The Age of Cryptocurrency- How Bitcoin and Digital Money Are Challenging the Global Economic
Paul Vigna

Major implications not only for currencies, but for the management of all life's transactions. This you have to know The authors of this book are reporters, and as a piece of reportage it is broad, deep, and well-balanced. They take you through the history of bitcoin, the alternatives to bitcoin, all the technology behind bitcoin, and extended uses for this disruptive technology which could have wide implications throughout society. They provide a broad discussion of the projects underway in 2014 to employ bitcoin.

If the book has one shortcoming, it does not define how it all works quite precisely enough for a techie. The reader of this review may find it useful to mix my point of view with that of the book itself in trying to envision the mechanics.

The casual reader is somewhat familiar with the bitcoin phenomenon. It appears to have been started by a single idiosyncratic individual calling himself Satoshi Nakamoto but whose identity remains unknown and who dropped out of sight some three years ago. What this gifted technician did was to envision the architecture of an entire system, implement that system, find a group of disciples, fanatics if you will, to carry it on, and then quietly disappear. This is truly the stuff of science fiction

The thing that he invented is the thing that is most difficult to describe. Here I go in my own words, rearranging some thoughts from these authors.

The first question is what a currency is. We are familiar with fiat currencies such as the dollar the euro and the yen. We are familiar with the fact that these have all evolved from metallic representations, such as silver dollars and $20 gold pieces, to paper certificates indicating that metal was once held in storage to back them up, to fiat currencies which have nothing whatsoever behind them. The dollar today is an artificial construction, a unit of exchange.

Actually, what every currency must be is three things. It must be a unit of exchange, something that can be offered in exchange for goods or services. It must also be a store of wealth, so that today's labor can be converted into currency and stored to be spent later. Or vice versa, it can be borrowed against future earnings. The third measure is a unit of account. Everybody has income stated in some currency or another. You may make $2,000 a month and have a net worth of 700,000 Francs. Businesses especially need such a measure of their performance.

That's what currencies are. They have different strengths and weaknesses. Gold his difficult to carry and safeguard and doesn't come in small denominations. Fiat currencies are imminently bankable, they can be moved around electronically with great ease. However, they are subject to counterfeiting and inflation. The counterfeiter can create false paper money, and a financial manipulator or central bank can arbitrarily dilute current holders, expanding the money supply by creating dollars out of thin air. Moreover, the rapacious bankers scrape off a slice of every transaction, from 3% on a typical credit card transaction to 10% and more on international remittances. No currency is ideal.

One characteristic that all traditional currencies have had is that they are fungible. If I have $1,000 in the bank, I could not possibly say who previously owned those dollars. It's a silly question even to ask, like asking what happened to a raindrop falling into the ocean. Even the tangible stuff like the pennies in my pockets carry no history with them.

I make an analogy that the authors do not: to real estate. Real property is recorded by a registrar. The fact that I own my house is known to the state and it is public information available to anybody. Not only that, but who I brought my house from, and who they bought from, is a matter of public record. How the land my house sits on was defined is public record. It was probably subdivided from some farm back in time. Thus, where land records are complete, there is a chain of ownership reflected in land records that guarantees the authenticity of a title.

This is the most essential difference between bitcoin and other currencies: a perpetual chain of ownership. There is a permanent record electronic record of every past owner of every particular coin or fraction thereof, and of every transaction ever completed within the system.

The implications of being able to trace the history of every transaction in which a piece of money has been involved are extremely broad. It means that there can be no question as to the validity of a transaction. Unlike with a bank,

there cannot be an overdrawn account. If the money isn't there, the transaction is not accepted. If it is, the transaction is final. Unlike paper money you cannot have counterfeit. Unlike a Federal Reserve System you cannot have $85 billion created every month out of thin air. The whole bitcoin universe knows where every piece of money came from.

The bitcoin concept ,which is called the block chain concept is revolutionary in that sense. There is a publicly available record of every transaction ever done within the system going back to Nakamoto's genesis block.

Every account is identified only by a number, a large one at 25-36 alphameric characters. The accounts are anonymous and password protected. Lose the password and the money is gone. There is no bureaucracy to help you out. Password length is up to user discretion, but the longer the better.

It raises questions of control - who owns the system, and how is new money introduced, if it is at all. Lastly, and most importantly, it raises the technological question. How do you do that? The answer to the latter is called the block chain.

