Part

I

Understanding the Technology

As digital investigators, we have a tendency to want to get straight to the proverbial coal face and start looking at the data. However, with cryptocurrencies, it is important to understand the underlying technologies and how blockchains function to be able to effectively and accurately investigate the evidence.

CHAPTER

1

What Is a Cryptocurrency?

Over the past few years, the term *cryptocurrency* has become a well-used term in financial circles, new business plans, and news headlines. Often the term is associated with criminal activity on the so-called "dark web," but more recently with the increasing value of currencies like Bitcoin, the word, concept, and products are entering mainstream consciousness.

But what really is a cryptocurrency and how does it work? In this chapter, we will examine the concept, the history, and the uses for cryptocurrencies and look at how to set up a Bitcoin trading node.

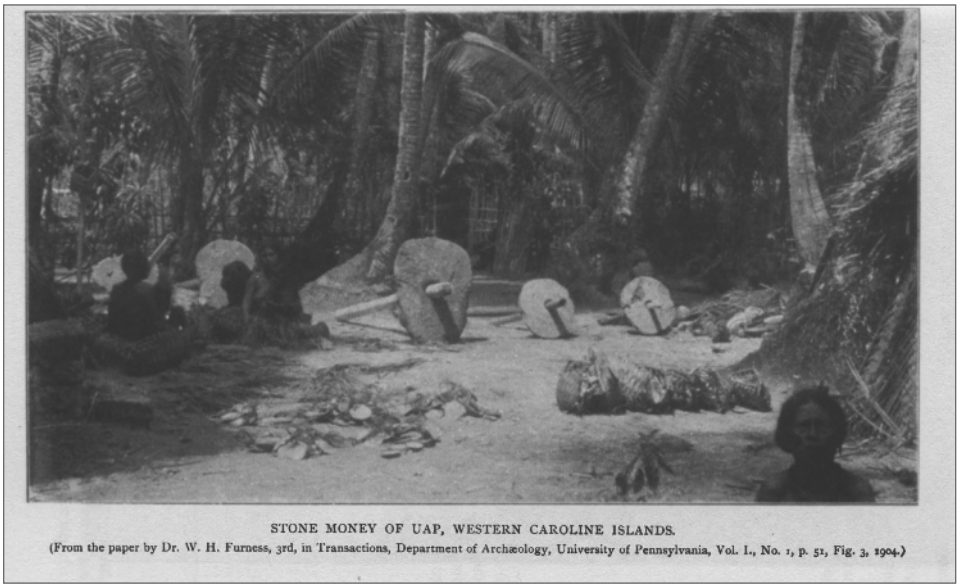
Why does an investigator need to know this? Understanding the concept of these online currencies can help you form a good foundation to build a more comprehensive technical understanding. It can also help you to see the criminal uses of these currencies.

A New Concept?

In the far western Pacific region of Micronesia is a tiny cluster of islands named Yap. Conspicuous against the deep blue of the ocean, this tiny group of "high islands" comprises rolling hills covered with dense, lush forest. The islands share a coral reef that provides sustenance for the islanders from the fish that seek protection from ocean predators.

As far back as the thirteenth century, the sultan of Egypt referenced islands at the far east of the Persian Empire, where the only currency was millstones. This was later confirmed by the Spanish when they "discovered" the island group in 1528. If you visit today, you can still see the stone coins that made up the primary currency of the islanders for many centuries; in fact, they are still used today in trades involving land or marriages.

The stones are a variety of sizes—some as small as 3.5 centimeters—but the ones that draw the most attention are up to 4 meters in diameter (see Figure 1-1). The Internet boasts many pictures of tourists standing next to these vast doughnut-shaped disks of calcite named Rai coins.



STONE MONEY OF UAP, WESTERN CAROLINE ISLANDS.
(From the paper by Dr. W. H. Furness, 3rd, in Transactions, Department of Archæology, University of Pennsylvania, Vol. I., No. 1, p. 51, Fig. 3, 1904.)

Figure 1-1: Stone money of Yap.

The stones do not originate on Yap but are mined and shipped from other islands such as Palau, which is 450 kilometers away. For centuries, these coins were loaded onto sail-driven rafts, and brought across the open ocean to the island, unloaded, and moved to a location somewhere on the island where they would generally stay put forever.

