So just what the hell is Bitcoin anyway?

by Isaac Dimitrovsky, July 2018

- A bunch of smart but non-technical people have recently, in strictest confidence, asked me just what the hell Bitcoin actually is. In response I wrote the article below.
- This article is exactly what you need to fix your current predicament where everyone's talking about Bitcoin and you're nodding wisely but hoping nobody calls on you.
- It should be understandable (with some effort) even by non-technical readers, and if you understand it you should have a reasonably good idea of what Bitcoin is.
- Plus, it just might have some relevant information if you're interested in Bitcoin as a trade or investment.

The usual introduction to Bitcoin starts with an attempt to explain the method that makes it work internally, which is called blockchain. But that would probably require some equations, and the usual rule is that each equation costs you half your non-technical readers. So, I'm going to start in a different way, with a completely imaginary construct that I'll call Bobcoin.

Imagine you had a neighbor Bob that everyone considered completely trustworthy. One day, while you're having a couple of beers with Bob in your basement, he tells you about this idea he has for Bobcoin. The way it works is, when someone new wants some Bobcoins, they call Bob up on a secure line. Bob then goes into a locked bugproof room in his basement and generates two random 20-digit numbers by rolling dice a bunch of times. Bob gives the two numbers to the person who wanted the Bobcoins. The first number is going to be the person's public ID for future Bobcoin transactions, and the second will be his password by which he can authenticate himself to Bob. Therefore, Bob warns him to keep that password secret and not to lose it, since it's the only way to access his Bobcoins. As long as he does keep it secret and Bob remains trustworthy, it would be almost impossible for anyone else to discover the number since it's so long and random.

Bob writes the two numbers on a new page in the Bobcoin book that he keeps in a secure safe in his basement. Bob then accepts payment for the number of Bobcoins (say, 100) the person wants, and makes a note on the new person's page that he's now the proud owner of 100 newly minted Bobcoins. Note that one of the forms of payment Bob accepts is cash left in a brown paper bag on his front porch, and therefore the new Bobcoin owner can stay anonymous if desired.

What about when a return customer wants some more Bobcoins (say, 50 more)? He can skip the first steps and just give Bob his password. After Bob finds the page with that password in the Bobcoin book, he accepts payment for the new Bobcoins, and makes a note recording that the customer now owns 50 more newly minted Bobcoins. Again, the customer can be anonymous if desired since Bob is just given the password and payment.

What about when someone wants to transfer some Bobcoins (say, 50) to someone else (presumably in exchange for payment or for some good or service)? He tells Bob that he wants to transfer 50 Bobcoins to the other person. He authenticates himself to Bob by giving his password, and he specifies the person to transfer to by giving Bob that person's public ID number. Bob looks up all the numbers and checks the transaction is valid, and then makes notes on the appropriate pages in the Bobcoin book that the first person now owns 50 fewer Bobcoins, and the second person now owns 50 more. Again, this transfer could be anonymous since Bob is just being given the password and public ID numbers to specify it. Note that this method of transferring Bobcoins enables holders of Bobcoins to sell them back and forth to each other, creating a market in which the value of Bobcoins would fluctuate depending on what people were willing to pay. As is the case for other assets like stocks and options, exchanges could then be established to make trading in Bobcoins more secure and convenient.

Finally, recognizing that in the setup described so far Bob could issue an unlimited number of Bobcoins, Bob solemnly commits to issuing a total of no more than 21 million so that they will retain their value.

So far, you find Bob's idea far-fetched but kind of an interesting thought experiment, or at the least a welcome break from debating whether Game of Thrones went downhill after they introduced zombies. However, Bob then tells you he's planning to set Bobcoin up as an alternative asset class and since you're friends he'll reserve a thousand Bobcoins for you for just a dollar apiece. At this point you understand Bob is actually serious about this sh*t, realize he has lost his mind, and start smiling uncomfortably while making a mental note not to lend him any more of your power tools. And then you forget all about it until last week, when you fall into a deep depression after seeing Bobcoin has just hit $7,000.

