
Payden & Rygel
POINT of VIEW

FALL 2017

Our Perspective on Issues Affecting Global Financial Markets

BEYOND BITCOIN: THE DAWN OF “CRYPTOECONOMICS”

A few years ago we wrote about bitcoin. Since then, the price of a bitcoin soared to more than USD 4,500. But the media and many investors focus too much on bitcoin’s price, betraying little understanding of more fundamental institutional developments. We write to help catch investors up on “cryptoeconomics” and urge them not to dismiss bitcoin’s rise so easily.

Beyond bitcoin: The Dawn of “Cryptoeconomics”

If you’re holding on to your university economics textbook as reference material, toss it in the bin. It’s out of date. A new subfield of economics, *cryptoeconomics*, has emerged. So new is the burgeoning field that a query of Webster’s dictionary for “cryptoeconomics” returns: “The word you’ve entered isn’t in the dictionary.”

“Crypto-what?” you might be thinking. *Cryptoeconomics* refers to digital currencies like bitcoin that use a combination of cryptography and economic incentives to function instead of relying on a central authority. *Cryptoeconomics* may be a new term but, surely, you’ve heard of bitcoin before. A few years ago we wrote about the fledgling digital currency (see “Bitcoin: The Future of Money,” January-February 2014)¹. Since then, the price of a bitcoin soared to more than USD 4,500 in September 2017, attracting plenty of media and investor attention alike.

For example, Charlie Munger said of bitcoin, “I think it’s rat poison. I regard it as deeply flakey.”² JPMorgan’s CEO Jamie Dimon opined,

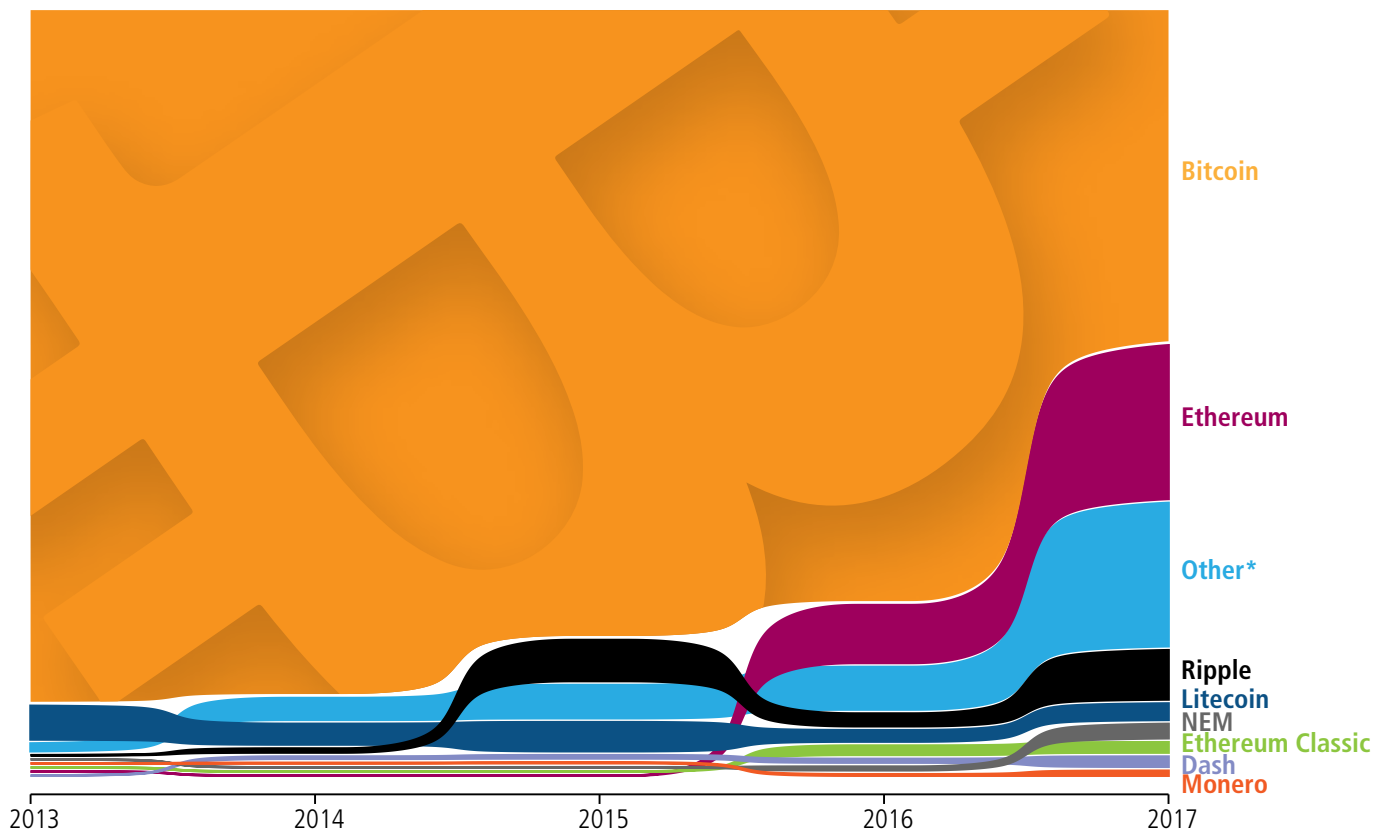
“It’s worse than tulip bulbs. It won’t end well. Someone is going to get killed.”³ Howard Marks wrote: “But they’re not real!”⁴ Robert Shiller, the Nobel Prize-winning economist famous for writing a book on financial bubbles, said, “The best example [of a bubble] right now is bitcoin.”⁵

We think almost everyone is wrong about bitcoin.

**«WE THINK ALMOST
EVERYONE IS WRONG
ABOUT BITCOIN.»**

We write to help catch investors up on “cryptoeconomics.” The birth of bitcoin marks the arrival of a novel economic institution—just like the emergence of nation-states, joint stock corporations, private clubs, or stock markets before it. Below, we’ll explore “cryptoeconomics” through a few classroom lessons using the example of bitcoin. Bit-

fig. 1 BEYOND BITCOIN: SHARE OF CRYPTOCURRENCY MARKET CAPITALIZATION



Source: Coinmarketcap.com, Payden Calculations

*Includes more than 800 different types of cryptocurrencies

coin is the first of what are now more than 900 cryptocurrencies, with a handful of others gaining share of the global cryptocurrency market capitalization of late (see Figure 1 on previous page).⁶

So, sit up, pay attention, class is in session.

LESSON #1: THE PROBLEM TO BE SOLVED

To start one must ask: “what is *the* problem bitcoin solved?”⁷ You have two main options when buying stuff: cash (from your pocket) or credit (from a trusted third party like Visa).

With cash, the merchant has an advantage: your shoeshine guy doesn’t care who you are, he only cares that the dollar bills you present aren’t fake. Once the cash changes hands, the transaction is complete.

Historically, many types of “difficult-to-counterfeit” objects served the same role in cash-like payments, including shells or gold coins. In the modern era, banknotes fit the bill (*ahem*). Again, either banknotes are made such that they are “difficult-to-counterfeit” and/or feature serial numbers so that a trusted third-party like a bank can verify their authenticity.⁸

But, buying stuff on the internet is more of a challenge. Cash payments? Impossible. And credit card online purchases present plenty of frictions, too. Often one needs to re-enter the card and cardholder information each time one makes a purchase. Worse, transaction fees are high and many people around the world don’t own credit cards.

These are the problems bitcoin sought to remedy. The world needed a way to make peer-to-peer, “cash-like” payments *online*. In 2008, the pseudonymous bitcoin creator Satoshi Nakamoto wrote in a paper detailing the idea behind bitcoin that, while “costs and payment uncertainties can be avoided in person by using physical currency...no mechanism exists to make payments over a communications channel without a trusted party.”⁹

Lesson: *the entire point of bitcoin* was to create a form of “digital cash” for use in *the digital world*.

LESSON #2: A CHAIN OF ENCRYPTED MESSAGES INSTEAD OF “BANKNOTES”

In the digital world, nothing seems scarce. Think about the digital items you own: such as music or pictures from your summer vacation. Think of how easily you can copy, paste, and send photos to grandmas and grandpas around the world.

Imagine, then, the challenge of creating “difficult-to-counterfeit” digital money! How can we guarantee that Alice hasn’t just “copy-pasted” her digital cash to send to Bob, much like she made a copy of her

favorite new Taylor Swift song? Where would the value be in such a currency?

Previous digital money attempts used a “mint”—a central institution that checked every transaction for authenticity. Think of it this way: if sending “digital cash” meant sending a picture of a dollar bill, there would need to be a single, central authority to check the serial numbers on the bills to make sure they weren’t spent elsewhere.

On the bitcoin network, when Alice sends Bob some value, she broadcasts to the entire network the transaction.¹⁰ And she doesn’t just send any message, using cryptography Alice can send a message to Bob that only Bob can unlock and only Alice can send. It’s an irrevocable message once it’s broadcast—just like a cash payment exchanging hands.

Who collects the messages?

The answer: *anyone* and *everyone*! All one needs to do is download the open source software and, voila, you’re a participant in a global network. But, more specifically, the group creating a running list of all transactions are called “miners.” Miners gather ALL the transactions and group them into “blocks” every 10 minutes. And this is very important, by gathering and verifying ALL transactions in the order the message are sent, the miners prevent Alice from sending money first to Bob and then sending the same money “copy-paste”-style to someone else.

What’s created is a single, “time-stamped,” agreed-upon list or “chain” that serves as “a single history of the order in which they were received.” In that way any user could track whether a sender had already spent “coins” elsewhere. The inclusion of transaction in chain of transactions that the majority of the network agrees upon is what makes the transaction “real.” “We define an electronic coin as a chain of digital signatures,” as Satoshi says. Digital scarcity is imposed by the list or chain of transactions through time.

«SO MUCH COMPUTING POWER IS DEDICATED TO THE NETWORK THAT IF WE LINED UP THE WORLD’S TOP 500 SUPERCOMPUTERS AND DEVOTED THEM TO BITCOIN MINING, THEY WOULD ADD UP TO LESS THAN 0.001% OF THE NETWORK COMPUTING POWER!»

Lesson: In bitcoin, instead of “difficult-to-counterfeit” coins or cash, we have a chain of “impossible-to-fake” encrypted messages transferring value from Alice to Bob.

LESSON #3: SHOW YOUR WORK, PROVE YOUR WORTH

You might wonder: couldn't a miner just add new transactions to the list or alter older transactions? In theory, yes! Fortunately, the author of bitcoin adopted a novel way of dealing with such a problem.

Bitcoin requires that each miner solve a “proof of work” puzzle to participate in the adding of blocks of transactions. In short, the puzzle requires nodes to “guess” at a certain number, and devote computing resources to making the guesses. The difficulty of solving that puzzle adjusts based on network transaction volume. The more computing resources devoted to the problems, the more guesses per second, or “hashes,” a miner can make.

The “proof-of-work” idea was originally conceived as a spam email deterrent. In order for a random financial newsletter writer to email you, they would first have to show you they devoted time, money and resources to solving a tedious puzzle. If each email required a puzzle that cost computing resources and, say, one second to solve, would spammers send as much email? Perhaps not. While the process was never adopted by email providers (just look at your “spam folder!”), bitcoin made use of the scheme to control contributions to the chain of blocks.