You may be wondering: How do the islanders use such huge coins in actual transactions? How do they value them? How do they know who owns each coin?

The Rai coins are interesting because they almost exactly prefigured the way a blockchain in a cryptocurrency works—in fact, similar questions can be asked about a cryptocurrency. How can you trade something that doesn't really exist, such as a Bitcoin? How is a blockchain-based coin valued, and how can

you know who owns a coin with no central bank controlling the movement of funds? Examining the Yapese currency helps us to understand the blockchain currency concept.

So why does a large stone disk have value? Let's say that Bob from Yap wants a 3-meter coin. First, the coin must be mined. Consider the difficulty involved. Workers have to be employed and sent in boats to an island 450 kilometers away. Calcite must then be mined, and the resulting stone carved into the distinctive doughnut shape. This final "coin" must then be loaded onto a boat and sailed back across the stretch of Pacific Ocean with its obvious dangers. The work and considerable expense involved to mine the coin are what gives it its perceived and agreed value to the islanders. Indeed, the bigger the coin, the higher the difficulty—so the value is commensurately greater.

One of the first questions I am asked about cryptocurrencies is where does the money come from? The answer, of course, is that the money comes from nowhere, but that is not really a fair answer. If you know anything about any cryptocurrency, you will know that new coins are "mined." This concept will be discussed later, but in simple terms, computers work to solve really, really hard mathematical problems, and when they find a solution, they are rewarded with "new" coins. But just like mining a Yapese Rai coin, work is involved that carries a very real cost. Although Bitcoin miners, for example, are not chartering a ship and crossing oceans, they must spend real money on expensive, specialized custom ASICs (application specific integrated circuits) capable of carrying out trillions of calculations a second. They must then spend money on providing considerable amounts of electricity for running the computers and keeping them cool. Just like their stone counterparts, it's difficult and expensive to mine cryptocurrency coins, which gives them a perceived and generally agreed value due to their scarcity and the fact that eventually Bitcoin will "mine out," where all coins will be mined and no more can be produced.

It is notable that in 1874, a captain named David O'Keefe imported a large number of coins from Palau to trade with the Yapese. Interestingly, this "had its disadvantages, not least the introduction of inflation, caused by the sudden increase in the stock of money" (see `https://www.smithsonianmag.com/history/david-okeefe-the-king-of-hard-currency-37051930/`). In the same way, if the "difficulty of work" to mine cryptocurrency coins became easier, it would directly affect their accepted value.

How do the Yapese trade their coins? Most of the coins are too big to move, so the Yapese use a very simple but effective form of what we would now call a distributed ledger. For example, let's say there was villager named Bob, and when Bob's coin arrived by boat from Palau, it would be placed near a pathway or some other visible place. All the villagers would know that the coin "on the path by the beach" belonged to Bob, because everyone would be told this and

would add it to their individual mental note that included the other large coins on the island. If Bob wanted to buy some land from Alice, they would agree on the transfer of coin for land, and they would then tell all the villagers that the coin "on the path by the beach" now belonged to Alice. With no centralized person keeping a record or ledger, the possibilities of fraud are massively reduced. If a pretender named Nick told others that he owned the coin "on the path by the beach," the majority of villagers could reject the claim due to their collective knowledge of ownership.

Amazingly, blockchain-based cryptocurrencies work in almost exactly the same way. When you wish to pay for goods or services, a record of the transaction is sent to every (full-node) user of the currency (covered in more detail in "Setting Yourself Up as a Bitcoin User" at the end of the chapter). This means that there isn't just one record of the transaction, but thousands all around the world. You are, in effect, saying, "Hi everyone, the coin you can find at this address now belongs to Alice." Should anyone else try to claim ownership of a coin, the large number of ledgers around the world can disagree, preventing any fraud.

It was reported that a coin being transported to Yap was lost overboard in a storm, but as all the villagers knew of the mishap, the owner was still credited with the coin, and although no one had ever seen it, it was still traded as "the coin in the bay." This demonstrates that a coin does not need a physical manifestation to be accepted as real, tradable tender. A cryptocurrency coin such as a bitcoin or Ethereum ether coin never has a physical representation, but because all the users of the currency trust its existence and accept the work that went into mining it, its value is accepted as real and hence it can be traded.

