IP-based Wallet grouping service for BAT

Question 3)
I describe thereafter an approach based on asymmetrical cryptography. Although we will not store neither the IP nor the hash of the IP, the inducted computational costs will be much bigger.

Process:

- When wallet_id is being connected with an IP, we use a deterministic (chosen in advanced) algorithm to derivate a keypair from this IP
- The wallet_id is signed using the generated private key
- (wallet_id, signature) is stored in the database
- Using the public key, we try to match it to the existing signatures of the tuple (wallet_id, signature) currently stored in the database. If there is a match, we group the wallet_id together
- The public and private keys generated as well as the IP of the user can be dumped at this point

Note:

- When studying the identification of fraudulent users, we could also think about behavior analysis (detecting some defined recognizable sequence of actions that they would do).
- Finally, there is the possibility of extracting other information from the device (universally unique identifier, mac address, etc). We should still hash these data for privacy purposes. Nevertheless, collecting them would also be more intrusive for the user/ might require more permission as well.

Question 4)
False negatives: One fraudster could easily change its IP (i.e. using proxy and VPNs), and therefore not being flagged as such.

False positives: Legitimate users could have the same IP because they are behind the same NAT (especially in public & crowded places), yet they are on different devices and honest.

Because of these possible situations, it would be complicated to identify a threshold for the right number of users per IP. We would have to collect additional data to tackle this issue (such as the ones quoted earlier for example). An internal reputation system for these ids could be designed to evaluate the probability of one user to be fraudulent, based on our parameters/analysis.