Why Bitcoin Matters

Marc Andreessen ⋮ 23-30 minutes ⋮ Invalid Date

Photo

Marc Andreessen, a co-founder of the venture capital firm Andreessen Horowitz.Credit Keith Bedford/Reuters

Editor's note: Marc Andreessen's venture capital firm, Andreessen Horowitz, has invested just under $50 million in Bitcoin-related start-ups. The firm is actively searching for more Bitcoin-based investment opportunities. He does not personally own more than a de minimis amount of Bitcoin.

A mysterious new technology emerges, seemingly out of nowhere, but actually the result of two decades of intense research and development by nearly anonymous researchers.

Political idealists project visions of liberation and revolution onto it; establishment elites heap contempt and scorn on it.

On the other hand, technologists – nerds – are transfixed by it. They see within it enormous potential and spend their nights and weekends tinkering with it.

Video

Bitcoin Believers

While regulators debate the pros and cons of bitcoins, this volatile digital currency inspires the question: What makes money, money?

By Channon Hodge, David Gillen, Kimberly Moy and Aaron Byrd on Publish Date November 24, 2013.

Eventually mainstream products, companies and industries emerge to commercialize it; its effects become profound; and later, many people wonder why its powerful promise wasn't more obvious from the start.

What technology am I talking about? Personal computers in 1975, the Internet in 1993, and – I believe – Bitcoin in 2014.

One can hardly accuse Bitcoin of being an uncovered topic, yet the gulf between what the press and many regular people believe Bitcoin is, and what a growing critical mass of technologists believe Bitcoin is, remains enormous. In this post, I will explain why Bitcoin has so many Silicon Valley programmers and entrepreneurs all lathered up, and what I think Bitcoin's future potential is.

First, Bitcoin at its most fundamental level is a breakthrough in computer science – one that builds on 20 years of research into cryptographic currency, and 40 years of research in cryptography, by thousands of researchers around the world.

Bitcoin is the first practical solution to a longstanding problem in computer science called the Byzantine Generals Problem. To quote from the original paper defining the B.G.P.: "[Imagine] a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement."

More generally, the B.G.P. poses the question of how to establish trust between otherwise unrelated parties over an untrusted network like the Internet.

The practical consequence of solving this problem is that Bitcoin gives us, for the first time, a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge

the legitimacy of the transfer. The consequences of this breakthrough are hard to overstate.

What kinds of digital property might be transferred in this way? Think about digital signatures, digital contracts, digital keys (to physical locks, or to online lockers), digital ownership of physical assets such as cars and houses, digital stocks and bonds … and digital money.

All these are exchanged through a distributed network of trust that does not require or rely upon a central intermediary like a bank or broker. And all in a way where only the owner of an asset can send it, only the intended recipient can receive it, the asset can only exist in one place at a time, and everyone can validate transactions and ownership of all assets anytime they want.

How does this work?

Bitcoin is an Internet-wide distributed ledger. You buy into the ledger by purchasing one of a fixed number of slots, either with cash or by selling a product and service for Bitcoin. You sell out of the ledger by trading your Bitcoin to someone else who wants to buy into the ledger. Anyone in the world can buy into or sell out of the ledger any time they want – with no approval needed, and with no or very low fees. The Bitcoin "coins" themselves are simply slots in the ledger, analogous in some ways to seats on a stock exchange, except much more broadly applicable to real world transactions.

The Bitcoin ledger is a new kind of payment system. Anyone in the world can pay anyone else in the world any amount of value of Bitcoin by simply transferring ownership of the corresponding slot in the ledger. Put value in, transfer it, the recipient gets value out, no authorization required, and in many cases, no fees.

That last part is enormously important. Bitcoin is the first Internetwide payment system where transactions either happen with no fees or very low fees (down to fractions of pennies). Existing payment systems charge fees of about 2 to 3 percent – and that's in the developed world. In lots of other places, there either are no modern payment systems or the rates are significantly higher. We'll come back to that.

Bitcoin is a digital bearer instrument. It is a way to exchange money or assets between parties with no pre-existing trust: A string of numbers is sent over email or text message in the simplest case. The sender doesn't need to know or trust the receiver or vice versa. Related, there are no chargebacks – this is the part that is literally like cash – if you have the money or the asset, you can pay with it; if you don't, you can't. This is brand new. This has never existed in digital form before.

Bitcoin is a digital currency, whose value is based directly on two things: use of the payment system today – volume and velocity of payments running through the ledger – and speculation on future use of the payment system. This is one part that is confusing people. It's not as much that the Bitcoin currency has some arbitrary value and then people are trading with it; it's more that people can trade with Bitcoin (anywhere, everywhere, with no fraud and no or very low fees) and as a result it has value.