Now back to the original question: What is a cryptocurrency? There is considerable debate over the definition of a currency when related to so-called cryptocurrencies. The cryptology community is uncomfortable with the widening and often inaccurate use of the term "crypto" in news headlines and press releases and even financiers are suggesting that the term "currency" in cryptocurrency should be replaced with the word "asset." However, a currency is generally understood to be a tradable system of money. But in reality, anything can be a currency if it is accepted as representing an agreed value; effectively, we are using a barter system where we perceive value in the currency that we trade for goods and services. Although we tend to think of a currency as the monetary notes in our purse or wallet, we use many tradable "tokens" in our everyday life. Perhaps you recently paid for a flight with air miles or used a coupon to get a free item when you bought another. Although these "tokens" do not have a traditional monetary value in the same way as a dollar bill or euro note, they are still tradable at an agreed rate or even flexible rate.

Here's an analogy: A parent or teacher may use simple marks on a board to indicate when a child has behaved well or achieved something. There may be

an agreement that 10 marks equal a certain treat, trip, or other benefit. In this situation, the marks on the board become a currency of sorts. They have a value that can be traded, even if it's in a very limited way.

As we have seen, a stone slab at the bottom of the ocean can be a tradable currency, so using the same reasoning, a block of text in a database that states that it carries a particular value—for example, one bitcoin—can also be traded. But that doesn't answer the "crypto" part of a cryptocurrency.

On Yap, the system of trust works because collectively the villagers are believed to be reliable witnesses. If many villagers clubbed together and formed a majority, they could then prove that a coin belonged to someone other than its rightful owner, but that would put their own coins at risk should they fall out of the new dishonest collective. This creates a paradigm of dependability where the majority can always be trusted. The same concept works in cryptocurrency. Users of a cryptocurrency such as Ethereum, Bitcoin, or others are encouraged to run a "full node"—that is, a complete record of every single transaction that has ever happened on the currency. This prevents individuals from dishonestly claiming ownership of currency, as the rest of the world's full nodes will disagree. The "crypto" part forms the underlying basis for authenticating the ownership of coins. In fact, cryptographic systems are used in every part of the process.

The definition of cryptography in its simplest form is from the Greek meaning "secret writing." Today, we define it as generating codes that allow information to be kept secret. With a cryptocurrency, we are not keeping information about a transaction secret—quite the opposite, every transaction can be read by everyone. We are using the techniques applied in messaging cryptography to enable people to prove that they are the rightful owner of monies, or more accurately, that they are the rightful owner of a transaction where they were the approved receiver of the money. Bitcoin, for example, uses a mixture of SHA256 hashing, Elliptic Curve cryptography, and others to not just secure a transaction but keep securing it repeatedly, forever. You will learn more about those systems in Chapter 2, "The Hard Bit."

The idea of being able to pay for goods and services over the Internet is not new. David Chaum developed Digicase in the late 1980s, which was arguably the first concept of Internet money. But it wasn't until 1998 that an attempt at public online payments based on the concept on an online wallet appeared and became successful with PayPal, which was led by the now hugely successful businessman Elon Musk. As I mentioned in this book's Introduction, PayPal still relies on the legacy banking world to handle the storing of money, and PayPal accounts are still primarily linked to real-world bank accounts today.

Interestingly, the crown for the first e-currency really goes to E-Gold, which was set up in 1996 by the unusual business pairing of an oncologist and an attorney. This system was based on stored gold, and users could make value transfers to other users of the system purely online. The E-Gold developers

were way ahead of their time, using SSL (encryption) to move the payment data and an API for other developers to leverage the E-Gold system. Sadly, its demise came in 2013, after attention by the U.S. authorities regarding the use of the system for illegal payments. Ultimately, the owners were not implicated in any wrongdoing.

Leading Currencies in the Field

It was tempting to write an investigations book about Bitcoin since, at the time of writing, it is the brand synonymous with the word cryptocurrency in the public mind. However, as I spent more time with Monero, Litecoin, Ethereum, and others, I realized that although they were all subtly or sometimes significantly different and set out to provide certain abilities to their users, for an investigator, they all worked in the same fundamental way. When you consider that technology is a hard taskmaster and that online services hit the proverbial fan almost as fast as they spend their venture capital money (MySpace anyone?), will Bitcoin still be valuable and newsworthy in two years, or even a year? Could Ethereum be the next Facebook of the currency world and become the default choice for transactions and contracts of all types? Only the future will answer that question, but the methods of investigating crime involving a cryptocurrency will remain basically the same. So, although Part II of this book deals with investigations that are focused on tools for Bitcoin with its spin-offs and alt-coins, and Ethereum, this is only because tools are available for them. Should Monero take the limelight in a few years' time, undoubtedly an investigator will be able to find similar tools to help them investigate effectively.

