Meanwhile proposing different ways to commit to state has been a hot topic lately (RSA accumulators, Sparse Merkle tree, etc), I came across this paper that proposes doing so using algebraic vector commitments that I think may be worth discussing.

The crux of the paper is that if you commit to the state using algebraic vector commitments, and you want to achieve stateless validation, then you can make it possible for Alice to send money to Bob, and only provide the proof of Alice's balance. With a Merkle tree, you'd also need to provide proof of Bob's balance. This may be nice, because that means everyone one needs to store their own state; Alice doesn't need to know Bob's state. However, it appears to require a trusted setup.

Here's the crux of it: