

From a theoretical and layman's terms perspective (I do not have a background in cryptography or coding), I was hoping I could receive answers to a few questions regarding Guy's recent comments on MPC and the future path of Enigma. I was told this is the best place to ask.

1. The whitepaper makes a compelling case for MPC providing privacy and scalability to blockchains. Theoretically, the act of sharding data and sending discrete pieces to nodes, within the construct of a protocol that can create computation results from the aggregation of those nodes, makes sense as a way to increase speed, scalability and privacy. Guy recently said that TEE can produce results in 40 seconds that MPC takes 40 hours to perform. This order of magnitude discrepancy leads me to think MPC has a flaw that was previously unknown. Is that the case and, if so, can you please elaborate.
2. If, for technical reasons, TEE is the best solution, what is Enigma's proprietary edge? How are you different than iExec or Oasis Labs?
3. Is the reason for the pivot to focusing on adoption near term because the answer to the second question is a lack of edge? I fully support the team and believe in your expertise in the field, but I find it disconcerting when the original tech has been diminished and adoption prioritized. Is this a push for first-mover advantage because of a lack of differentiation?

I apologize in advance if these questions come off as aggressive or accusatory; especially given my lack of technical background. However, as an investor from the beginning and someone who truly is passionate about a decentralized future, I would hope you understand my concerns.