

CSS
INDEPENDENT
STUDY 2020

Bitcoin

THE BEST DIGITAL CURRENCY
THAT NO ONE KNOWS ABOUT



By Charlie Russell

CONTENTS

03	INTRODUCTION	15	BITCOIN FUN FACTS
04	BITCOIN PAPER	16	QUOTE FROM RJ HERRICK
13	BITCOIN GAME	17	RECOMMENDED YOUTUBE VIDEOS
14	BITCOIN CHARTS	18	CONCLUSION



Introduction

Have you heard of bitcoin? Probably not. The concept of bitcoin is so overly complex that many people just can not comprehend it. The reason I chose bitcoin as my topic is that I wanted a complex topic and I wanted to try to understand it. The reason that bitcoin is related to sustainability is that bitcoin has a more secure and easy system than modern money. Therefore, it is sustainable. However, this does not mean that it is better for the environment. I am still wondering why bitcoin has to use so much energy to function, that is why it is bad for the environment. I am very proud of all my work to understand this complex topic. Now you have the opportunity to understand it. Let's put you to the test.



BITCOIN EXPLAINED

By Charlie Russell

Introduction

Did you know that \$160.4 billion dollars worldwide are in the form of a cryptocurrency called bitcoin? A cryptocurrency is a currency that only exists online. Many people believe that cryptocurrencies like bitcoin represent the future of our monetary system. If you would like to know more about bitcoin and cryptocurrencies, read this paper. It is divided into five main sections: the invention of bitcoin, what is bitcoin, how it works, the pros and cons of cryptocurrencies, and other things you need to know about bitcoin and cryptocurrencies.

The Invention of Bitcoin

In 2008 there were no cryptocurrencies in existence. But a mysterious inventor who goes by the pseudonym Satoshi Nakamoto had big plans. In 2008 Satoshi wrote a paper called "Bitcoin, a Peer-to-Peer Digital Cash System." It was no coincidence that bitcoin came about in 2008. That year, the world was going through a financial crisis that caused a lot of people to question the practices of the traditional banking system. It was during this crisis that bitcoin was created. Part of the reason bitcoin was invented was to help prevent a financial crisis of this kind from happening in the future. There is also renewed interest in bitcoin in 2020 as we are potentially experiencing another global financial crisis like the one in 2008.

Back to Satoshi Nakamoto: After he (or she) published that paper, they went missing. To this day, we still have no idea who the creator of bitcoin is. Some of the evidence points to Craig Wright, an Australian computer scientist, or Dorian Nakamoto, a Japanese software designer, as being the mysterious inventor, but so far there has been no definitive answer as to who Satoshi Nakamoto actually is.

What is Bitcoin?

Bitcoin is the first cryptocurrency ever invented and it is decentralized. You probably don't understand a word I just said!

Let's start with cryptocurrency. You already know that a cryptocurrency is a currency that only exists online. Bitcoin is the most famous cryptocurrency, but there are others out there, like Ethereum and Litecoin. In this paper, I will be focused on bitcoin because it is the most well-known. The main reason bitcoin is the most well-known is that it was the first available cryptocurrency.

What does decentralized mean? You probably know something about how banking works. If you don't, here is the big idea -- banking is centralized. With a centralized currency, you have to rely on something or someone, like a bank, to keep your money safe. With a decentralized currency like bitcoin, no one relies on anything, and there is no central authority managing it because it is all done by a computer. That makes it safer because there is no one who has too much power. Bitcoin has a lot of benefits, but it also has some disadvantages. You can learn more about those in the "Bitcoin Pros and Cons" section.

How Does Bitcoin Work?

Now that you know what bitcoin is, let's dive into how it works. First, you need some background information. Bitcoin is backed by blockchain technology and uses cryptography to keep its network safe. Cryptography is the art of writing or solving codes. It uses public keys and private keys to make sure that the transaction is accurate and secure. The way those keys work is when someone plugs in the public key, they can figure out if the transaction was signed by the correct private key.



