SOCIETY OF ACTUARIES

Investment Section

INVESTMENT FALLACIES 2014

Bitcoin Fallacies

by Larry Zhao

As an investment professional, we have learned many fallacies such as "Sell in May and go away." The question is how we do with these fallacies we know about, in particular, how we apply the knowledge to new concepts, new situations, and new investments.

Introduced by the pseudonymous developer Satoish Nakamoto a few years ago, Bitcoin has brought with it excitement, drama, myths, and fallacies. Some people take it as a déjà vu of the Tulipmania that struck the Dutch in 1636. Some view it as another Ponzi scheme. A prominent economist and Nobel Prize laureate simply called it evil.

What is Bitcoin?

Bitcoin is the first decentralized digital currency designed to facilitate transactions between two parties over a peer-to-peer global network. First and foremost, it is a new technology – a black swan technology that grows out of decades of research in computer security and cryptography by tens of thousands of researchers and scientists globally. Bitcoin is potentially disruptive – just as Google has disrupted the traditional retrieval and catalog system, Bitcoin might seriously challenge the status quo of the current credit/debit and banking system and international remittance markets, because Bitcoin has removed the middle-men facilitating transactions.

How Bitcoin works?

As a payment system running on open-source software, Bitcoin secures transactions using asymmetric key cryptography, which requires a public key and a private key. The public key is distributed widely (i.e., QR codes) while the private key should be kept secret all the time. A secure transaction is done this way: 1) a sender encrypts a payment using the recipient's public key and broadcasts to the Bitcoin network; 2) the payment cannot be decrypted by anyone without the recipient's private key; 3) before the payment is sent, a signature is also created with the sender's private key and the signature can be verified by the recipient using the sender's public key – any tempering of the payment during transition will result in mismatch of the signature.

What are the benefits?

With no third-party intermediary, the cost is zero or near-zero. With no authority to approve, the transaction can be done in minutes between peers at any corners of the globe. Because it is computationally impossible to recover the private key from the encryption, the transaction is secure. Because neither the sender's nor the recipient's information is transmitted, the transaction is free of identity-fraud.

Bitcoin fallacies

Is *Bitcoin* another *Tulipmania* bubble waiting to burst? This is a legitimate question even if the original narrative of Tulipmania was historically inaccurate. After all, unlike gold, Bitcoin has no intrinsic value; and unlike fiat money, there is no backing up central authority. The fact that Bitcoin has limited supply (21 million) does not guarantee the value of Bitcoin in the future because the demand could drop sharply if everyone suddenly loses confidence and stops using it due to unpredictable events. Theoretically its value could drop to zero, like any currency of dissolved states in history. However, Bitcoin derives its value not from the role of digital currency but rather from its *utility* – the usefulness of the Bitcoin system to provide fast, low-or-no-fee, secure, peer-to-peer transactions, and the speculation on future use of the system. As more and more consumers and merchants are using and accepting bitcoins daily and globally, and as more and more Bitcoin tools and technologies are created and improved, it will create a positive feedback-loop and an expanding ecological system, just like elevators, tele-

phones, or Internet. You might see flash crashes occasionally, but Bitcoin more likely than not can survive on the basis of being used entirely as an e-payment system.

Is Bitcoin the dream tool for drug dealers, money launderers, and terrorists to transfer money anonymously without impunity?

No, this is a fallacy. Bitcoin is pseudonymous, not anonymous. Every transaction in the Bitcoin network is tracked and logged permanently, available for any one to see (http://blockchain.info). Bitcoin is significantly easier for law enforcement to trace than cash or gold. Criminals and thugs will continue to use the best tools and technology available no matter what. For migrant workers who go to work in hard jobs in foreign countries, Bitcoin offers a far better alternative than paying 10% or higher fees in order to send money back to their families.

Is Bitcoin a Ponzi scheme?

A Ponzi scheme is a zero sum game – early investors can only profit at the expense of late investors. Bitcoin, however, could have win-win outcomes where early investors profit from the rise in value and late investors benefit from an e-cash system that is inexpensive, fast, flexible and globally accepted. The fact that early investors benefit more does not necessarily make Bitcoin a Ponzi scheme. All good investments in successful companies have this quality. Secondly, Bitcoin does not promise a higher return to maintain a continual stream of investment. Investment continually flows in as people gradually realize its value and potential as they use bitcoins in transactions during everyday life.

Is Bitcoin evil?

Paul Krugman dislikes Bitcoin because of its inherent Libertarian political agenda – to undermine the ability of governments to collect taxes and monitor financial transactions among their citizens. The wonderful features of Bitcoin as a payment system, in his opinion, are simply positive economics – how things work; but on the normative economics level – how things should be – Bitcoin fails, and on this very basis he thinks Bitcoin is evil. As always, Krugman is insightful, because he looks beyond Bitcoin as a payment system but as an idea – a dangerous idea, because no one government can shut it down. What governments and regulators can do is impede its progress and innovation. Bitcoin is a discovery, similar to the discovery of fission, based on which nuclear reactors are built and electricity is generated. Most people focus on the pros and cons of nuclear reactors, or the price and use of electricity, while missing the point that fission in itself changes physics, changes energy, changes worldviews, changes everything. Government can regulate Bitcoin, but cannot make the discovery disappear.

Should you invest in Bitcoin?

Make no mistake. Debunking the fallacies is to offer a balanced view, but not to encourage anyone to invest in Bitcoin unless you truly understand the risks and rewards.

Price volatility is a major impediment to Bitcoin's wide adoption as a viable payment system. Bloomberg data shows that, since inception, the annualized volatility of bitcoin returns in US dollars is about 150%, about 10 times of the S&P 500 index, while the annualized return is about 350%, about 40 times of the S&P 500 index. Its momentum to maintain high future annualized returns is questionable.

But over long term, it behaves like a special asset class with a binary pay-off: it can worth quite a lot or almost nothing.

One investment strategy is to use it as a "tail risk hedge", where a small position invested early on can still offer a substantial return over many years, or lose very little should Bitcoin die or be usurped.

I invest precisely what I can lose 100% of the investment.

The operational risk, however, cannot be underestimated. Misplacing the private key can result in the entire loss of your bitcoins, which cannot be replaced by any organization. Internet hacks, security breaches and counterparty risk at Bitcoin exchanges such as MtGox and BitStamp are perennial headaches to investors.

Larry Zhao, FSA, CERA, CFA, FRM, PhD, is an associate vice president at Nationwide Financial. He can be reached at zhaol1@nationwide.com

The thoughts and insights shared herein are not necessarily those of the Society of Actuaries, the Investment section of the Society of Actuaries, or corresponding employers of the authors.