



THE LONG READ



HOW BITCOIN SECURED CURRENCY



DEVINA MEHRA

DEMYSTIFYING THE CRYPTOCURRENCY CHAMPION THAT'S DEFIED LEGACY AND TAKEN THE NEW WORLD BY STORM: IS IT A BANKABLE INVESTMENT OR NOT? THE JURY IS OUT...

On 12 January, 2009, the pseudonymous Satoshi Nakamoto made the first-ever Bitcoin (BTC) transaction, sending 10 BTCs to developer Hal Finney and just like that a new asset, or rather a new asset class was born. Never mind that the 'value' of the asset was still minuscule. The first-ever USD/BTC rate was \$1 = 1,309.03 BTC, or inversely, 1 BTC was worth just \$0.00076, or a mere 0.076 cents on October 2009. A few months later, on 4 February, 2010, the first-ever Bitcoin exchange was established.

Going back a bit further, triggered by the 2008 financial crisis, Namoto mined the first-ever Bitcoin block, named the genesis block, on 3 January, 2009, awarding Satoshi the first 50 Bitcoins of the 21 million that will ever be created. To put this in perspective, about 18.6 million Bitcoins have already been created, leaving only 2.4 million or so to be mined.

In May 2010, a developer and early adopter, Laszlo, offered 10,000 BTC for two large pizzas, in bitcoinalk.org. Someone took him up on that offer. With a cost of around \$25 dollars, these pizzas set the first "real-life" value for Bitcoin at 80,002.5 dollars. This was a significant milestone, and has since been celebrated in the ecosystem as "Bitcoin Pizza Day".

On 9 February, 2011, Bitcoin reached parity with the dollar as Mt. Gox (a Bitcoin exchange that dominated the market until February 2014). On 2 June, it reached \$10; by 8 June, it climbed to its highest price yet of \$119.1, only to plummet again to \$10 four days later, on 12 June. This movement would be known as "The Great Bubble of 2011", and it wouldn't be the last parabolic movement in Bitcoin prices.

In April 2013, Bitcoin surpassed \$100 for the first time and the market cap broke the \$1 billion-dollar threshold. Bitcoin reached \$266, before crashing again to around \$100, after another exchange hack. That's when governments began to notice Bitcoin and tried to figure out how to regulate, control, or even control this new digital currency.

In October 2013, the FBI managed to shut down the infamous dark web site Silk Road and seize its assets. This cast a shadow on Bitcoin as the coin of criminals and money laundering.

But once again Bitcoin saw a huge price surge, going from a little over \$100 in October to breaking the \$1,000 barrier in November. But a bar from China and the bankruptcy of Mt. Gox, both in a span of a couple of months, drove the price down again, and Bitcoin didn't reach that psychological barrier again until January 2017.

2017 was a very interesting year for Bitcoin and the ecosystem in general. There were innovations like multi-million Initial Coin Offerings (ICOs), forked coins etc. And, of course, the bull run brought a lot of huzz around "the new digital currency", the cryptocurrency rallied from around the \$1,000 mark to almost \$19,000 by December 2017.

In 2017, Bitcoin also gained more legitimacy among lawmakers and legacy financial companies. For example, Japan passed a law to accept Bitcoin as a legal payment method, and Russia had announced that it will legalise the use of cryptocurrencies such as Bitcoin. However, by 2018, regulations also started creeping up. In January 2018, South Korea brought in a regulation that requires all Bitcoin traders to reveal

Bitcoin is to millennials what gold was to a generation ago. It's liquid, mobile, hedges against inflation and gives growth. All attributes that we grew up associating with gold, the current generation associates with Bitcoin

Vineet Arora



their identity, thus putting a ban on anonymous trading of Bitcoins.

Come March 2020, Bitcoin was no exception to the "dash for cash", considering it tanked more than 50 per cent at the height of the Covid crisis to \$4,800. But the rebound has been as fierce: it hit an all-time high of \$64,000 on 14 April 2021. The recent top came in coincidentally on the exact same day that we witnessed a bumper listing of Coinbase (COIN) on NASDAQ at an eye-popping valuation of \$100 billion.

Meanwhile, acceptance of this novel cryptocurrency kept accelerating. In October 2020, PayPal launched a new service enabling users to buy, hold and sell cryptocurrency. And in March 2021, Elon Musk tweeted, "you can now buy a Tesla with Bitcoin."

How Bitcoin works
Imagine a pearl lying on the sidewalk. I find that pearl and give it to you; you now have one pearl and I have zero. Now let's look closely at what happened: I put my pearl in your hand, we both know it was real, we experienced it.

"Did we need a third person to confirm that this transfer occurred? No. So what does this mean? Well, the pearl is now yours, I can't give you another pearl because I gave you my only one. I am officially 'pearl-less' and you are currently in full control of that pearl. You can give it to a friend and they can give it to someone else and so on or you could just leave it on the sidewalk. The choice is yours. That's how an in-person exchange works."

Now, let's say I have one "digital pearl" and I give it to you. The problem? How would you know that I didn't duplicate the digital pearl before sending it to you? How would you know I didn't send the same pearl to my friend on Instagram? You wouldn't know. Only I would. Now you can see that this digital exchange has some significant flaws: sending digital pearls is not the same as sending physical pearls. This problem has a name, it's called "Double Spending".

Just like a physical ledger, where you record all transactions, we need a digital ledger for the above online transfer or transaction and have someone in charge of it. However, that brings up another issue: what if the person in charge of the ledger wanted to create some more digital pearls? Well, they could. No one's stopping them from adding/bringing more pearls into existence, thus adding to the supply and reducing its value.

