

Popping the Bitcoin Bubble Releases Ethereum

Prof. Michael R. King, co-Director, Scotiabank Digital Banking Lab at Ivey Business School, Western University

January 31, 2018

Cryptocurrency skeptics will be rejoicing at the popping of the Bitcoin bubble, with the electronic money dropping from US\$20,000 per bitcoin (BTC) in mid-December to around half this amount by mid-January. Despite being caught up in the sell-off, I believe the second largest cryptocurrency, Ethereum, will rise out of the ashes because it offers something socially valuable and potentially game-changing.

Ethereum is the brainchild of Russian-Canadian programmer Vitalik Buterin, who dropped out of University of Waterloo in mid-2013 to focus full-time on Bitcoin. Later that year, this 19-year old came up with the idea for Ethereum, which he saw as an evolution that addressed the shortcomings of Bitcoin. In 2014, Buterin received the means to pursue his vision when he was chosen for a Thiel fellowship – a \$100,000 two-year award offered by PayPal founder and tech billionaire, Peter Thiel. Buterin relocated to Zug, Switzerland, an area known as Crypto Valley due to its ecosystem of blockchain and cryptographic start-ups. Buterin then raised US\$15 million in crowdfunding to hire coders and fund development, with core developers Gavin Wood and Jeffrey Wilcke.



The Ethereum Project has a mission everyone can support: to provide an open and secure platform for developers to build decentralized applications (or “dapps”) on the internet.¹ Ethereum provides a free platform to build similar dapps that Buterin claims will reduce costs, remove points of failure, prevent censorship, and ensure transparency and trust among

all the parties to a transaction without the need for an intermediary.

The Ethereum platform is built on an open-source, public blockchain that includes its own programming language and a messaging function. The blockchain provides the security. Ethereum’s programming language Solidity is Turing-complete, meaning coders can build whatever application they can imagine. Most significantly, Ethereum can support smart contracts, which are programs that execute a series of transactions after some pre-specified event.² A smart contract, for example, may transfer money to a vendor after receiving confirmation of delivery of a product.

Smart contracts can be used to create a virtual, electronic company, called a decentralized autonomous organization (or “DAO”). The early press for this concept was unfortunately negative after an early DAO launched in mid-2016 by the German company Slock.it was hacked and had one third of the US\$150 million in crowdfunding siphoned off. The security flaw lay in the design of this specific DAO, not the Ethereum platform. While the funds were recovered, the incident led to negative press that still lingers.

¹ See: <https://www.ethereum.org/>

² See: <https://www.ethereum.org/greeter>

As suggested in an open letter written by Chain CEO Adam Ludwin, we should all stop using the term *cryptocurrencies*, because it carries too much baggage.³ Instead, we should talk about *cryptoassets* or digital tokens that are designed to run decentralized applications. One example of such a token is the PokéCoin, a currency used for in-game purchases in the Pokémon Go game. Want to find Pikachu faster? Then pay up. But who would ever think to speculate on the value of PokéCoin?

Ethereum's token is called *ether* and it serves two functions. First, it is used to charge users for running applications on the Ethereum platform. While coding and hosting a decentralized application is free, running a program has a cost related to the complexity and computational power required. Much like running your car, Ethereum runs on 'gas', which is a virtual form of fuel priced in ether. If you want to run programs on Ethereum, you need to buy gas. This cost ensures developers write efficient applications that conserve gas and keep the network healthy. So ether is the crypto-fuel used to run decentralized applications.

Second, ether are used to reward miners who validate transactions. Similar to bitcoin, ether is currently mined using a proof-of-work algorithm by miners who solve a cryptographic problem to verify transactions and claim the reward. A new ether block is created every 12-15 seconds, with miners receiving 5 ether per block. Ethereum can process around 15 transactions per second with settlement time of 2 to 5 minutes and an average cost of \$1 to \$2 per transaction. This is faster than Bitcoin but much slower than VISA, which can process up to 50,000 transactions per second. Ethereum miners choose which transactions to confirm based on the amount of gas offered, so ether provides an incentive for miners to verify and secure transactions on the Ethereum blockchain.

Mining bitcoin and ether consume a lot of electricity, which is bad for the environment and society.⁴ Recognizing this, in the next year or two Ethereum will move to a new way to verify transactions called proof-of-stake. Miners (who will be called "validators") must deposit ether into an escrow account and are randomly selected to verify transactions in proportion to the amount of ether on deposit (thus the term "stake"). This process will be more energy efficient than proof-of-work and better for the planet.

Given the attractive features of the Ethereum platform, many business consortiums and even central banks are experimenting with it. In 2016, the Bank of Canada collaborated with the private sector to test how a distributed ledger technology could transform the wholesale payments system.⁵ Codenamed Project Jasper, the parties built and tested a permissioned blockchain on the Ethereum platform. This pilot provided insights that may lead to the creation of a digital version of the Canadian dollar in the future.

Some readers may be wondering if it makes sense to invest in Ethereum's token ether? While Ethereum may be the most useful programmable blockchain out there, I would not recommend buying ether unless you plan to run an application on the platform. It would be like buying TTC tokens to the Toronto subway in the hopes that they would appreciate. While you may be able to use them to get a ride from Bay Street to Main Street, you won't be able to use them to pay for much else. But if you want to run a smart contract on Ethereum, you won't get far without ether.

³ See: <https://blog.chain.com/a-letter-to-jamie-dimon-de89d417cb80>

⁴ See: <https://digiconomist.net/bitcoin-energy-consumption>

⁵ See: <https://www.bankofcanada.ca/research/digital-currencies-and-fintech/fintech-experiments-and-projects/>