The soundest sleepers are those who have the least issue trusting someone to hold their seed for them, but this is backwards and untenable and not a foundation for individuals or institutions to build on. While this sounds contrary to what seems to be the majority of bitcoin users, I'll argue that institutions that fail to take custody seriously will not only fail first, but also the most severely, as well as having the potential to take down their industry and/or a portion of the financial system with them.

Holding bitcoin in self-custody is not like holding fiat for a simple reason. The likelihood of a mistake that makes the bitcoin unspendable is much higher, and there is no bailout possible. Imagine this scenario: The year is 2030. BlackRock's IBIT ETF has acquired 2 million bitcoin on behalf of its users, and by then, bitcoin reaches gold's market capitalization of $20 trillion. That's about $1M a bitcoin. Humor me in this scenario, as bitcoin's path to today is far stranger. BlackRock's ETF would represent 10% of that value, or $2 trillion. That's $2 trillion of value on balance sheets of companies all over the world. Imagine we get to 2030 and discover that BlackRock cannot sell back that bitcoin because its custodian cannot perform the signatures required to move the keys. BlackRock loses $2 trillion, and all of their customers have to write down 100% of that value on their balance sheets. *Poof*. Cryptography is ruthless in this way, and there are two types of people in the world — those who have been burned and those who have yet to be.