So if I understand it correctly, private transactions have proofs created locally and then are submitted to the sequencer - but for the sequencer to update the state, it must have a way of learning what the transaction is no?

SO on aztec is the privacy limited to at most the sequencer knowing what my transaction is?

If not, and the sequencer does not see individual transactions, at the least it should now the state change right?

Could it then not infer qualities about the included transactions from this state change and thus reduce privacy?

i.e. only one tx affecting “uniswapETHUSDpool” contract, would reveal info?