There is a second issue. When I first give you my pearl, it was just you and me. Imagine that the person in charge has to verify the ledger every time there is an exchange. Not very efficient, is it? Here's where Bitcoin comes up with a nifty solution—a "peer-to-peer" network.

What if we gave this ledger to everybody? Instead of a single ledger lying on a third party's computer, everyone involved would have a copy of all the transactions that have ever happened. These digital pearl transactions are recorded on everyone's ledger, so you can't cheat. I can't send you digital pearls I don't have since that wouldn't sync in with everyone in the system. It would be a tough system to beat especially if you need to change hundreds of thousands of other ledgers. As the system gets bigger, it also gets harder to hack or take control of.

Plus, it's decentralised, so no one can decide to give themselves more digital pearls. The rules of the system were defined at the beginning and the code and rules are open source.

You could participate in this network, update the ledger and make sure it all checks out ("mining Bitcoin"). In fact, that's the only way to create more digital pearls in the system. For your trouble, you could get some digital pearls as a reward. This system exists, and is called the "Bitcoin Protocol". All those digital pearls are the Bitcoins within the system.

The rules define the total supply of Bitcoin, subject to a total maximum of 21 million as mentioned earlier. When I make an exchange, I can certify that the Bitcoin left my possession and is now entirely yours because it's a public ledger. I didn't need a third party to make sure I didn't cheat. We can now deal with 1,000 Bitcoins or 1 million Bitcoins or even a tiny fraction of a Bitcoin. I can send it with a click of a button, even if I was in



Devrat Moondhra

We are still early in the adoption cycle... there will be volatility, but, in the long run, Bitcoin will become a store of value like gold is

Devrat Moondhra

Rather than assess Bitcoin on a standalone basis, it is important to look at any investment as part of a portfolio to assess whether it adds any value, in terms of risk-adjusted return, to your original portfolio

Harsh Shivlani



Dubai and you were in Denmark or Denver.

Bitcoin vs gold: store of value
Bitcoin is largely being touted as "digital gold" or as a store of value. However, gold itself survived the end of gold coinage, the rise of paper money, the end of the gold standard and so on. It fended off many challenges to become what it is today.

So, it is only natural to expect that we will witness volatility in this novel asset class/payment system. Here, the idea of anti-fragility could be applicable; i.e., the more it survives, the more reputable it becomes.

On a comparison with gold, this is what Vineet Arora, Managing Director, DVA Wealth Management has to say: "Bitcoin is millennials what gold was to a generation ago. It's liquid, mobile, hedges against inflation and gives growth. All attributes that we grew up associating with gold, the current generation associates with Bitcoin. Whether we like it or like to dislike it, it's here to stay."

The safety aspect depends on an investor's definition of "safe". Let's consider two simple ways of assessing this: price volatility and maximum drawdown (the maximum decline from a high peak to a pullback low).

If we look at volatility, Bitcoin is more than five times as volatile as gold and 10 times as volatile as the US dollar. Meanwhile, the maximum drawdown of Bitcoin is a whopping 83 per cent, compared to 20 per cent and 14 per cent for gold and USD respectively. Another empirical evidence of Bitcoin's notorious risk profile can be encapsulated by looking at the maximum one-day loss registered — 27 per cent (on 12 March, 2020). Doesn't look like a store of value, does it?

Another possible risk is the complete loss of principal. By storing your Bitcoins on an exchange wallet ("hot wallet" or "online wallet"), you are taking on counterparty risk (hack, default, etc.). A "cold wallet" comes in handy here. A cold wallet is a wallet that is not connected to the Internet and therefore stands a far lesser risk of being compromised.

Does this mean Bitcoin should not be a part of an investment portfolio? "It wouldn't dismiss it just yet," says Harsh Shivlani of First Global. "Rather than assess it only on a standalone basis, it is important to look at any investment as part of a portfolio to assess whether it adds any value, in terms of risk-adjusted return, to your original portfolio."

Will the future of currency be digital?
The primary goal of any form of currency is to be a reliable and convenient source of payment. For this to happen, you would expect the value of the currency to be fairly stable over time and the infrastructure surrounding it to have the ability to process sizeable transactions relatively quickly.

Currently, Bitcoin can't come even close to competing with legacy payment systems. With a capacity of just 7 transactions per second and confirmation times of 10 minutes on average, it's far behind Visa's maximum capacity of 65,000 transactions per second and its nearly instant payments.

Furthermore, because only so many transactions can fit in a block when the network is congested, fees skyrocket in a bidding war between users to get their transaction in the next block. However, there are certain upgrades in line that could solve all these problems, such as the "Lightning Network".

According to a survey by the Bank for International Settlements, one in 10 central banks expect to issue their own digital currencies within the next three years.

The views on cryptocurrencies remain quite diverse. "While CBDCs may replace currency, in the near term I still find it hard to accept Bitcoin or any altcoins as a store of value and a medium of exchange. Blockchain as a technology, however, does seem poised for a great future," says Prashant Mehta, Chief Investment Officer, KIP Holdings Ltd.

On the other hand, Devrat Moondhra, Director, Duro Steel AG and Blockchain Investor, says, "Bitcoin is like lithium. Initially there are few believers and many non-believers (atheists), but eventually there are more and more believers, following which there is mass adoption. We are still early in the adoption cycle... there will be volatility, but, in the long run, Bitcoin will become a store of value like gold is."

(Devina Mehra is co-founder of Vira Global, a global quantitative asset management group. The views expressed are personal.)

While CBDCs may replace currency, in the near term I still find it hard to accept Bitcoin or any altcoins as a store of value and a medium of exchange

Prashant Mehta