Sending a Transaction

Say that Bob wants to send some bitcoins to Fred. Bob writes his account number, which looks something like this 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2 along with Fred's account number (which also looks something like this) on an empty transaction. An account number is different from a public or private key. The account number is only used when you want to clarify who you are sending bitcoins to. Next Bob puts in the number of bitcoins that he wants to send to Fred. Then he signs the transaction with his private key and links his public key to the transaction. Finally, he pays a fee (usually around 50 cents) to send the transaction. The reason for a fee is to encourage the miners to choose your transaction over other transactions (explained in the "Bitcoin Mining" section). Once the transaction is sent, it goes into the unconfirmed transaction pool, also called the mempool, and waits until a miner comes along and puts it in a block.



Bitcoin Mining

Bitcoin mining is the process of computers solving complex math problems generated by the bitcoin system. Miners solve these problems. Miners are both computers and people. The computer does the real mining, but it is monitored by real people. Miners are sent a copy of the blockchain so they can accept and decline transactions. The blockchain is a ledger with all the blocks ever accepted (I explain more about that below). When a miner solves the problem, also called mining a block, 6.25 bitcoins are awarded to that computer owner's bitcoin account. These bitcoins are randomly generated and put in your account; no real person is paying them. Then the miner picks all the transactions with the highest fees out of the unconfirmed transaction pool, and those fees get sent to that computer owner's bitcoin account. The transactions that the computer picked get put into the block, and that block is confirmed by all the other miners' computers. The way the other miners confirm the transactions is by running the program with the public key that is linked to every transaction. If the public key works, that is proof that the transaction was signed by that person's private key, which makes it valid. If all the transactions are valid, then the block becomes part of the blockchain, and that updated blockchain is sent out to all the miners.