In an economics sense, the “proof of work” means that miners must devote real resources to the computer network, enforcing “skin in the game”—time, computing power, electricity, etc.—in order to participate. In the words of Satoshi, “If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes.”¹¹ A miner *could* deviate from the consensus protocol. But doing so would be costly. At present, the so-called “hashing power” of the network is enormous, approaching 8 million terahashes per second (trillions of hashes per second), a rough proxy for how much computing resources are devoted to the network.¹² In fact, so much computing power is dedicated to the network that if we lined up the world's Top 500 supercomputers and devoted them to bitcoin mining, they would add up to less than 0.001% of the network computing power!¹³

As of September 2017, nearly 10,000 computer “nodes” run the bitcoin open source software, spanning 96 countries.¹⁴ There's now even a satellite in space running a full bitcoin node.¹⁵ It's a truly global, distributed network. Counter to JPMorgan's CEO Jamie Dimon's

recent claim (“It's just not a real thing, eventually it will be closed”), the network will prove difficult to shut down.¹⁶ No single person or entity controls the bitcoin network. And with a decentralized network that has no single owner nor a single physical location there's no single point of failure.

«THE PROCESS ALSO MAKES NEW BITCOINS “PROVABLY COSTLY TO CREATE,” PLAYING THE ROLE IN THE DIGITAL WORLD OF GOLD IN THE PHYSICAL WORLD, GOLD BEING RARE AND COSTLY TO EXTRACT THUS PROVING ITS SCARCITY.»

Lesson: “skin in the game” through computing resources deters mischief-makers from joining or altering the network, making it more likely—or at least less *costly*—they will cooperate.

LESSON #4: WHY MAINTAIN A LEDGER? WHAT'S IN IT FOR ME? THE ADDED ECONOMIC INCENTIVES

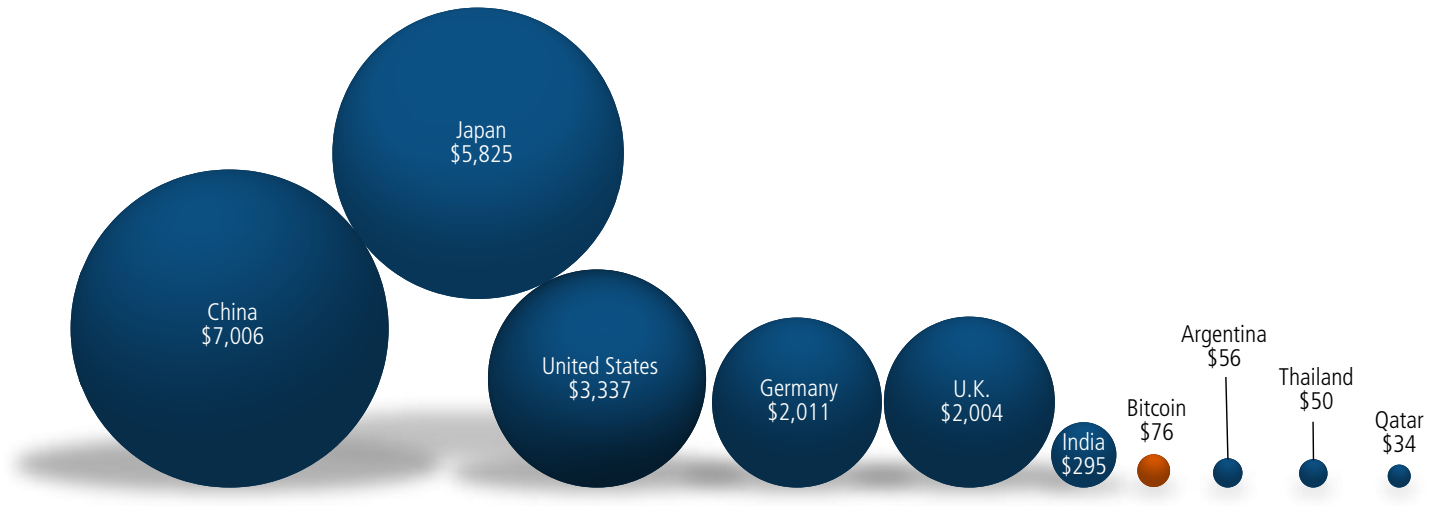
Ok, so now we have a chain of blocks (the list of transactions), appended only by “miners” who conduct a “proof of work” (puzzle) to show that the transactions are valid and that the miners have devoted real resources to the network. We still have a nagging question: who would actually spend time and resources to maintain such a ledger?!

