LOBBY SEVEN

Volume 22 April 5, 2018

"They write politics, we write government"

BITCOIN

Finally, A Practical Use for Mathematics

"Many individuals grew suddenly rich. A golden bait hung temptingly out before the people, and, one after the other, they rushed to the tulip marts, like flies around a honey-pot. Every one imagined that the passion for tulips would last forever," – Charles Mackey, Popular Delusions and the Madness of Crowds, 1841.

"The market can stay irrational longer than you can stay solvent," – John Maynard Keynes

It is either a revolutionary way to conduct all of life's transactions, or a means to move dark money for illegal activities. It is based on a piece of mathematics that will either change the way we think about record keeping or a complex formula whose calculations waste more electricity than used by the nation of Nigeria. They are worth $20,000 each or nothing at all.

Whatever it is, Bitcoin has captured the world's attention. A meteoric rise created millions - and millionaires - out of thin air. But the problems with a decentralized, unregulated currency have shown themselves to all but Bitcoin's most aggressive backers. Without rules to be enforced, scams and frauds have added to the risk inherent in any new investment.

Any asset - stock, bond, currency or real property - is worth what somebody will pay for it. But having worth is not the same as having value. Just because somebody will pay for something doesn't mean that they should. Here, we will describe Bitcoin is, and we'll try to decide if there is a good reason for it to exist.

- What is blockchain?
- What is Bitcoin?
- Does bitcoin have any value?

What is blockchain?

A ledger is a system for storing the records of who owns what. Your bankbook, showing all the deposits and withdrawals you've made, is a ledger of your account balance.[1] The collection of deeds kept by your local government is a ledger of who owns what real estate. The Depository Trust Company facilitates trading of financial assets by helping to create a ledger of who they belong to. You might consider cash itself to be a ledger, representing ownership of a theoretical currency in the background.

There are a lot of problems with traditional methods of keeping ledgers. An entire industry, title insurance, exists to interpret the real property ledger; you will pay one of these companies a lot of money when you want to buy a home.[2] Ledgers for some assets are kept on paper, with all the risks thus entailed. Those kept on a computer are susceptible to attacks of the digital kind. Banks have massive security measures in place against those who

[1] Because a lot of people still have bankbooks, right?

[2] Or at least if you want a mortgage against it. So far as I know, there is no legal requirement to buy title insurance, but every bank requires it in order to lend.

would access their ledgers, but it is easy to imagine an attack that created fictitious transactions, moving your money to the account of the attacker.

We can classify the problems of a traditional ledger into several categories:

- Centralization: If the ledger exists only in one place, it is impossible to differentiate real and fake transactions. Making a copy doesn't help; if one copy was altered, how would you determine the true ledger from the altered version? Also, there is little recourse against the centralization agency unilaterally modifying the ledger.
- Cost: As in the case of title insurance, traditional ledgers can greatly increase the cost of completing transactions. Your bank spends a fortune on data security; these costs are eventually passed along to customers.
- Trust: Traditional ledgers generally require asynchronous execution. For example, my book editor required half of her payment upfront, with the remainder on delivery. This required that I trust her not to walk away with the deposit; she had to complete the work, trusting I would pay for the balance.[3]

Blockchain was created to address these issues. Created in 2008, blockchain is a piece of open source software based on a brilliant mathematical foundation. It allows for the creation of digital ledgers. In theory, blockchain ledgers are completely decentralized, allow for low-cost transactions, and lack any central governing bodies in which participants must place trust. If this sounds revolutionary, that's because there is a real possibility that it might be.

Blockchain is not the first attempt at creating a digital ledger, but it is the first to solve the critical problem of **double spending**. Double spending is not an issue when using cash. If you have a $100 bill in your pocket, and spend it at the grocery store, you won't have the bill anymore and cannot spend it again. If you take $100 out of your checking account, the bank reduces your balance by this amount; if it was your last $100, the bank knows not to let you have any more money. In a decentralized ledger, it is far more difficult to prevent people from using assets they don't own. If I simultaneously put two transactions in the ledger, and the sum exceeds my balance, how do you know which transaction occurred first, and is therefore valid?