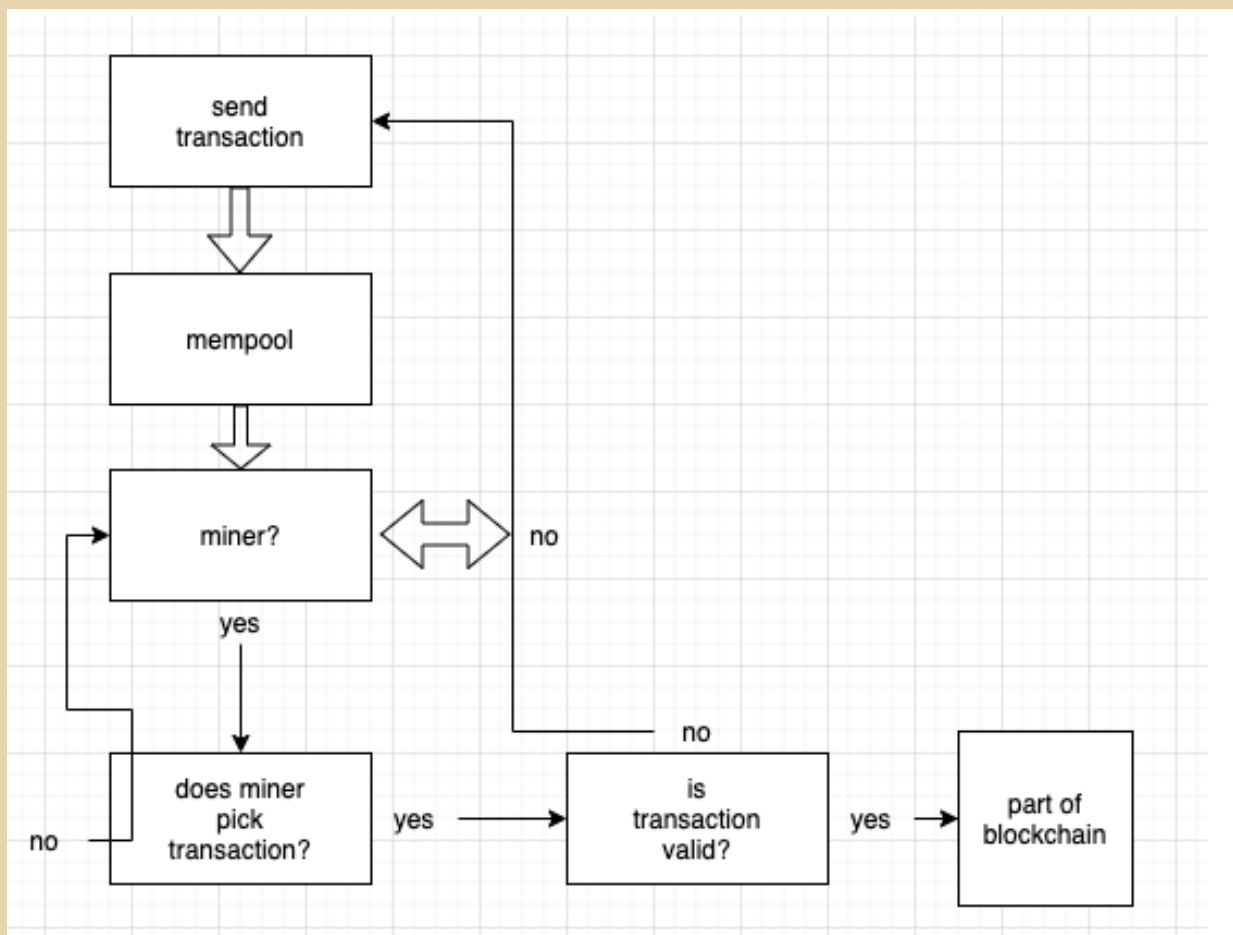
Mining Energy and Mining Farms

The reason people mine for bitcoins is the reward. 6.25 bitcoin is currently equal to about \$62,500. All around the world, people who are interested in making money with bitcoin have made 'mining farms' that use super-powerful computers called ASICs (Application-Specific Integrated Circuits) to mine bitcoins. The problem with bitcoin mining is that ASICs use a huge amount of electricity to run, so if you're not careful, your electric bill will be sky-high and the environment will suffer. For this reason, mining farms are usually made in places where the electricity cost is very low. The total power usage for bitcoin mining worldwide is 64.15 terawatts of electricity per year. Switzerland, by comparison, only uses 58.46 terawatts of electricity per year for the entire country.



Recap and Flowchart

The sections above explained the basics of how bitcoin works. If you still don't get it, don't worry. Only 0.8 percent of the population knows how it works! If you're now saying, "I want to be in that 0.8 percent!" then you should go back and read "How Does Bitcoin work?" again. Or if that was too long for you, you can read this recap. Let's go through the journey of the transaction again. It starts by being made by Bob and sent by Bob. Now it goes into the unconfirmed transaction pool. A random miner has just mined a block. That miner goes to the unconfirmed transaction pool and picks the transactions with the highest fee. The transaction Bob sent has a high fee, so the miner picks it and puts it in a block. That block is confirmed by all the other miners by using the public key to see if the transactions were signed by the correct private key. If all the transactions are accurate, the block becomes part of the blockchain. Here is a flowchart of the transaction's journey to the blockchain.



V. Bitcoin Pros and Cons

There are several important advantages of using bitcoin. One is that bitcoin has low transaction fees. They can be as low as \$.50, but at times they can go higher. Another pro of bitcoin is its limited supply. Bitcoin is not a fiat currency. A fiat currency is a currency like the U.S dollar. It has an unlimited supply which makes it subject to inflation. Inflation is when governments put money into the system and lower the value of the money itself. Bitcoin is different: It has a limited supply. There will be only 21 million bitcoins ever in existence. That means it is inflation-proof. Another great thing about bitcoin is that 15,174 businesses worldwide (1 out of every 2,023 businesses) currently accept bitcoin as payment. This number is slowly going up as more and more businesses are thinking about accepting bitcoin as payment. There are also some disadvantages to using bitcoin. A big issue with bitcoin is that its price is not stable; it could go down or up at any time. So if you bought bitcoin to send \$5 to a friend, the price could drop and the payment might end up being equal to only \$4 and not be enough. Another concern with bitcoin is that it is very slow. Bitcoin only accepts 7 transactions per second. On the other hand, Visa can accept up to 65,000. Yes, these numbers are accurate! However, Bitcoin's Lightning Network discussed below, may solve this speed problem. A third problem with bitcoin is the mining energy usage, discussed in the "Mining Energy and Mining Farms" section.



VI. Other Things You Should Know About Bitcoin

This section discusses several new additions to bitcoin.