It is perhaps true right at this moment that the value of Bitcoin currency is based more on speculation than actual payment volume, but it is equally true that that speculation is establishing a sufficiently high price for the currency that payments have become practically possible. The Bitcoin currency had to be worth something before it could bear any amount of real-world payment volume. This is the classic "chicken and egg" problem with new technology: new technology is not worth much until it's worth a lot. And so the fact that Bitcoin has risen in value in part because of speculation is making the reality of its usefulness arrive much faster than it would have otherwise.

Critics of Bitcoin point to limited usage by ordinary consumers and merchants, but that same criticism was leveled against PCs and the Internet at the same stage. Every day, more and more consumers and merchants are buying, using and selling Bitcoin, all around the world. The overall numbers are still small, but they are growing quickly. And ease of use for all participants is rapidly increasing as Bitcoin tools and technologies are improved. Remember, it used to be technically challenging to even get on the Internet. Now it's not.

The criticism that merchants will not accept Bitcoin because of its volatility is also incorrect. Bitcoin can be used entirely as a payment system; merchants do not need to hold any Bitcoin currency or be exposed to Bitcoin volatility at any time. Any consumer or merchant can trade in and out of Bitcoin and other currencies any time they want.

Why would any merchant – online or in the real world – want to accept Bitcoin as payment, given the currently small number of consumers who want to pay with it? My partner Chris Dixon recently gave this example:

“Let’s say you sell electronics online. Profit margins in those businesses are usually under 5 percent, which means conventional 2.5 percent payment fees consume half the margin. That’s money that could be reinvested in the business, passed back to consumers or taxed by the government. Of all of those choices, handing 2.5 percent to banks to move bits around the Internet is the worst possible choice. Another challenge merchants have with payments is accepting international payments. If you are wondering why your favorite product or service isn’t available in your country, the answer is often payments.”

In addition, merchants are highly attracted to Bitcoin because it eliminates the risk of credit card fraud. This is the form of fraud that motivates so many criminals to put so much work into stealing personal customer information and credit card numbers.

Since Bitcoin is a digital bearer instrument, the receiver of a payment does not get any information from the sender that can be used to steal money from the sender in the future, either by that merchant or by a criminal who steals that information from the merchant.

Credit card fraud is such a big deal for merchants, credit card processors and banks that online fraud detection systems are hair-trigger wired to stop transactions that look even slightly suspicious, whether or not they are actually fraudulent. As a result, many online merchants are forced to turn away 5 to 10 percent of incoming orders that they could take without fear if the customers were paying with Bitcoin, where such fraud would not be possible. Since these are orders that were coming in already, they are inherently the highest margin orders a merchant can get, and so being able to take them will drastically increase many merchants’ profit margins.

Bitcoin’s antifraud properties even extend into the physical world of retail stores and shoppers.

For example, with Bitcoin, the huge hack that recently stole 70 million consumers’ credit card information from the Target department store chain would not have been possible. Here’s how that would work:

You fill your cart and go to the checkout station like you do now. But instead of handing over your credit card to pay, you pull out your smartphone and take a snapshot of a QR code displayed by the cash register. The QR code contains all the information required for you to send Bitcoin to Target, including the amount. You click “Confirm” on your phone and the transaction is done (including converting dollars from your account into Bitcoin, if you did not own any Bitcoin).

Target is happy because it has the money in the form of Bitcoin, which it can immediately turn into dollars if it wants, and it paid no or very low payment processing fees; you are happy because there is no way for hackers to steal any of your personal information; and organized crime is unhappy. (Well, maybe criminals are still happy: They can try to steal money directly from poorly-secured merchant computer systems. But even if they succeed, consumers bear no risk of loss, fraud or identity theft.)

Finally, I’d like to address the claim made by some critics that Bitcoin is a haven for bad behavior, for criminals and terrorists to transfer money anonymously with impunity. This is a myth, fostered mostly by sensationalistic press coverage and an incomplete understanding of the technology. Much like email, which is quite traceable, Bitcoin is pseudonymous, not anonymous. Further, every transaction in the Bitcoin network is tracked and logged forever in the Bitcoin blockchain, or permanent record, available for all to see. As a result, Bitcoin is considerably easier for law enforcement to trace than cash, gold or diamonds.

What’s the future of Bitcoin?

Bitcoin is a classic network effect, a positive feedback loop. The more people who use Bitcoin, the more valuable Bitcoin is for everyone who uses it, and the higher the incentive for the next user to start using the technology. Bitcoin shares this network effect property with the telephone system, the web, and popular Internet services like eBay and Facebook.

In fact, Bitcoin is a four-sided network effect. There are four constituencies that participate in expanding the value of Bitcoin as a consequence of their own self-interested participation. Those constituencies are (1) consumers who pay with Bitcoin, (2) merchants who accept Bitcoin, (3) “miners” who run the computers that process and validate all the transactions and enable the distributed trust network to exist, and (4) developers and entrepreneurs who are building new products and services with and on top of Bitcoin.

All four sides of the network effect are playing a valuable part in expanding the value of the overall system, but the fourth is particularly important.

