The Institution of Engineering and Technology

VIT
Vellore Institute of Technology
(Deemed to be University under section 3 of the UGC Act, 1956)

PERSISTENCE PROBLEM STATEMENENT

Problem Statements:

Front-Running prevention: In a maker-taker market, ***Front-Running*** is a prohibited practice where an observer of the order book submits a slightly better bid/offer than the trade already placed in the order book, driving up the price of the order and hence making profit. In Blockchain applications, the problem is especially prevalent where the mem-pool of all transaction is publicly visible and an observer can replicate the transactions present in the mem-pool albeit, with a higher gas price to get their transaction executed before the transactions are already present in the mem-pool.
Statement: Given a signed transaction is already present in the mem-pool of transaction, devise a strategy such that, the oldest transaction is always executed before the newer transactions(for buy/sell of the same entity).

Gaming: Turn based adversarial games requires to know the move of the opponent and hence the strategy of the opponent is hidden from the other player till the other player's move is executed/committed.
Statement: Design a blockchain based game where the opponents cannot preempt the moves of the other adversary until the move is irreversibly committed on the state of the Blockchain.

Oracle system: Many applications on blockchain can benefit from recording events that originate outside the state of the Blockchain but lack a mechanism to import the information without introducing centralised forms of failures.
Statement: Design an oracle system on blockchain where Oracle actors independently observe and record data from events outside the state of the Blockchain and the system corroborates this data to commit it to the blockchain state, avoiding centralisation/collusion.

Digital assets and rights management and exchange: Digital assets and rights are notoriously difficult to maintain and exchange because of replication, sharing and hacking. For example, a video game access key, a Netflix account, rights to stream a movie in a theater are all meant for single owner but it can be replicated or access shared or hacked away.
Statement: Design a digital access and rights management system on blockchain where any application can verify the current singular ownership of the asset, allowing exchange and preventing replication.

Identity: Each application maintains their own KYC with their customers and a lot of effort is spent or reconciliation of data between the applications or the customers having to repeat the same process across applications.
Statement: Design an identity management system on blockchain, like OAuth, which singularly saimatins unique identity of individuals which can be verified by applications without exposing this information on the public state of the blockchain application.