To: Members of the MDP Class of 2021-2022 **September 27, 2021**
Fr: Andy Davies

Re: "A Detailed Guide to How Cryptocurrencies Work"

Bitcoin, Dogecoin and Ethereum are among thousands that are confusing many Americans, but it doesn't have to be that way.

***The Washington Post*, July 6, 2021** **by Dalvin Brown**

****

We all know what a dollar bill looks like. We know what a penny looks like. But what about a bitcoin?

Cryptocurrencies such as bitcoin, dogecoin and ethereum have risen in popularity in recent years, introducing a host of new terminology and concepts to the public that can be tough to visualize and troubling to understand. A 2017 CNBC poll found that 33 percent of Americans hadn't seen, read or heard anything about bitcoin. And 44 percent had said they had seen, read or heard "just some" about it.

Yet conversations about cryptocurrencies are becoming increasingly common, especially as ransomware attacks, whose perpetrators demand payments in cryptocurrency, heighten awareness among victimized people, companies and municipalities.

Last month, El Salvador became the first country to formally adopt bitcoin as a legal tender in a move that would allow citizens to pay taxes via cryptocurrency. In the United States, the NBA's Dallas Mavericks and Tesla made announcements this year to accept cryptocurrency for merchandise, although Tesla chief executive Elon Musk later rescinded his comments.

So, what's actually going on? We'll answer some basic questions to help increase your familiarity.

What is cryptocurrency?

In its simplest form, a cryptocurrency is a computer code generated by publicly available software that allows people to store and send value online.

The open-source code originated with bitcoin over a decade ago and runs on an extensive network of private computers around the globe.

The code verifies and groups transactions onto a public record known as a blockchain. This is a large file containing every transaction ever made and can take days to download the first time.

The value of a cryptocurrency is usually expressed in dollars and is set by public trading conducted by exchange houses. That value can vary wildly; the cost of a single bitcoin equates to roughly $34,000 today, down from nearly $60,000 in May.

How is cryptocurrency made?

Think of cryptocurrencies as digital gold. "We believe gold has value because others agree that it has value, and there's only so much of it available," said David Sacco, a practitioner in residence at the University of New Haven in the finance and economics departments. The same idea governs the value of cryptocurrency. If more people are investing in crypto because they believe others see its value, the price for the crypto will rise and vice versa. But that also means the amount of cryptocurrency available must be closely controlled to preserve its value.

The algorithm that generates a cryptocurrency is available for download on developer websites like GitHub and, in theory, is available for anyone to use to create new cryptocurrency. But the process is highly competitive because the actual amount of cryptocurrency to be put in circulation is limited. These limits vary depending on the cryptocurrency and are set by whoever created the code. For instance, the bitcoin algorithm limits the number of bitcoin that can be generated to 21 million. At that point, no more will be made.

Creating new currency requires enormous computing power to solve the complex mathematical equations that generate a unit of cryptocurrency. Globally, the process devours more electricity than the Netherlands in a given year, according to an analysis by the University of Cambridge.

There may be roughly 70,000 computers running bitcoin blockchain software today, according to an online mine counter created by Luke Dashjr, a prominent bitcoin developer. Still, the exact number is hard to know because the software allows computers to operate privately, without announcing their presence to the broader network.

At the bare minimum, running a bitcoin mine, also known as a full node, requires a strong Internet connection with generous download capacities and 350 gigabytes of usable storage space, which can be found in most new laptops. Nodes also require at least 512 megabytes of random access memory, far less than the average laptop. The developers behind Bitcoin.org recommend having much more.

The software distributes new bitcoin based on how fast a miner's computers add transactions to the blockchain. So unless you're among the fastest, you probably won't create very many. Today, the system allows the creation of 6.25 bitcoin every 10 minutes, and the code halves that number every four years.

Some firms and entrepreneurs operate massive crypto mines for a better chance at grabbing a larger share of new coins entering circulation. Riot Blockchain, a public American company, is thought to run one of the world's largest. The firm's 190,000-square-foot facility is in Rockdale, Tex., a town with a population of about 5,800 and cheap electricity access that has welcomed cryptocurrency investment.

How many cryptocurrencies are there?

There are thousands of different types of cryptocurrencies to buy and trade, and more are being created. But they're not all created equal.