Blockchain solved this problem by introducing the concept of blocks. A block is a group of transactions that, with respect to the ledger, occur at the same time. All transactions in a block are checked against the ledger to be sure that the senders have the asset they are attempting to spend. If they do, the information for these transactions – sender, receiver, amount – becomes a valid block. Then, a bunch of computers run some really complex calculations on this block. The product of this work is to link the block to previous blocks via a code that is called a **hash**. Through the hash, each new block validates all previous blocks. In this way, the blocks form a chain.[4] As the chain is known to everybody in the blockchain network, there is no central authority and no need to trust other network members. The process of adding new blocks to the chain is called mining, for reason that will shortly become clear.

One obvious question arises: what if two different blockchain miners choose different blocks to add to the chain? This would create two different versions of the ledger. The blockchain protocol has an algorithm for determining which of two ledgers is the "best." Generally, the best chain is the one that is the longest. When a miner sees a chain that is better than the one on which it is working, it begins work on the new chain, and the old one is discarded. This miner will also send the new chain on to other members of the mining network. While it is theoretically possible to change old blocks in the chain, it is highly impractical to do so. Because blocks are linked by the hash, a miner attempting to alter transactions in a block would need to mine every following block, in order to be long enough to be viewed by the network as the valid chain. Given the massive computing power required to mine blocks, this is a practical impossibility. The blockchain ledger is secure due to the amount of work required to change it.

[3] For larger transactions we've developed elaborate schemes of escrow to minimize the trust required to complete transactions. Any escrow arrangement requires trust in whoever holds the escrow account.

[4] As usual, I'm taking liberties on the math for simplicity's sake. There are a lot of resources to give more accurate and complete descriptions of blockchain. I found Coindesk to have a nice overview. The genesis of blockchain was this white paper, written by the pseudonymous Satoshi Nakamoto.

What is Bitcoin?

Because the mathematics of blockchain is open source, with a little work, anybody can create their own decentralized ledger, processing any transactions their hearts might desire.[5] While its creators intentionally permitted anybody to use it, there was also a specific application for which it was created: the cryptocurrency Bitcoin[6].

Bitcoin is an instance of a blockchain ledger. It began with a "genesis block" showing the initial state of the ledger. This block stated the initial owner of every bitcoin. The owner of a bitcoin can transfer it by appending a signature, based on a secret code to which only they have access. Despite the secret code being impossible to reproduce, it is easy to verify.[7] The amount of bitcoin in the transaction is checked against the ledger to ensure that the sender has a large enough balance to complete the transaction. Verified transactions are included in a block, which is then connected to the chain via mining, as we described above.

But, who does the mining? In order to add a block to the chain, Bitcoin requires around 200 quintillion calculations.[8] Mining Bitcoin requires an enormous amount of computing power – nobody will do it for free. Miners are paid in two ways. First, those wishing to have their transactions mined into the Bitcoin blockchain can include an optional transaction fee. Miners are incentivized to prioritize the processing of transactions that pay the most fees. Second, miners who complete blocks are rewarded with a one-time payment in bitcoin. At the time of this writing, the reward is 12.5 bitcoins, worth about $100,000. A new block is added to the chain every ten minutes. Between rewards and transaction fees, there is around $20 million in daily revenues available to miners.[9]

Bitcoin was explicitly created to be outside the control of government regulations. Because they are based on an owner's private code, transactions in bitcoin are virtually anonymous. The creators of Bitcoin attempted to create a monetary policy for Bitcoin via artificial scarcity. The reward for new Bitcoin blocks will be halved every four years. Around the year 2140, there will be 21 million bitcoins in circulation; at this point, there will never be another bitcoin created.[10] According to Bitcoin proponents, the limited circulation will prevent them from experiencing inflation of the type that affects all other currencies. Because of this, they say, Bitcoin has enormous value.

