ANNEALBC.COM

ANNEAL
BUSINESS COACHING

What the Heck is Bitcoin?

WHAT THE HECK IS BITCOIN?

First, what is Bitcoin? It is simply a digital record stored on a bunch of computers. Lest that freak you out, I'll remind you that most of your dollars are also simply digital records stored on a bunch of computers.

Both Bitcoin and dollars are money you can use to buy things. The amount of things you can buy with money is its value. For money to have value, history teaches us that it must be portable, durable, divisible, recognizable and scarce. We'll just accept that both dollars and Bitcoin are portable, durable, divisible, and recognizable but the last part, scarcity, is the big bugaboo when it comes to the value of money.

SCARCITY

If we could all create our own money, it would no longer be scarce and would no longer have value. Gold has long been recognized as an ideal money because it is portable, durable, divisible, recognizable AND because it is naturally scarce*. Miners can and do increase the amount of available gold,** but it takes great effort to increase the supply by even very small amounts. Anyone who has ever watched the Discovery Channel show Gold Rush can attest to that.

Scarcity is different with digital money. The scarcity of digital money such as dollars and Bitcoin depends on rules and processes to prevent people from creating an unlimited supply.

Dollars are suspect in that regard because they are among the so-called fiat currencies. "Fiat" literally means "let it be done," as when someone says "Let there be more dollars" and - poof - there are more dollars. The scarcity of dollars is enforced by laws that say only the U.S. government, through The Federal Reserve, can create them.*** The flaw in the system is that The Federal Reserve is made up of people whose decisions are fallible and subject to the

whims of political influence. Fiat currency is soft ground on which to base the value of a currency.

The creators of Bitcoin think the scarcity of money should not be entrusted to human-influenced institutions, so they created Bitcoin as an alternative.
Bitcoins, like gold, are also created through "mining." However Bitcoin mining does not involve bulldozers or dynamite, but rather a process of miners' doing (expensive) work on behalf of the Bitcoin system. Once the requisite work is done, miners are allowed to guess a correct number from a very, very large list of numbers. The first miner to complete the work and guess the right number is rewarded by having their name affixed as the first owner of newly "mined" coin(s).

The total supply of coins is predetermined by an algorithm and cannot increase above 21 million coins (of which about 16.5 million have been mined). The number of Bitcoins awarded to successful miners is reduced by half every four years and will continue to be halved every four years until the final Bitcoin is mined in about the year 2140. Halving the amount of Bitcoin rewarded for the same or more work means that the value of Bitcoins must go up or miners will quit mining them. This is a built-in guard against devaluation of Bitcoin by mining. After 21 million coins have been mined, the total number of Bitcoins will remain fixed except for coins lost to the system for various reasons.****
So, an algorithm, skill, effort, and expense replace human judgment in determining the available supply of Bitcoin, but what about after Bitcoin are created?

SAFEGUARDING MONEY

Gold is protected from theft by the fact that it's gold. If a scallywag wants to steal your gold, he has to come and get it. That's why we have vaults and bars and alarm systems.

Digital dollars are protected by passwords, two factor authentication, transaction confirmation and all the other hoops you jump through to access your money while protecting against identity theft. The safeguards generally work, but theft still happens to the tune of about $56 billion in 2020.
Bitcoin is protected by blockchains and "a distributed ledger," neither of which has ever been successfully breached.*****

Blockchains are lists of digital entries recorded in "blocks" each of which is a record of a single bookkeeping transaction showing who sold and who acquired all or part of a Bitcoin. Each block, once accepted as valid, becomes a new link in a blockchain and cannot be altered.

The blockchain therefore is a digital record of ownership listing transfer after transfer, seller after seller, buyer after buyer, beginning with the original miner up to and including the current owner. If the current owner sells all or part of a Bitcoin, a new block is created and the blockchain becomes one link longer.

Okay but can't really smart hackers break into the system to create new Bitcoin or change an ownership record on a block? Well, no. Not even "theoretically."

Blocks and Blockchains use two strategies to protect against forging unauthorized Bitcoin or altering a record of ownership. First, a block containing a new transaction has to be accepted into a blockchain. Acceptance involves matching some very complicated "keys" (think passwords) coded into the blocks. The seller's password has to match the last password on the block chain. Block passwords are not your ordinary birthday- or home address- type passwords. They are made up of a 256 character code generated by the system and available only to the current owner. In order to change a record, the hacker must either have or solve for the current owner's password. There

are 938 followed by 78 digits possible combinations in a 256 bit password. My research tells me it would take the most powerful computer in the world about 1 million years to decipher one.