In late 2017, investopedia.com, the world's largest financial educational website, named Litecoin, Ethereum, Zcash, Dash, Ripple, and Monero as the best investable cryptocurrencies aside from Bitcoin, but that should not necessarily drive research by an investigator. Some of the new breeds of currency lend themselves to criminal uses. For example, Zcash offers "shielded" transactions where the sender's and receiver's details are hidden, and Dash provides increased anonymity over Bitcoin. It is more likely that these features, rather than Bitcoins' burgeoning value, would attract someone with the need to hide his or her transactions for nefarious purposes.

I should be clear that I am in no way accusing these companies of deliberately attracting a certain type of client any more than Tor (which was partly developed and funded by the U.S. government) was designed to hide terrorists and pedophiles. However, if you, as an investigator, are aware of the specific security and anonymity features of a particular currency, you may be more prepared to research and ultimately exploit them during an investigation.

Due to these issues, I will decline from the obvious inclusion of a list of available cryptocurrencies, since by the time you read this, there may be a new pretender in town being used by our suspects. Instead, this book will try to both be specific as to investigation methods you can use now and look at the generic principles behind this type of analysis.

The website Coinmarketcap.com maintains a constantly updating list of the primary cryptocurrencies, almost 900 were listed at the time of writing.

If you are interested in launching your own cryptocurrency and becoming wildly wealthy, you will find an excellent tutorial at `www.ethereum.org/token`. (And once you are a billionaire, please remember who gave you the tip and at least invite me onto your boat!)

Is Blockchain Technology Just for Cryptocurrencies?

Although we look in detail at what a blockchain is in Chapter 3, suffice it to say that it is simply a list of transactions, distributed to many nodes on a network, grouped into clusters called blocks, and—using a physical analogy—stacked on top of one another like a Lego™ brick tower.

The concept of a virtually anonymous, distributed ledger, contract-led blockchain-based system certainly has some significant possibilities, but believing what you read in the press and in a company's marketing materials would be a major mistake. In 2018, you need to include two terms in your prospectus to float your company on the stock market or add to your brochure to sell your latest product: artificial intelligence (AI) and blockchain! In fact, throwing a bit of "cloud" in there couldn't hurt either. I saw the marketing headline "The First A.I. Big Data Marketing Cloud for Blockchain" on a software website recently. It seems that any system that adds up 2 + 2 or includes an "if . . . then" decision tree is now considered AI that may take over the planet at any moment. It's not and it won't, even if it's got a lot of "big data in the cloud"!

It is the same issue with the blockchain: Business analysts have watched the extraordinary rise in the value of Bitcoin, read an article on the technology it is based on, and then added the word to any system that needs to sound a bit more hip and cool (although I am well aware that the words "hip" and "cool" themselves are no longer considered "hip" or even "cool").

A quick search of the Internet reveals insurance companies that will put your insurance agreement on the blockchain, delivery companies that will use smart contracts to deliver your parcel, auction sites that use the blockchain to reduce fraud, and security companies that promise the blockchain will prevent you from ever being hacked again. Sound far-fetched? Most are. But consider the following auction-house example.

Several years ago, I bought an old book at auction—or at least I thought I had bought it since I was the final bidder. However, the auction house told me later that it did not have a record of my final bid, and since the previous bid hadn't reached the reserve, the book would be put up for sale again. Because the auction software was hosted in a single location and the auction house controlled it, I had no recourse or way of proving otherwise. However, I had taken a screenshot of my browser with my high bid and my successful purchase message. The auction house then told me that it had "lost the book." After a few choice words and threats of legal action from me, it "found" the book and honored the bid. It was clear that the auction house wanted more from the auction and simply wanted a chance to sell again with a better audience. How would a blockchain-based system have improved this situation?