Does Bitcoin have any value?

Let's talk about two words: worth and value. While they are often used interchangeably, they mean different things. Worth signifies how much somebody is willing to pay for something. If you can sell a Picasso for $100 million, its worth $100 million. If apartments in Manhattan have an average sales price of $1,800 per square foot, this is how much they are worth. If you paid $0.99 for a stupid, time-wasting mobile game, then the game was worth this amount.[11] We know that Bitcoin has a worth of the exact amount it is trading for right now on the various Bitcoin exchanges.

On the other hand, the value of something is related to its usefulness or desirability. An apple has value because you can eat it. A house has value because you can live in it, a car because you can drive it. A Picasso has value because people will pay to see it, and because it is aesthetically pleasing. Something can have value without being worth anything; the air you breathe is important, but nobody will pay for it. In the long term, it is difficult for an item to be worth significantly more than any value it has, as we know from Dutch tulips, internet bubble stocks and subprime mortgages.[12]

---

[5] Please seek advice from legal counsel before doing so.

[6] As an aside, the rules for capitalization of Bitcoin/bitcoin have nearly driven me to distraction. I've tried to say Bitcoin when referring to the system or technology behind the currency and bitcoin when referring to an amount of the currency. I always capitalize Bitcoin mining. If you disagree with my choices, feel free to start your own blog dedicated to the issue.

[7] Think of this like a physical signature. It is very difficult for me to forge your handwriting and sign checks in your name, but easy for me to see that your signed check matches the signature on your driver's license or passport. This principle is also why we use fingerprints or retinal scans as a security device. It is simple to verify that a thumbprint is yours, but fiendishly difficult to recreate the print without your thumb.

[8] Remember that the security of the chain is based on the difficulty of its computation, making this enormous number a feature of Bitcoin rather than a bug.

[9] This is, of course, highly dependent on the price of bitcoin. At the time of this writing, 1 BTC = $8,335.

[10] Meaning that after this point miners will be paid only via transaction fees.

[11] This worth is dubious, because there is no way to sell the game to somebody.

[12] Yes, these all have some value, but their worth greatly diverged from any reasonable idea of how useful they were, causing their owners to lose money.

Currencies have been a part of human society for at least 3000 years. They have existed in many forms, from early coins with intrinsic value, to gold-backed banknotes, to today's "fiat currency", to the enormous Rai stones used by Micronesian cultures. Currencies are useful for two things: as a means of exchange and a store of wealth. A currency lacking either of these will have suspect usefulness; a currency lacking both is hard-pressed to have any value.[13]

On both of these tests, Bitcoin fails. Rising from a price of approximately zero to be worth $20,000 does not make Bitcoin a store of wealth. Even forgetting that it is now worth a wee-bit less than its peak, a currency that rapidly increases in value is little better than one that rapidly decreases. A merchant who purchased inventory one year ago would have no chance of selling it for as many bitcoins as it cost. Somebody who borrowed $100 in Bitcoin in late 2010 might now owe $8,000,000. This is obviously infeasible.[14]

Bitcoin proponents might argue that current fluctuations are simply the result of the currency being new; as it matures, they expect it to become more stable. They will add that the artificial scarcity inherent in Bitcoin will limit its inflationary tendencies, as opposed to virtually all other currencies.[15]

The artificial scarcity argument for Bitcoin having value is weak. The problem is that creating new cryptocurrencies is surprisingly easy. There are hundreds of them out there. Some, like Ethereum, are serious attempts to create blockchain-based currencies that address Bitcoin's flaws. Others, most famously Dogecoin, are intentionally created as jokes.[16] The point of this is that, because it is fairly easy for me to create a new cryptocurrency – or 1,000 new cryptocurrencies – if these currencies had value, then I would be able to create arbitrary amount of wealth for myself. As nice as this sounds, it seems more likely that my coins would all lack value.