Simple: the maintainers of the network derive value from securing the ledger by earning 12.5 bitcoin with every new, confirmed block added to the chain in which they solve the puzzle first.¹⁷ The process also makes new bitcoins “provably costly to create,” playing the role in the digital world of gold in the physical world, gold being rare and costly to extract thus proving its scarcity.

In other words, the network does not depend on the altruism of contributors to create the list or volunteers helping build the consensus list. Instead, bitcoin incentivizes good behavior to generate a consensus about who owns what. It's not the stick but the carrot that helps the network.

Lesson: The built-in incentives, in effect, glue people together. Devoting more resources to the network secure it while; the more secure the network the more economic value stakeholders derive.

fig. 2 IS BITCOIN THE HOTTEST CURRENCY? M1 MONEY SUPPLY* VALUE IN VARIOUS COUNTRIES COMPARED TO TOTAL VALUE OF BITCOIN (BILLIONS OF USD)



Source: Oxford Economics, Bloomberg, Payden Calculations
*M1 money supply = banknotes, coin and bank deposits

CRYPTOECONOMIC TRUST

Let's pause a moment and admire what's been created: to create a scarce, digital asset, we replaced the "mint" or "bank" with a single, agreed upon list (a "chain of blocks") maintained by a distributed network of computer nodes spread around the globe. It's the result of a combination of cryptography, a distributed ledger, "proof of work" and game theory (the incentives of the miners). Hence, cryptoeconomics.

As the term cryptoeconomics implies, bitcoin is not *merely* a new currency or technology or new asset, it's a new way of organizing economic activity. Think of the institutions important to the functioning of modern society: first to mind are often the nation-state, a central bank, the stock market, the joint stock corporation, and non-profits. Each embodies ways of organizing humans to achieve a desired end. More generally, these institutions create trust. In turn, "empirical studies, however, confirm the important role of trust in overcoming social dilemmas".

DID YOU KNOW?

We take technologies for granted that once appeared strange and novel—or even useless. Take for example the idea of a corporation owning its own internet address. Sounds normal, right? But in 1994, *Wired* magazine tried to give McDonald's—yes, the burger chain—the URL McDonalds.com. The reporter couldn't get anyone at the Golden Arches global headquarters on the phone to accept the free offer. Will every corporation one day have its own cryptocurrency?¹⁸

Those are the words of Elinor Ostrom, winner of the Nobel Prize in Economics in 2009. In her work she sought a "new theory to explain phenomena that do not fit in a dichotomous world of 'the market' and 'the state.'"¹⁹

The cryptoeconomic institution described above is in fact a new way to form consensus about underlying information *without* relying on a nation-state or a corporation. Stakeholders find motivation in the economic incentives associated with the network. The network bootstrapped itself into existence in a bottom-up process creating trust without relying on a central authority.

BUBBLE TROUBLE?

Of course, new technology and institutions breed hype—and often over-hype. In the words of Roy Amara, "We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run."²⁰


Carlota Perez, who has studied technological disruption and the role of finance, wrote: "What one can say with little risk of erring is that, once the design, product and profit space of a new paradigm is visible, the imagination of a vast number of potential engineers, designers and entrepreneurs is fired to innovate within the new general trajectories. As available finance makes their projects possible and as their astounding success makes the paradigm even more visible and attractive to a great number of people, the ranks of those that feel the calling will invariably swell."²¹

Nobody can predict the future. There are in fact, plenty of other cryptocurrencies that could do as well, if not better than bitcoin. But it's important to recognize important shifts when they happen. The birth

DID YOU KNOW?

