CSCI181AF: Advanced Data Structures
09/07/2022

Writeup HW #5

Applied Hash Functions Writeup

1. To combat DoS attacks, PEP wants to transition to a cryptographic hash function, from which they have decided that SipHash provides the best balance of speed and security and can be optimized and updated to perfom as fast as original hash function.

2. When building a cryptocurrency, we want to use a cryptographic hash function that is collision-resistent, hiding and binding and puzzle friendly, hash pointers of the data in each block, unique digital signatures, and public keys that represent an identity in our system.

3. Bitcoin is a peer-to-peer network, uses no real world identities, and relies on distributed consesus on the validity of blocks added to blockchain and valuation of coins, on miners who produce new blocks with incentive bitcoins, and on trust of the cryptocurrency.

4. Bitcoin ledgers track transactions and use Bitcoin scripts to verify transactions. Transactions are flooded to all peer nodes when heard. The blockchain is a linked list of Merkle trees for each ledger. Bitcoin is limited by transaction rates and crytographic hash function.

5. (Note, only the actually words were counted here for total number of works [e.g. not numbers or currency]).

   I looked at block 757,248 which accounted for 7,363.7 BTC output in transactions and approximately 147,000,000 USD in transactions. The miner was "SlushPool". The average transaction was $188,859 with the max input being 4172.66620739 BTC or approximately $83,000,000, and the min input transaction being 0.00001246 BTC or $0.24. The max accounted for 57% of total.