Lotteries on Bitcoin :

Procédure pour 2 joueurs A et B

1 - A et B génèrent leurs secrets + signatures

2 - A envoie clé publique + hash secret à B

3 - B envoie clé publique + hash secret à A

Init1 : signature + mise envoyée

Init2 : Si entrée init1 alors envoie sur la blockchain

Win : Si les mises ont été envoyé sur la blockchain alors on créer la première partie entre A et B

Match et Match 2 : Match entre A et B, on vérifie que les secrets correspondent bien

Winner : On définit que A gagne

Winner

Match2

Match

Win

InitBC

Créer\_secret

Créer\_pk

Init2

Init1