Bitcoin Halving

Every time 210,000 blocks are mined, a bitcoin halving occurs. Remember when I said the reward for mining a block was 6.25 bitcoins? The reward actually starts at 50 bitcoins; then, after 210,000 blocks, it is 25, and then after another 210,000 blocks, it is 12.5, and then after another 210,000 blocks, it is 6.25. The last halving happened in May of 2020. This does not mean the price of a bitcoin will drop; it just means that the people mining blocks will get less money.



Bitcoin Lightning Network

The Bitcoin Lightning Network is a way around the bitcoin speed problem. The basic idea of the Lightning Network is making microtransactions off-chain. The bitcoin blockchain is not very powerful (see the "Bitcoin Pros and Cons" section) because there are a lot of transactions happening per second, and the blockchain can only process seven per second. The Lightning Network takes a lot of load off of the blockchain and will overall make bitcoin faster.

How does the Bitcoin Lightning Network work? Say that Bob gets coffee every day from the coffee shop. Bob opens a payment channel with the coffee shop. To do that, Bob puts a little bit of bitcoin into the channel. That amount of bitcoin is recorded on the blockchain. Suppose that Bob put one bitcoin into the channel and the coffee costs 0.1 bitcoins. When Bob buys a coffee, he signs a microtransaction with his private key and links his public key to the transaction. The coffee shop does the same. Now the balances change; Bob has 0.9 bitcoins left in his deposit and the coffee shop has 0.1. Now Bob can buy his coffee until either Bob runs out of bitcoin in his deposit (and has to put more in), or Bob or the coffee shop decides to close the channel. Now let's suppose that Bob has 0.3 bitcoins left in his deposit when he decides to close the channel and the coffee shop has 0.7 bitcoins. Remember all those microtransactions? They were only one transaction on the blockchain. Bob and the coffee shop both get their bitcoins back. Now it is two transactions.

Now say that Bob wants to send some bitcoin to Fred. Fred also has a payment channel with the coffee shop. Bob doesn't want to open a whole other payment channel with Fred -- and he doesn't have to! He can just send the money to the coffee shop, which will send the money to Fred. The coffee shop can't interfere with this. The bitcoins are just passing through the channel.



VII. Conclusion

Bitcoin is very complex, but it also offers the chance to change the world's economy. Bitcoin probably will not replace the current system, but it can work alongside the current system to make sure that we all can transact easily with each other. If this paper still confuses you, don't worry. You're not alone! More than 880 million people know something about bitcoin but don't fully understand how it works.



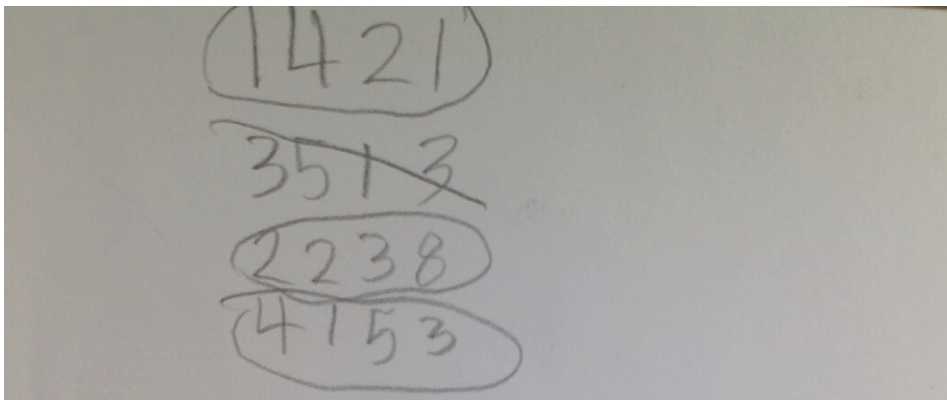
Bitcoin Game

SET-UP:

1. Paper and pencil
2. Find a bunch of random items around your house.
3. Give all of the players the same amount of items.
4. Assign one person to be the blockchain manager.
5. Give the blockchain manager the paper and the pencil.
6. Give everyone a number. If there are 3 people, then you would give the number 1 to one person, give the number 2 and the number 3 to the last person.

