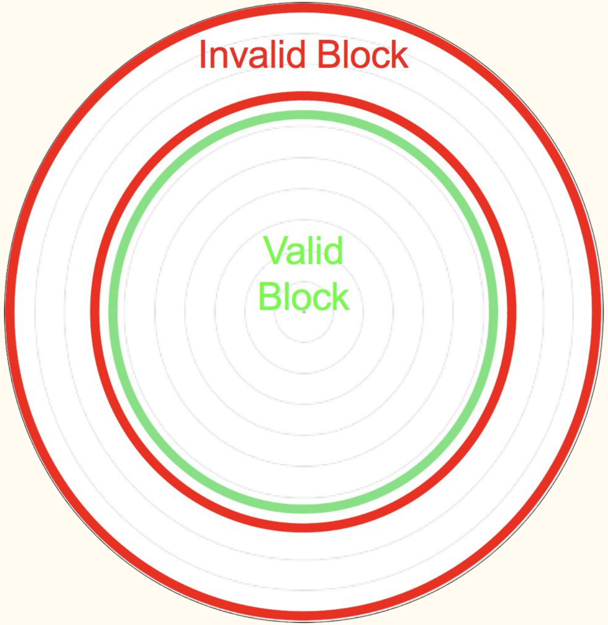
What a Miner Does

1. Download the entire chain to store the entire transaction history
2. Verify incoming transactions
3. Create a block using collected valid transactions
4. Find a valid nonce to create a valid block header (POW)
5. Hope that your block is accepted by other nodes and not defeated by a competitor block

Side Note - ASIC Miners

- Application Specific Integrated Circuits
- Used by most Bitcoin Mining farms
- Typically leads to centralization
- Memory bound functions are used to counteract ASIC usage

Block Difficulty



- Mining is like throwing darts at a target while blindfolded
  - Equal likelihood of hitting ANY ring
  - Faster throws results in more hits per second
  - The target is within the green ring
- Difficulty inversely proportional to green ring size
  - Green ring adjusts depending on average time to produce valid results
- If people get better at throwing darts, the green circle needs to get smaller

$$H(nonce \mid\mid prev\_hash \mid\mid merkle\_root) < target$$

POW - Puzzle

$$H(nonce \;||\; prev\_hash \;||\; merkle\_root) < target$$

1. Computationally difficult
2. Parameterizable (variable) cost
    a. Allows for adjustments with global hashrate increases
3. Easily Verifiable
    a. Should not be a need for a central authority to verify nonce validity; instead other miners can rehash the nonce to verify validity

Block Creation

- Miners select TX’s from mempool to form new block
  - https://etherscan.io/txsPending
- Plus one coinbase transaction (contains the block reward) to their address
- For a block to be accepted by the network, it need to contain only valid transactions: that means inputs that aren’t spent, inputs that have a valid amount, valid signatures etc.