The block chain works by hashing technology. Let's take an example.

The letters in this paragraph can be interpreted as a number. A very large number, and very likely to be different from any other paragraph even in a large manuscript.

Here is a table of the ASCII (internal) representations of the letters in the above paragraph. If you add up the values of the individual letters you get 15,050, a fairly large number. But if, just for instance, you interpret each string of six letters as a (12 place hexadecimal) number, and add those up, the result is huge: 5,642,316,386,171,830. That's five quadrillion, larger than the national debt measured in pennies. The probability that it is unique is extremely high. There is almost no way I could fiddle with the text in the paragraph without throwing the hash total off. Rest assured that bitcoin uses bigger numbers and a more sophisticated scheme than I show here.

T 84 h 104 e 101 <sp> 32 l 108 e 101 t 116 t 116 e 101 r 114 s 115 <sp> 32 i 105 n 110 <sp> 32 t 116 h 104 i 105 s 115 <sp> 32 p 112 a 97 r 114 a 97 g 103 r 114 a 97 p 112 h 104 <sp> 32 c 99 a 97 n 110 <sp> 32 b 98 e 101 <sp> 32 i 105 n 110 t 116 e 101 r 114 p 112 r 114 e 101 t 116 e 101 d 100 <sp> 32 a 97 s 115 <sp> 32 a 97 <sp> 32 n 110 u 117 m 109 b 98 e 101 r 114 . 46 <sp> 32 <sp> 32 A 65 <sp> 32 v 118 e 101 r 114 y 121 <sp> 32 l 108 a 97 r 114 g 103 e 101 <sp> 32 n 110 u 117 m 109 b 98 e 101 r 114 , 44 <sp> 32 a 97 n 110 d 100 <sp> 32 v 118 e 101 r 114 y 121 <sp> 32 l 108 i 105 k 107 e 101 l 108 y 121 <sp> 32 t 116 o 111 <sp> 32 b 98 e 101 <sp> 32 d 100 i 105 f 102 f 102 e 101 r 114 e 101 n 110 t 116 <sp> 32 f 102 r 114 o 111 m 109 <sp> 32 a 97 n 110 y 121 <sp> 32 o 111 t 116 h 104 e 101 r 114 <sp> 32 p 112 a 97 r 114 a 97 g 103 r 114 a 97 p 112 h 104 <sp> 32 i 105 n 110 <sp> 32 a 97 <sp> 32 l 108 a 97 r 114 g 103 e 101 <sp> 32 m 109 a 97 n 110 u 117 s 115 c 99 r 114 i 105 p 112 t 116 . 46

The take-home point is that a large volume of text can be (very close to) uniquely vouched for by a fairly compact number. If I changed any letter in the paragraph the number would change, indicating that the paragraph had lost its integrity. This device is called a hash total. Bitcoin uses hash total schemes, though certainly much fancier than this one, throughout.

Every transaction document can thus be represented uniquely enough for bitcoin's purposes by some string of numbers. It takes a large number, but one which is very small in comparison to the original document for which it vouches.

Bitcoin is capable of processing about seven transactions per second. It batches them every ten minutes. Each batch would thus contain fewer than 7x60x10 = 4200 transactions. The 4200 hash totals would themselves be combined into a hash. Most importantly, this hash also includes the hash from the previous batch, which has in the intervening ten minutes been vetted by a "proof of work" concept, authenticated and accepted by the electronic voting process of the bitcoin community. These summary hashes, combined with the backwards links in the block chain, knit together every transaction in the history of the bitcoin universe.

A little arithmetic (mine, not the authors') demonstrates that the data volumes are well within the realm of modern computing. If documenting each transaction took 10kb, with 400 transactions/minute over five years, the total database would be 10 terabytes. That is not a frightening number. It is highly conceivable that many sites could keep

the replicated copies of this data necessary for the integrity/voting process. The active data, the recent transactions and wallet/account balances, could be much smaller. Presumably, though it is not discussed, there is some kind of a tiered scheme, so as not to waste too much resource storing inactive data.

The block chain serves two functions it guarantees the integrity of the system and it makes it compact enough that there is a way to work with it. The people who need to see the original transactions can look at the particular block in which they occurred, but most users who are not affected by historical transactions only need to deal with blocks that involve their activity. However, the information is widely enough shared that its integrity is insured.

