Proof of Solvency is a Big Deal

Leave it to programmers to look at a catastrophic $350M financial-company collapse, and immediately think:

“Why not just code that sort of inelegance out of the economy?”

That’s exactly what’s happening in response to the recent implosion of early bitcoin-exchange MtGox. On the day MtGox filed for bankruptcy protection, CoinSetter, a bitcoin trading-market startup based in NYC, began a public process to determine how to do cryptographic proof-o--solvency.

This idea has profound implications for all financial institutions. Cryptographic proof of solvency refers to a way to publicly **prove**, beyond any possible doubt, that an organization’s finances are in order. The idea is essentially to link all deposits/liabilities of an organization and use cryptography to prove that they sum to a certain amount. The company can then use the public bitcoin blockchain to provably demonstrate control of at least that quantity of funds. Critically, this proof would not rely on the company’s own statements, or statements by its auditors, but on cryptography; in other words, the laws of mathematics. As we’ve seen so many times before (Enron, Worldcom, MFGlobal, Madoff), it’s probably not a good idea to unilaterally trust what companies, or their auditors, say.

Bitcoin gives the world completely new financial possibilities through the combination of the Blockchain (bitcoin’s public ledger) and cryptography. Proof-of-solvency is just the obvious first-step in giving financial companies the ability to provide customers with unprecedented transparency and control of funds. This has very large potential benefits to society, given the financial-system costs associated with insurance, fraud prevention, auditing, etc. Not to mention multi-trillion dollar public bailouts when those measures fail to be enough anyway.