But, maybe, Bitcoin is special. Maybe it has features that give it more value than the 435 new coins that were created in 2017.[17] Which goes to its usefulness as a means of exchange. As of July 2017, precisely three of the top 500 internet retailers accepted Bitcoin. The trend is not good; five retailers were accepting it one year ago.[18] If Bitcoin were truly special, and had value as a means of exchange, we would be seeing growth in its acceptance, not retreat.

There are a number of reasons why Bitcoin isn't accepted by more retailers. As we saw above, Bitcoin miners are earning $20 million per day; high transaction fees limit where Bitcoin can be efficiently used. In addition, there are real concerns about the societal cost of Bitcoin mining. The competitive nature of mining contributes annually an amount of carbon dioxide to the atmosphere equivalent to 1,000,000 transatlantic flights. Other payment processing systems also require energy, but Bitcoin is often not cheaper or simpler than credit cards. And if Bitcoin's price increases, the rewards for mining it would increase as well. Bitcoin's success would just create more prospective miners, chasing meaningless random numbers with their specialized computers, an activity ultimately unproductive to society.

For these reasons, my opinion is that Bitcoin – and cryptocurrencies in general – have virtually no value.[19] But, enthusiasts ask, if Bitcoin has no value, then why should government-controlled currencies have value? After all, governments can print as much of this paper as they wish. Historically, all currencies deflate over time.

There is, however, one big difference from bitcoins that results in dollars having value: the U.S. government will

[13] In other words, there is a good reason why Rai stones, which can weigh more than four tons, are not widely used.

[14] I know some bitcoiners talk about bitcoin as the currency of value. If everything was denominated in bitcoin, the issues around borrowing and lending it would be fewer. However, no asset has maintained a constant price in bitcoins during its rise and fall. Merchants who accept it have regularly changed prices based on bitcoin's exchange rate with dollars. Also, people who claim to have no concern about bitcoin's decline tend to be those who celebrated its previous rise. If their lives were truly based in bitcoin, they should have little cause to celebrate its appreciation against the maligned "fiat currencies."

[15] Just like with the gold standard, this scarcity means that monetary policy options would be highly limited for a nation using bitcoin as its primary currency. While modern currencies are imperfect, they produce more stable economies than those based on gold did in the past. It just makes no sense that a country should have an amount of currency in circulation no more than the number of shiny bars in its Fort Knox. In my opinion, the Increased ability and willingness of countries to allow for monetary intervention is an underappreciated cause of the global prosperity of the last five decades.

[16] The fact that Dogecoin is worth something is not a point in favor of cryptocurrencies.

[17] These new coins raised $5.6 billion in their initial coin offerings.

[18] See here.

[19] As always, these personal opinions should not be treated as an offer or sale of any securities products.

always accept them for payment of taxes. And we all have to pay taxes. Therefore, even if they served no other purpose, dollars would be a store of wealth (usable to eliminate tax liabilities) and a means of exchange (transmission of tax payments). No nation will last forever, but unless you think the United States is going away before your taxes are due, you will need dollars to pay them. This gives them immediate value.

As soon as one large, long-lived player agrees to accept dollars, their value propagates through economy. People will accept the paper currency in exchange for goods and services. They are happy to accept dollars, knowing that they will always have at least one use for them.

Determining that gold has value is trickier. There are various industrial uses for which it is the best-suited material but given the amount of gold that has been mined in human history,[20] the amount of gold needed for industry give it a value equal only to a fraction of what it is worth. To gain the rest of its value, we need to go back to our previous example of the Picasso painting. Aesthetic value is real value. Now, beauty is in the eye of the beholder, and maybe you don't like Picasso. But the vast majority of people from the vast majority of societies for nearly five millennia have desired gold for its use in decorating people and other objects. If you want to bet against this continuing, be my guest. I don't invest in gold, but I don't doubt that it has value.