This hash total functioning, and in fact almost all of the operation, is highly encrypted using public key cryptography. For a good description, see Nine Algorithms That Changed the Future: The Ingenious Ideas That Drive Today's Computers.

The there is a concept of "bitcoin mining" which is fundamental to the process. The mining involves the hashing process. In my simplistic example I said that we will digitize the representation of six characters and interpret the group as a large number. But in fact bitcoin uses much more complex algorithms, and the algorithms involve a variable part, a very long and unique number which is derived by an excruciatingly difficult series of computations. That bitcoin mining process involves coming up with the next suitable number. It is so computing-power intensive that one of the concerns about bitcoin is the carbon footprint that the computers executing bitcoin hashing algorithms use. Read the book to understand the difficulty. In any case understand that it is highly encrypted and robust against fraud. What fraud has occurred in bitcoin is due to human error rather than any architectural flaws.

Going back to the book the authors do a good job of reporting the early days of bitcoin and then surveying how it is used today. It is still a minor player in the financial transactions field. They observe that bitcoin can only handle 7 transactions per second versus the 10,000 or so that Visa is structured to manage. It is several orders of magnitude different. In order for bitcoin to emerge as a competitor with the big financial houses, its architecture may need to be rethought.

Bitcoin has been too unstable to serve as a store of wealth that allows one to sleep well at night. Its value rocketed from pennies up to over $1,000 and back down to the low hundreds. Presumably as it becomes more accepted the currency will achieve more stability.

Many people are concerned that a bitcoin itself has a no substance. There is no inherent value in this bunch of bits. The counterargument is that this is equally true of fiat currencies, and bitcoin has the benefit of scarcity. The original architecture of bitcoin calls for the introduction of new bitcoins as reward to the miners who come up with the new block total hashing numbers. As they become harder and harder to generate, it has resulted in the massive computer power and carbon footprint mentioned above. But the number of bitcoins to be eventually generated was specified at the very beginning and is strictly limited. So inflation is not going to be a problem with bitcoin. In fact, deflation is much more likely to occur. As the value of the coins goes up, the cost of things in bitcoins will go down.

Deflation works against governments, which depend on inflation to progressively hike people's tax brackets and things like that. How governments deal with bitcoin is an interesting question into which the authors delve at length. Bitcoin is difficult to control difficult to tax difficult to understand and difficult to define legally. The authors do a good job of examining all of these aspects.

The authors display a liberal bent. The thing that gets them most excited is that bitcoin may be a way to bring banking to that majority of mankind who do not currently have bank accounts. Such people are simply not worth the effort for banks to serve. Bitcoin transactions can be executed over telephones, not even smart phones. The authors look for entrepreneurs to make it work in the less-developed corners of the world. This sounds a bit idealistic, but one must recognize how idealistic it seemed only two decades ago to bring cell phone service to the same people. Now it is ubiquitous.

Blockchain technology could be used to track other kinds of titles. Land records are subject to fraud in many parts of the world. Bribe the right judge and he will change the paper land records, depriving you of a property right. A blockchain approach to land records would make it impossible. It could also make bribery more visible. Conversely, as has already been seen, the anonymity of bitcoin is a boon for drug dealers and money launderers.

Bitcoin is truly a transnational, borderless system. The authors talk about its attraction in a place like Argentina that has not had a reliable currency since Juan Peron in the 1950s. The currencies in many other parts of the world are under pressure right now. I have seen the value of my currency, the hryvnya, fall by 60% over the last year. Bitcoin could be a store of value. More important, it can serve as a medium of exchange among countries where the currencies are not functioning and are not easily exchangeable. The banks are controlled by governments, whereas bitcoin is out on its own. Therefore when the governments decree that you cannot change pesos or rubles or whatever the fiat currency is into something more attractive, bitcoin seems to offer an alternative. It would simply bypass the system. Governments are working hard to control it, and there is a question of how effective they will be in doing so given that anybody with a computer has the ability to work with bitcoin. The problem seems to be in the exchanges, going back and forth between bitcoin and fiat currencies.

This a long review. Let me close in saying that this book will give you an insight into the modern financial system and a good appreciation of bitcoin, which may represent the most serious intellectual challenge to the structure of finance, both national and international, to arise within the past couple of centuries. It is absolutely worth reading.