the of

1:A. A major challenge in design a lottery protocol is generating randomness which isn't possible in a blockchain. We overcome this by asking the players to generate random strings (s_1, s_2 & s_3) & then awarding the player who came in ($s_1 + s_2 + s_3$ i.3) time.

By using strings from all 3 players we've ensured that the only way to influence the answer, final winner is if all 3 players are collaborating which is non-profitable for them.

The protocol can be described as:

1. ROUND 0: Internal computing done by the players.
2. ROUND 1: Initial commitment.
3. ROUND 2: Verification
4. Reveal / Timeout

Let the players be A, B & C and their random strings be s_1, s_2 & s_3 respectively.

The contract constructor sets the bet amount, fair play penalty & starts the expiration timer with the no. of minutes provided.

Smart Contract

This is how our contract will operate.

Round 0: 0. Contract is deployed & its values set.
1. Each player will locally generate their own random strings.
2. They will hash the strings & store both as s_n & $H(s_n)$

Round 1:
3. Players must provide their hashes as commitments before the time expires.
   a. If the time expires then anyone can invoke a timeout function which will refund their money.
4. Once all players have committed, Round 1 ends.

Round 2:
5. All players must provide their original strings which are hashed & checked against their commitments.
   a. If a player provides the wrong string or provides nothing then the timeout function can be invoked. The contract balance will be split between the honest players & and

nothing will be refunded to the cheater as a penalty.

6. Once all three strings have been verified, round 2 ends.

REVEAL:

7. After round 2 is over, the reveal function is invoked which awards all the betting money to the winner who has the index of $[(s_1 + s_2 + s_3) \% 3]$, the rest of the the 2 players get their fair play penalty money back.

B: ABOLUTE:

Abzolute fairness is the fairness of info-rmation i.e. that at any given moment each player is exactly equally aware & unaware of the result. This is impossible in a lottery proto-col as it requires every step to happen spontaneously for every player.

PENALTY:

Penalty based fairness is where cheating is actively penalized & rehile honesty is incentivized. For a lottery protocol this denotes into monetary penalties & incentives.

C: I: My protocol is not absolutely fair as a player can see the strings of other players in Round 2 even if he hasn't shown his own. Therefore, he can find out if he will be the winner or not even though the other two can't.

II: My protocol is penalty based fair as a cheater will lose their fair play money if they cheat whereas they would receive it back even if they lose honestly. Therefore, it is better monetarily to be honest & lose instead of cheating i.e. honesty is ~~~~ incentivised while cheating is penalized.

D: A 3-party lottery protocol which utilizes direct communication instead is not viable as it requires a trustable 4th party to handle the money which is impossible. For example, if player C is made the banker & it turns out at the end that B has won then C can simply refuse to turn over the money. Any protocol which tries to operate through direct communication will inevitably as there is no trust & no way to enforce penalties to dissuade cheaters. Even if you use a system in which each players keeps the others in check, players can team up to cheat. The need for a trustable authority is why blockchains & smart contracts are such powerful tools.