Second, Bitcoin uses a “distributed ledger.” Suppose some hacker got lucky, and solved for a password in less than the predicted time, say half a million years. His hack would still not succeed because there is no single, central database of block chains in which to make the change. Instead, blockchain records are kept on a “distributed ledger” made up of a bunch of computers (currently around 10,000) which contain identical records of Blockchains. Any new block will not be added to any chain until it has been validated by a predetermined number (and eventually all) of the computers in the ledger. Validating transactions is part of the work miners do in order to earn rewards. A hacker attempting to change a transaction would have to change it on all the computers in the distributed ledger which would take longer than the expected future of the universe. (But beware! A hacker who managed to steal your 256 character password would likely get away with your Bitcoin, the same way someone who stole your bank password could get away with your dollars.)

SAFEGUARDING MONEY

The value of a dollar saved from 2008 until today has declined about 25 percent due to inflation. The value of a Bitcoin purchased in 2008 has, as of this writing, increased 117,500 percent from around $40 to over $47,000.
That’s quite a spread, but there is the matter of price stability to consider. The value of dollars declines steadily over time as inflation rises. Not so with Bitcoin. The value of Bitcoin has been going up year after year, but their value behaves more like a stock portfolio than a savings account. Bitcoin prices rise and fall dramatically and quickly under the influence of traders who buy and sell to make money from price changes. You could easily find yourself buying

Bitcoin at a peak, only to see them lose 50% or more of their value within a few months or even weeks. Of course you could always ride out the dip and wait for prices to recover - but that's not an option if you need immediate access to your savings. In order for Bitcoin to become really useful as a currency or a savings account, price swings need to settle down.

The wild price swings should settle down as more and more people with a savings mentality (like me) buy Bitcoin. As the percentage of savers' ownership rises, the percentage of traders' ownership will decline as will the effects of their transactions on price swings. I expect Bitcoin to see fewer and fewer wild price swings.

WHY BITCOIN?

As I have said repeatedly, for currency to have value it must be portable, durable, divisible, and recognizable and scarce. What I didn't say was that it also must be accepted. We all accept dollars - we're willing to be paid in dollars and are confident we can use dollars to buy about anything we want. That's not yet true for Bitcoin.

There are many so-called crypto currencies vying to become the new world standard for money. Predicting which will prevail is like predicting what video, if any, will go viral. Bitcoin may not yet qualify as "gone viral," but is at least trending. It is by far the most accepted crypto currency which is evident in the fact that Bitcoin makes up about 66% of all issued crypto currencies. Bitcoin will become more valuable the more widely it is accepted by buyers and sellers and the easier it is to use directly to make and receive payments. However, for most purchases today, we must first buy Bitcoin with dollars, then convert them back to dollars to buy things. That is changing as more and more businesses such as AT&T, Microsoft, Overstock, Home Depot, Starbucks, and Whole Foods, accept Bitcoin directly.

Bitcoin is a logical, well-thought out, fascinating advance in money with ramifications far beyond what we've discussed here or that I fully comprehend. It looks like Bitcoin is here to stay (so long as governments allow it).

If you have any further questions, please don't hesitate to mail me at Martin@annealbc.com or visit www.annealbc.com

---

*About 200,000 total tons of gold have been mined worldwide. That sounds like a lot, but the entire amount would fit in a cube measuring about 100 feet on each side.

**Alchemy was the medieval precursor to chemistry, the purpose of which was to convert lead into gold. Of course it didn't (and doesn't) work, but England outlawed alchemy in 1404 AD out of fear that an increased supply would devalue the country's gold reserves. (There's really nothing new under the sun!)

*** Banks also "create" money by lending the same money multiple times through the fractional banking system. However, the original source of the money is the Fed.

**** Hang on to your Bitcoin password!

*****The criminal activity associated with Bitcoin is not from people hacking the system. It is from criminals blackmailing or ransoming people into handing over their Bitcoin the same way you might pay someone online.

Martin Holland

Martin Holland is the son of a successful entrepreneur. He grew up hearing about margins and markets, R&D and sales, risk and return on investment. He learned to love the language and rigors of business and grew to believe that business is both the most human of all endeavors and the highest calling. After selling a company in 2011, Martin became a coach in order to help other owners build profitable businesses that do not require their day-to-day involvement.

A native of Norman, Martin earned a B.A. degree from Hastings College in Hastings, Nebraska and a Masters in Business Administration degree from the University of Oklahoma. Over the past 7 years he has written business plans that have raised over $52.4 million in bank and investor financing. He has helped 157 (and counting) business owners reduce stress and increase performance through clarity of purpose, better marriages, more money, and more free time away from the business.