Cheap Compared to Gold and Many “Currencies”

Based on the bitcoin protocol, the supply of bitcoin will approach 21 million in 2140. With 16,586,438 already in digital wallets around the world, scarcity and predictability are baked into the software’s design.²² Why does that matter? Are you prone to doubt the wisdom of central bankers tinkering with currencies in say, Venezuela or Argentina or China? Do you seek to protect the wealth of your family from the whims of monetary policy makers and their mistakes? Are you drawn to the shiny metal, gold? Or rare paintings? Well a scarce digital asset may provide you an additional option. We’re not saying put all your assets in the cryptobasket. But, one recent example, the German central bank completed a move of gold bank from New York and Paris to its vault in Frankfurt. The bank moved EUR 24 billion worth of gold bars. It took four years to complete.²³ Maybe there are better options? And despite the recent runup in price, bitcoin remains cheap compared to roughly comparable assets. For example, the current market capitalization (i.e., the amount outstanding multiplied by the current market price) of gold is USD 9 *trillion*, roughly 120 times the market cap of bitcoin at USD 76 billion as of September 2017. Further, compared to the M1 money supply of many major world economies, bitcoin also appears to have plenty of upside value potential (see *Figure 2 on previous page*).

of a new economic institution is one of those shifts. It’s not every day or year or even every decade or even every century that a new asset class supported by a new, novel institution comes along. Whether or not the new institutions bears fruit—and what that fruit may be—remains to be seen. 

SOURCES

1. <https://www.payden.com/library/pov/POVQ413.pdf>
2. <http://video.foxbusiness.com/v/2359385547001/?#sp=show-clips>
3. <https://www.cnbc.com/2017/09/12/jpmorgan-ceo-jamie-dimon-raises-flag-on-trading-revenue-sees-20-percent-fall-for-the-third-quarter.html>
4. <https://www.oaktreecapital.com/insights/howard-marks-memos>
5. <https://qz.com/1067557/robert-shiller-wrote-the-book-on-bubbles-he-says-the-best-example-right-now-is-bitcoin/>
6. <https://coinmarketcap.com/all/views/all/>
7. There’s a lot of confusion on this topic. We’ll avoid many of the technical details, but if you’re interested there’s no better place to start than the white paper issued by the pseudonymous bitcoin creator Satoshi Nakamoto.
8. Tunku Varadarajan. “The Blockchain Is the Internet of Money.” *Wall Street Journal*, September 22, 2017.
9. <https://bitcoin.org/bitcoin.pdf>
10. <http://cryptocouple.com/#>
11. <https://bitcoin.org/bitcoin.pdf>
12. <https://blockchain.info/charts/hash-rate>
13. https://www.reddit.com/r/Bitcoin/comments/5kfuxk/how_powerful_is_the_bitcoin_network/
14. <https://bitnodes.21.co/>
15. <https://blockstream.com/satellite/satellite/>
16. <https://www.cnbc.com/2017/09/19/ray-dalio-says-bitcoin-is-bubble.html>
17. The so-called “block reward” halves approximately every 4 years. The next time: June 2020, to 6.25.
18. <https://www.wired.com/1994/10/mcdonalds/>
19. Elinor Ostrom. “Beyond Markets and States: Polycentric Governance of Complex Economics Systems.” Nobel Prize Lecture. December 8, 2009.
20. https://en.wikipedia.org/wiki/Roy_Amara
21. Carlota Perez. “Technological Revolutions and Financial Capital: The Dynamics of Bubbles and Gold Ages.” Edward Elgar: Cheltenham, UK, 2002.
22. <http://www.bitcoinblockhalf.com/>
23. <https://www.ft.com/content/f08e7e00-3602-36a3-ab78-be34d66cb6e7>