Some, like bitcoin, have a stronger history and greater brand recognition. Others such as dogecoin are the result of Internet hype.

Typically, they're controlled by computers running free, open-source code.

Bitcoin was the first and is the most popular cryptocurrency by far. At its height this year, bitcoin held 70 percent of the cryptocurrency market, but that share has dropped to about 40 percent amid renewed regulatory hurdles in China.

CoinMarketCap.com keeps a running list of cryptocurrencies that are added through an authenticity verification process.

Who creates cryptocurrencies?

Cryptocurrencies are usually created by developers and entrepreneurs with various political or economic visions.

Bitcoin was started in 2009 by someone under the pseudonym Satoshi Nakamoto who has largely remained anonymous. Ethereum was created by Toronto native Vitalik Buterin in 2015 to complement bitcoin and enable automatic business payments. Software engineer Billy Markus created dogecoin in 2013, mostly as a joke.

Where is cryptocurrency stored?

Cryptocurrency isn't technically stored anywhere. It's not saved in a folder or on a hard drive. Evidence of how much cryptocurrency you hold is stored on the blockchain.

The ledger is updated across the network with each new transaction — when a new bitcoin is mined as well as when someone moves their cryptocurrency.

To access your personal cryptocurrencies, you need a private key or complicated password that's generated by code when you create a wallet. In bitcoin, the private key is a 256-bit password, which is cryptography language meaning there could be dozens of characters in a seemingly endless number of variations.

The private key creates a unique signature that enables you to use your cryptocurrency to make transactions.

The private key also correlates to a public key, which miners can see, and a bitcoin address, which you can think of as similar to a public bank account number. The address is a unique, 26- to 35-character, case-sensitive string of letters and numbers, showing where cryptocurrency is sent on the blockchain.

The private keys can be stored inside specialized virtual wallets, which are apps offered by crypto exchanges. You get a wallet when you sign up to buy cryptocurrency.

The complex passwords can also be saved in hardware wallets or on a smartphone or computer. You can also print out a copy of the keys to store in a safe place.

The crypto wallets differ from the smartphone wallet you might be storing your debit and credit card information in. They're often encrypted, and if you lose your password, you can be locked out of your cryptocurrency forever.

How is cryptocurrency passed among people and businesses?

While traditional payment systems rely on banks to verify transactions, cryptocurrency transactions are verified by miners on the blockchain. Miners run mathematical checks to make sure that a transaction is valid, and a majority of the nodes must agree that it was a valid transaction before it's added to the blockchain.

Most people rely on crypto exchange services like Coinbase, eToro, Binance or Robinhood to buy and sell cryptocurrency. People can also give bitcoin to others, similar to transferring money to someone else's bank account.

As more companies embrace cryptocurrency, people are able to do more with it. Some firms such as AT&T and CheapAir.com now accept cryptocurrency as tender. You can now use it to pay your phone bill or buy travel tickets.

What government regulations exist?

Part of the reason cryptocurrency has become more popular is that it's not controlled by the Federal Reserve or any other agency within the government. It is, however, subject to taxes in circumstances laid out by the Internal Revenue Service in 2014. Generally, taxpayers are expected to convert their cryptocurrency transactions into U.S. dollars to report gains and losses to the IRS.

Beyond taxes, exchanging crypto is largely unregulated on the federal level, but states like Wyoming and Ohio have made moves to welcome it locally. Wyoming signed into law a "Utility Token Bill," making it easier to operate a blockchain business, while Ohio allows firms to pay a variety of taxes with cryptocurrency.

Are cryptocurrency transactions secret?

No, they are recorded. What is secret, or at least difficult to know, is who received and sent a transaction because no name is attached to the transaction listed on the blockchain. But the crypto exchange that sets up a wallet does require clients to identify themselves. And the recent FBI seizure of $2 million in bitcoin that was part of the Colonial Pipeline ransomware hack suggests more can be known about crypto transactions than is generally acknowledged.

Because cryptocurrencies are exchanged on a public document, it's possible to see when funds are transferred and where they go. The FBI affidavit requesting court approval to seize the Colonial Pipeline ransom recounted the money's movement from account to account in detail. It's not clear how the FBI gained access to the wallet where the Colonial Pipeline ransom had been stored. But Sacco said the seizure from that address shows that cryptocurrencies might not be as private as people thought they were.

dalvin.brown@washpost.com