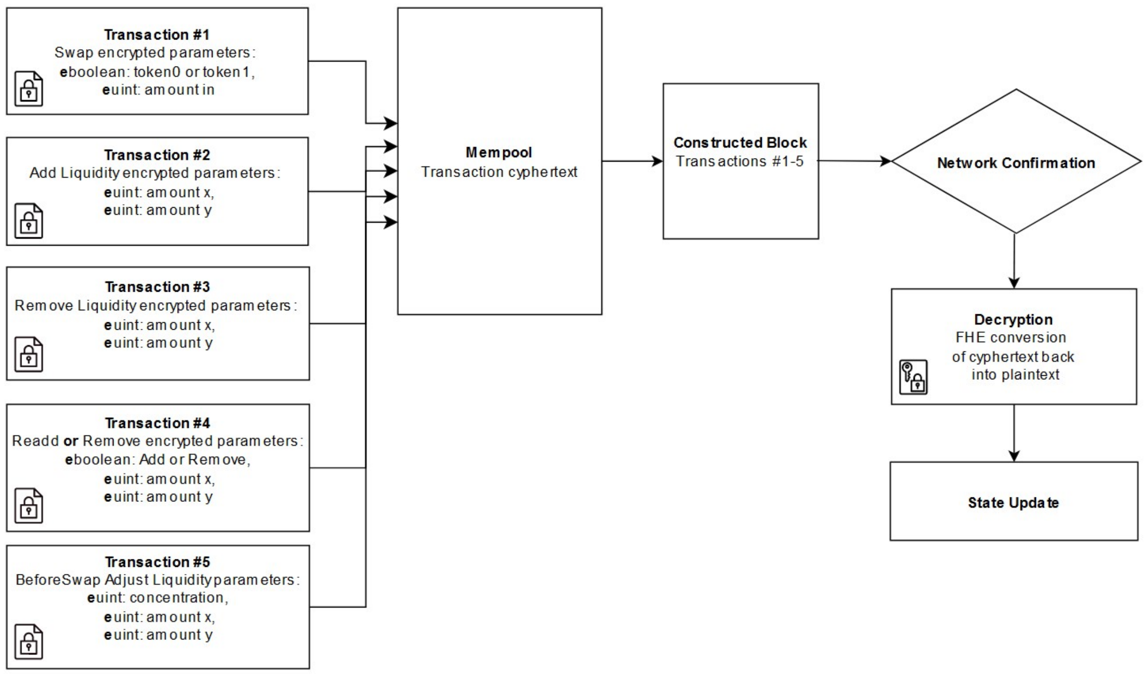


**Figure 1.** Variables for AMM interaction are obfuscated before entering the mempool. After network confirmation the cyphertext is converted back to plaintext.

Combine the obfuscation of an encrypted unsigned integer *euint* in Fully Homomorphic Encryption (FHE) with the following game theory. A MEV extractor aims to maximize compounding returns which can be expressed with the Kelly criterion as:

$$f^* = p - \frac{1-p}{b} \tag{1}$$

where $f^*$ represents a MEV extractor's portfolio allocation in a MEV attack with the probability of success $p$ and betting odds $b$. By aiming for Kelly-neutrality we set a MEV extractor's Kelly betting amount $f^* = 0$ rearranging for the following equality to hold:

$$p = \frac{1-p}{b}. \tag{2}$$

By introducing two encrypted boolean values for swapping or for providing liquidity $B_{swap} = [0, 1], B_{LP} = [0, 1]$. Is the LP removing ($B_{LP} = 0$) or re-adding ($B_{LP} = 1$) liquidity? Is the swapper exchanging USDC for ETH ($B_{swap} = 0$) or exchanging ETH for USDC ($B_{swap} = 1$)? We can also encrypt as euints the quantity of the swap amount $dx$ thereby making it unclear of the size of the betting odds $b$. Where the odds for a MEV extractor can be expressed in terms of gain $G$ and the cost $L$ of attempting to re-arrange or decrypt a transaction.

$$E\langle B_{swap}\rangle = \frac{1 - E\langle B_{swap}\rangle}{\frac{E\langle G\rangle}{E\langle L\rangle}} \quad , \quad E\langle B_{LP}\rangle = \frac{1 - E\langle B_{LP}\rangle}{\frac{E\langle G\rangle}{E\langle L\rangle}} \tag{3}$$

$$0.5 = \frac{1 - 0.5}{\frac{U_{[0,\infty)}}{U_{[0,\infty)}}} = \frac{0.5}{1} \tag{4}$$

Setting the expected value of a MEV extractor's Kelly bet $E\langle f^*\rangle = 0$. The drawback of this approach being high gas cost for FHE encryption and decryption.