Project Ideas

- Survey of consensus algorithms or a detailed study of one most recently developed algorithm (easy)
- Study of the most recent development of blockchain technology or a detailed analysis of one real application widely used in industry (easy)
- Information security related issues in cryptocurrencies (mild)
- Simulation of bitcoin blockchain mining process (hard: requires Java programming)
- Smart contract application (hard: requires programming)

Complete Mining Algorithm

- Each miner (full node) keeps a complete set of tries including state trie, transaction trie, receipt trie, and storage trie locally.
- Each miner listens to the broadcast of transactions and blocks information and relays the information around.
- For each transaction included in a block (either the new block the miner is working on or the most recent blocks just received from the network), the miner verifies (executes) the transaction.
- Each transaction consumes gas, the fees collected from executing the transaction go to the miner. The transfer amount and the fees will be deducted from the transaction sender’s account. And the accounts of the transaction receivers and miner will be credited with appropriate amount.
- The miner then computes the hash values of all roots. If the block is received from the network, the miner asserts that the hash values match.
- If the block is the new block (not from network), the miner find a proper nonce to adjust the block hash to meet the preset difficult level, and then broadcasts the block ASAP.

Questions Related to Mining Algorithm

- Will the block contain a complete set of tries including state trie, transaction trie, receipt trie, and storage trie?
- Can a miner ignore block verification (execution of transactions)?
- What if many miners ignore block verification?
- What if there are conflicting transactions in the block being worked on and the received block?
- Does it make sense to keep working on the current block even there is a new block received?