OK - now back to reality, and the punchline. Believe it or not (and I'm guessing not), **what Bobcoin does is pretty much all that Bitcoin does**. That is, it keeps track of the ownership of some units of an entirely imaginary and intangible item, in such a way that owners can stay anonymous, and also can, if they want, transfer some of those imaginary items to other owners. The one significant thing that distinguishes Bitcoin from Bobcoin is that **it doesn't require Bob**. In other words, it doesn't require a trusted central authority to keep track of the ownership of those imaginary items. Instead, Bitcoin uses a couple of clever ideas in order to keep track of ownership using the collective action of a bunch of computers scattered around the world. ***Side note 1:*** *This may explain Bitcoin's strangely intense appeal to Silicon Valley libertarians like Peter Thiel. The combination of eliminating a trusted central authority, which libertarians generally consider the greatest evil facing the world,* ***and*** *using a cool software technique to do so, must have hit those Silicon Valley guys like opium-laced catnip.* ***Side note 2:*** *A couple of people, upon reading the above, have asked me why the hell anyone would buy an imaginary asset. I believe the two main reasons are: A) Because they believe*

they can sell it later for a higher price, and B) Because a certain group of people really wants a form of payment that is anonymous, untraceable, and irreversible – I'll leave it as an exercise to figure out who's in that group.

This concludes my explanation of what Bitcoin actually is; I'll wrap things up with a little more information about those two clever ideas that are used internally to implement Bitcoin. The first clever idea, called blockchain, is the mathematical technique that enables that collection of computers to replace Bob in the system above and keep track of those imaginary items. The interesting and surprising thing is that this can be done in a pretty robust way by an ad-hoc collection of computers that are directed by their owners to participate (I use "robust" here in the computer security sense, meaning resistant to computer failures and attacks by hackers). Note: the blockchain method could also be used to track ownership of tangible assets like real estate, possibly more efficiently than current methods for doing so. However, in the case of Bitcoin and most other so-called cryptocurrencies, the "asset" being tracked is completely imaginary. I would say it was conjured up out of thin air, except that thin air actually seems considerably more tangible to me.

Note: the next paragraph is strictly for extra credit. Read it only if you want to fully commit to the red pill – if you proceed, you might end up knowing more about Bitcoin than those people you hear talking about it! For completeness, I'll add that blockchain, while clever, is by no means flawless. For one thing, it seems almost perversely designed to consume vast amounts of electricity. This happens because, as part of the blockchain process, the computers involved must submit something called a "proof of work" that demonstrates they have done a large amount of computing on a particular problem. Since all practical computers run on electricity, this effectively means using large amounts of electricity – electricity that could otherwise be used to synthesize drugs, smelt aluminum, power streetlights, or any number of other tangibly useful activities. Another caveat is that blockchain appears resistant but not impervious to hacker attacks. In fact, blockchain is known to be vulnerable to something called a 51% attack that seems difficult but not impossible to pull off. While Bitcoin itself hasn't been subjected to this kind of attack yet, other systems that use the blockchain method have been. Also, even if blockchain itself isn't compromised, hackers can attack Bitcoin by gaining control of the computers used by Bitcoin owners or the exchanges used by owners to help them trade Bitcoin – this can be done with standard hacking techniques like Trojans.

The second clever idea behind Bitcoin doesn't get as much appreciation as blockchain, but to me is actually the cleverest bit of Bitcoin. As you may recall, blockchain uses a vast amount of electricity, which gets quite expensive. Therefore, the collection of computers that maintains the underlying blockchain for Bitcoin probably couldn't operate without compensation. So how does all that computer power get paid for? In a rather jaw-dropping bit of circularity, what happens is that those computers are paid for maintaining Bitcoin – in Bitcoin! That is, in

exchange for the computing work of maintaining Bitcoin, the owners of those computers are themselves rewarded with some newly minted Bitcoins. This is the origin of the term “Bitcoin miner” to refer to the computers that maintain Bitcoin. And, that entrancing bit of perpetual motion machinery seems like as good a place as any to … stop.