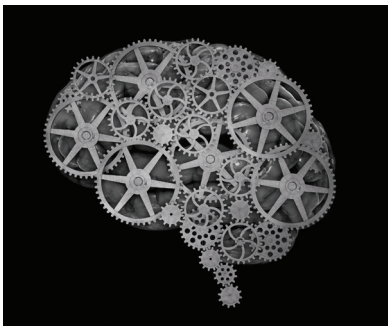

All That Glitters Is Not Gold

David Alan Grier, *George Washington University*

Just because a new algorithm solves one kind of problem doesn't mean that it can solve them all.

Be careful with your predictions about the future: it's a vengeful little beast and not to be trusted. Once you've made any prediction about the way things will be this year, next year, or even a decade from now, the future will find the weakness in your ideas. It will snatch any value you once claimed for your work and compel you to admit that your ideas weren't to have been trusted in the first place.

Dylan got exposed by the future earlier this month. In the midst of telling me about a new job, new skills, and a new city, she mentioned that she had become fascinated with Bitcoin. A real "game changer," she called it. She especially liked Blockchain, the ledger that tracked all Bitcoin transactions. That vision became fodder for the future, when the Bitcoin exchange Mt. Gox announced that it had been drained of its assets. Apparently, the game-changing algorithm wasn't as trustworthy as some had claimed, and it allowed an attacker to compel the Mt. Gox system to trust false transactions.

The problem of trust, of course, is the problem that Bitcoin's founder(s) were attempting to solve. Many commentators have suggested that Bitcoin was created to launder money or to create a form of currency beyond the control of nation-states, but the founding document makes no such claims. Instead, this document argued that the technology was created to correct the "inherent weaknesses of the trust-based model." Bitcoin algorithms would replace the various mechanisms that we've used throughout human history to compel people to complete transactions. Indeed, "transactions that are computationally impractical to reverse," explained the Bitcoin paper, "would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers."

When I raised Mt. Gox's failure with Dylan, she dismissed it with an excuse commonly invoked by Bitcoin's defenders. Mt. Gox, she claimed, "didn't properly implement the Bitcoin model" and the problem would eventually be fixed. This argument is true as far as it goes, but it doesn't address the bigger issue that hangs over Bitcoin: it was designed to solve a fairly narrow set of problems. It might not solve other problems that can be found in financial systems. In fact, it could actually exacerbate some.

As important as the trust between buyer and seller may be, it's only one of the problems that can beset a financial system. Speculators can manipulate markets. Thieves can defraud buyers, sellers, or both. Governments can inflate or deflate currencies to achieve their ends. Bitcoin may or may not be able to solve these issues, but it was never designed for such ends. At the moment, it can't even protect the assets of its own exchanges.

The age of information has generally been a period of tempered expectations. We create a technology to solve a specific problem and then transfer its benefits to a host of other issues. The glittering richness of our own work can be just a little too tempting. The free flow of information over the Internet has generally been good, but it doesn't always protect us from those who wish us ill. The transparency of governments has made it harder for central institutions to defraud their citizens, but it hasn't always made government offices more efficient. Electronic payment systems, such as Bitcoin, might reduce the cost of business transactions, but they shouldn't be expected to solve all our economic woes.

David Alan Grier *is the author of* The Company We Keep *(IEEE CS Press, 2013). His video podcasts can be found at video.dagrier.net.*

Published by the IEEE Computer Society