There is, of course, an elephant in the room. One of the benefits of creating a currency outside of the confines of governmental support is that it can be used for transactions that run far afoul of governmental regulations. For those wishing to move large amounts of wealth outside of the prying eye of law enforcement, Bitcoin has already become a go-to currency for all types of organizations of ill repute. Drug traffickers use Bitcoin, as does organized crime. Armed militias and terrorist cells use Bitcoin. The rogue nation of North Korea is rumored to be a large holder.

Using similar logic by which governments guaranteeing acceptance for taxes propagates the currency through the economy, the prevalence of Bitcoin in the black market could cause Bitcoin to have value. If Boko Haram is willing to accept Bitcoin, perhaps local merchants should be as well. But I can't imagine crypto enthusiasts are sanguine about their currency's foundation being foundationally based on acceptance by Boko Haram. If this were the case, then every transaction in Bitcoin is directly supporting terrorists.[21]

Governments won't let this go on forever. If it becomes clear that the only real use for Bitcoin is in illegal transactions, responsible regulators will find ways to make it less efficient for such use. Because of its anonymity, it would be difficult for the authorities to confiscate your bitcoins. It would, however, be easy for them to stringently regulate those who would transform bitcoins back in to fiat currency. If no financial institutions – neither global mega-banks nor storefront money-changing stands – were able to give usable currency in exchange for bitcoins, it would cease to be a store of value. If merchants, who have no choice but to fit inside some types of government regulations, are prohibited from accepting Bitcoin, it would cease to be a means of exchange.[22] If Bitcoin becomes the exclusive currency of the underworld, it will become a victim of its own "success".

Bitcoin's mining economy has also put its vaunted decentralization-based security at risk. As Bitcoin mining has become more sophisticated, the barrier to entry has forced miners to get bigger. No longer can you run a small rig from your basement and hope to mine the occasional block. Satoshi's dream of millions of miners has become his nightmare of several large mining pools dominating the network. Today, four large mining pools control about 60% of global mining capacity. All four are based in China.[23]

Blockchain's security is based on competition. Blockchain mining with collusion is fatal to the integrity of the chain. Even the potential for collusion should greatly erode trust

[20] So far, humans have probably mined around 175,000 tons of gold, although we don't know for sure. Because gold is seldom lost, and never destroyed, humanity has approximately this amount currently in our possession. It would fit into a cube approximately 20 meters on each side.

[21] And the analogue works: every time I accept dollars as an item of value, I am supporting the U.S. government. Even in the age of Trump, I'm OK with this.

[22] Even if not prohibited, requiring documentation of large bitcoin-to-currency transactions would severely curtail its usefulness. Such regulation already exists for large currency transactions, for example withdrawals of over $10,000 from U.S. banks.

[23] Going further, about 15 pools control over 90% of capacity between them. Some of these are located outside of China.

in the system. Blocks go into the chain are based on the consensus of the network. If over 50% of the network agreed to include a fictitious block, into the chain it would go. The colluding miners could spend their own bitcoins multiple times or transfer any bitcoins to their own accounts. Obviously, concentration of miners increases the likelihood of such collusion. As far as I know, there is no defense against this type of attack by a group of miners with enough power.

Even if Bitcoin is unlikely to be the future of money, blockchain can still have value as a backbone of other ledgers. Corporations, from mega-banks to technology firms to consultants, are investing in blockchain startups, blockchain systems, blockchain applications and more. It has the potential to improve efficiency in many areas of record keeping. If property deeds were maintained in a blockchain, the cost of title insurance might be a fraction of what it is currently. Banks, spending billions on transaction clearing and reconciliation, salivate at the potential savings. And the concept of distributed ledgers, built off the concepts of blockchain (and Bitcoin) will only improve over time. Flaws will be addressed, new applications developed, and lessons of scams and breaches will be learned. Even if the blockchain's intended application does not obviate the need for legitimate currencies, its underlying structure might change its small piece of the world.