In the most recent All Core Devs call@vbuterin again proposed that we use Kate Commitments when committing to contract code. They've been mentioned a few times before, starting a thread to centralize the discussion of whether we want to use them.

In stateless ethereum miners will need to add proofs for all executed code to the witness. Currently our proof sizes are linear in the size of the code, we must include the entire code segment. Our plan is code merkelization, which will give us proofs which grow logarithmically with the size of the contract code; @sinamahmoodi and others have done a lot of work in that direction.

Kate commitments go further; they promise constant sized proofs. The witness for a contract's code will need to include the executed code chunks along with a single group element (~48 bytes), this is almost no overhead at all! Given that witness size is a key factor in whether stateless ethereum is possible at all this makes Kate commitments seem quite appealing.

It has a big drawback:

- It requires a trusted setup. As far as I can tell we will only need to run the trusted setup once, we can reuse the group it generates for each commitment.

To start things off, I think there are some open questions:

- How large are code merkle proofs, by how much would moving to Kate commitments reduce witness sizes?
- How much time does it take to create a commitment, create a proof, or verify a proof? I think these are relatively fast, but if this adds an additional second to block processing that's likely not tenable.
- Has someone (Aztec?) already gone through a trusted setup, that we might use the group they're using?
- What does running our own trusted setup require? We will have to pick an MPC protocol, write multiple independent implementations of the setup client, then advertise it and ask many people to run it. How much will this work delay stateless ethereum?
- I can't tell for sure, but it seems that Kate commitments are not quantum-secure. Do we want to build a system which we'll need to replace with something else in 5-10 years.