All over Silicon Valley and around the world, many thousands of programmers are using Bitcoin as a building

block for a kaleidoscope of new product and service ideas that were not possible before. And at our venture capital firm, Andreessen Horowitz, we are seeing a rapidly increasing number of outstanding entrepreneurs – not a few with highly respected track records in the financial industry – building companies on top of Bitcoin.

For this reason alone, new challengers to Bitcoin face a hard uphill battle. If something is to displace Bitcoin now, it will have to have sizable improvements and it will have to happen quickly. Otherwise, this network effect will carry Bitcoin to dominance.

One immediately obvious and enormous area for Bitcoin-based innovation is international remittance. Every day, hundreds of millions of low-income people go to work in hard jobs in foreign countries to make money to send back to their families in their home countries – over $400 billion in total annually, according to the World Bank. Every day, banks and payment companies extract mind-boggling fees, up to 10 percent and sometimes even higher, to send this money.

Switching to Bitcoin, which charges no or very low fees, for these remittance payments will therefore raise the quality of life of migrant workers and their families significantly. In fact, it is hard to think of any one thing that would have a faster and more positive effect on so many people in the world's poorest countries.

Moreover, Bitcoin generally can be a powerful force to bring a much larger number of people around the world into the modern economic system. Only about 20 countries around the world have what we would consider to be fully modern banking and payment systems; the other roughly 175 have a long way to go. As a result, many people in many countries are excluded from products and services that we in the West take for granted. Even Netflix, a completely virtual service, is only available in about 40 countries. Bitcoin, as a global payment system anyone can use from anywhere at any time, can be a powerful catalyst to extend the benefits of the modern economic system to virtually everyone on the planet.

And even here in the United States, a long-recognized problem is the extremely high fees that the "unbanked" — people without conventional bank accounts – pay for even basic financial services. Bitcoin can be used to go straight at that problem, by making it easy to offer extremely low-fee services to people outside of the traditional financial system.

A third fascinating use case for Bitcoin is micropayments, or ultrasmall payments. Micropayments have never been feasible, despite 20 years of attempts, because it is not cost effective to run small payments (think $1 and below, down to pennies or fractions of a penny) through the existing credit/debit and banking systems. The fee structure of those systems makes that nonviable.

All of a sudden, with Bitcoin, that's trivially easy. Bitcoins have the nifty property of infinite divisibility: currently down to eight decimal places after the dot, but more in the future. So you can specify an arbitrarily small amount of money, like a thousandth of a penny, and send it to anyone in the world for free or near-free.

Think about content monetization, for example. One reason media businesses such as newspapers struggle to charge for content is because they need to charge either all (pay the entire subscription fee for all the content) or nothing (which then results in all those terrible banner ads everywhere on the web). All of a sudden, with Bitcoin, there is an economically viable way to charge arbitrarily small amounts of money per article, or per section, or per hour, or per video play, or per archive access, or per news alert.

Another potential use of Bitcoin micropayments is to fight spam. Future email systems and social networks could refuse to accept incoming messages unless they were accompanied with tiny amounts of Bitcoin – tiny enough to not matter to the sender, but large enough to deter spammers, who today can send uncounted billions of spam messages for free with impunity.

Finally, a fourth interesting use case is public payments. This idea first came to my attention in a news article a few months ago. A random spectator at a televised sports event held up a placard with a QR code and the text "Send me Bitcoin!" He received $25,000 in Bitcoin in the first 24 hours, all from people he had never met. This was the first time in history that you could see someone holding up a sign, in person or on TV or in a photo, and then send them money with two clicks on your smartphone: take the photo of the QR code on the sign, and click to send the money.

Think about the implications for protest movements. Today protesters want to get on TV so people learn about their cause. Tomorrow they'll want to get on TV because that's how they'll raise money, by literally holding up signs that let people anywhere in the world who sympathize with them send them money on the spot. Bitcoin is a financial technology dream come true for even the most hardened anticapitalist political organizer.

The coming years will be a period of great drama and excitement revolving around this new technology.

For example, some prominent economists are deeply skeptical of Bitcoin, even though Ben S. Bernanke, formerly Federal Reserve chairman, recently wrote that digital currencies like Bitcoin "may hold long-term promise, particularly if they promote a faster, more secure and more efficient payment system." And in 1999, the legendary economist Milton Friedman said: "One thing that's missing but will soon be developed is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B without A knowing B or B knowing A – the way I can take a $20 bill and hand it over to you, and you may get that without knowing who I am."

Economists who attack Bitcoin today might be correct, but I'm with Ben and Milton.

Further, there is no shortage of regulatory topics and issues that will have to be addressed, since almost no country's regulatory framework for banking and payments anticipated a technology like Bitcoin.

But I hope that I have given you a sense of the enormous promise of Bitcoin. Far from a mere libertarian fairy tale or a simple Silicon Valley exercise in hype, Bitcoin offers a sweeping vista of opportunity to reimagine how the financial system can and should work in the Internet era, and a catalyst to reshape that system in ways that are more powerful for individuals and businesses alike.