GAMEPLAY:

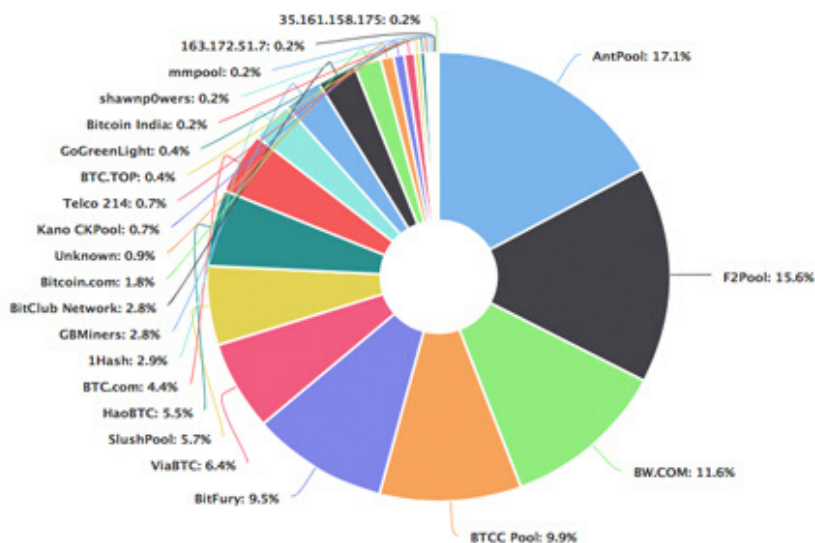
Everyone starts with 10 bitcoins. You can sell your items for bitcoins. To sell your items, you have to number each item. You can also buy items. When you want to buy items, you say to the blockchain manager, "I want to buy an item" and they will give you the piece of paper and a pencil. Now on the piece of paper, you write the person's number that you are buying from and also your number and also the item number and also the amount your are willing to pay. For example, you would write 1214 on the paper. The person you are buying from number is 1, so you put a 1 first. Your number is 2 so you put it next. The item number that you are buying is 1. Lastly, the 4 is how much you are willing to pay. If that person sees that you want to buy their items, they can check it, and then the trade happens. If someone tries to cheat and check something that is not theirs, then the blockchain manager will make sure that does not happen.



Bitcoin Charts



Bitcoin price since 2009



Pie chart of the percentage of the bitcoin network each mining pool is taking up

Bitcoin Fun Facts

The first bitcoin purchase ever was a pizza

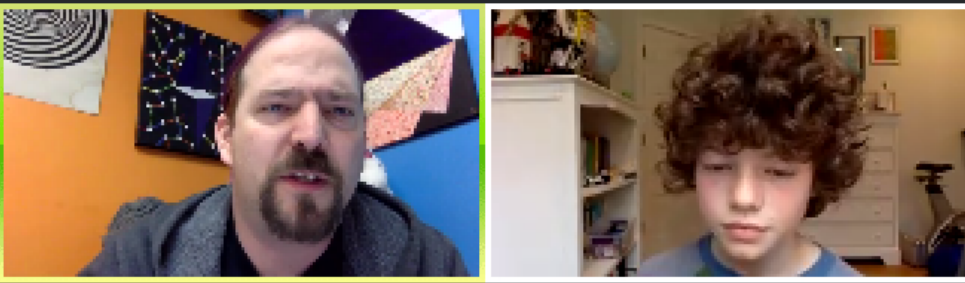
The inventor of bitcoin is a mystery

Bitcoin uses cryptography to make its network safe

Quantum computers could kill bitcoin

There are real places called Mining farms where people have tons of computers that get you bitcoins

If you lose your private key, you lose your bitcoins



**"I think to
understand
Bitcoin, you need
to go back to the
1990s, when the
internet was first
created."**

- RJ Herrick

Recommended Youtube Videos

Here are some youtube videos that I found helpful to understand Bitcoin.



<https://www.youtube.com/watch?v=kubGCSj5y3k>



https://www.youtube.com/watch?v=41JCpzvnn_0



<https://www.youtube.com/watch?v=L-Qhv8kLESY>

Conclusion

It is true that bitcoin is complex, but it is possible to understand it. I hope that you learned how bitcoin works and enjoyed my ebook.