A blockchain auction system could work as follows: Every bidder is a node on the blockchain. A product to be auctioned is set up as a token with a contract of sale connected to it, based, for example, on the Ethereum network. Each bid made is a transaction between the auction and the highest bidder with the "token" moving seamlessly from high bidder to high bidder. Whoever is the final bidder when the real or virtual gavel comes down is left as the owner of the token. Everyone on the blockchain can see the final transaction, and the contract is set. I own the item because I own the token, and it's proven by every node on the network. The sales contract can also form part of the blockchain contract, minimizing paperwork. (If anyone sets this system up and makes a million, please once again remember me when you are out on your yacht.)

How does this affect the investigator? Blockchain transactions on Bitcoin are one aspect of the technology and require a skill set that you will learn about in this book. However, in the future expect to find blockchain-based systems with transaction-centered contracts in a wide variety of business sectors. An analyst will need to have the skills to learn how a blockchain functions, and be able to decode contracts, and follow the flow of contract transactions. I will cover contracts in a little more detail later in the book, but if you choose to carry out further research on the smart contract-based platforms such as Ethereum, it would not be a waste of time.

Setting Yourself Up as a Bitcoin User

If you have not had a chance to either trade cryptocurrencies or just play around with the technology, I suggest that this would be a good time to just go and spend some time looking at transactions—perhaps by going to an online blockchain viewer such as `www.blockchain.info`, which we will use numerous times during the book. You will see block numbers—click one. Then you will see a long

list of transactions. What can you figure out just from looking at this list? (We will cover everything in due course.)

Primarily, it would be a good time to set yourself up as a "full node" Bitcoin user. This will be necessary if you are to follow and practice some of the more advanced investigation techniques later in the book.

Here's the setup procedure:

1. Browse to `bitcoin.org/en/download` and download Bitcoin Core.
2. Install Bitcoin Core to the default locations.

As soon as you run Bitcoin Core for the first time, it will start to download the entire blockchain. This is fine, but at the time of writing, it takes up about 170 GB on the disk, so you will need to make sure that you have enough space for the initial download as well as the space for it to grow as it synchronizes with the Bitcoin network. It's also a good idea to experiment with the Bitcoin Testnet network where you can't lose any money. You will need another 80 GB or so for that.

If you wish to have the blockchain files on a different drive, it's easy to do. Just follow these steps:

1. Right-click your desktop and create a new shortcut. The path is usually:

   ```
   C:\Program Files\Bitcoin\bitcoin-qt.exe
   ```

2. Add the following to the end of the command:

   ```
   -datadir=d:\Bitcoinfiles
   ```

   where the path is the new folder where you would like the blockchain created (see Figure 1-2).

Figure 1-2: Dialog box to create a shortcut to run Bitcoin Core.

Remember to start Bitcoin Core from this shortcut each time. Start Bitcoin Core and allow a couple of days for the blockchain to fully download. You can stop and start it as you wish, and it will carry on from where you stopped it.

Initially it will be beneficial to use Bitcoin Testnet. This is a fully working Bitcoin environment, but the coins are free, and you can send them around and analyze the results exactly as if you were on the actual live Bitcoin environment. Follow these steps to access and use Testnet:

1. Locate the Start Menu Bitcoin Core group and the green shortcut to start the testnet version (see Figure 1-3).

   Again, you can edit this shortcut with `-datadir` if you wish to change where the blockchain will be stored.

Figure 1-3: The three options in the Bitcoin Core program group.

TIP **If your path has a space, remember to enclose it in double quote marks. For example:** `-datadir="d:\bitcoin files"`

2. Start Bitcoin Testnet and allow the blockchain to download.

   You can run the main core and the Testnet at the same time.

3. Send your wallet some coins.

   You do not need to wait for the blockchain to finish before doing this, although you will need to wait to see the coins in your wallet and send them on again.

4. While you are waiting, select **`File` ➪ `Receiving Addresses`** on the Bitcoin Testnet wallet.

   You will see a long sequence of letters and numbers. This is a bitcoin address. (It's actually a value represented in Base58, but more about that later.)

5. Right-click and copy the address onto your clipboard.

6. Browse to `http://bit.ly/2fcuEEl` and paste in your address.

   Two testnet Bitcoins will be sent to your wallet. Once the blockchain has finished downloading, you will see a balance that you can now spend.

7. Go back to the Receiving Addresses dialog box and click the New button.

8. Copy the new address onto the clipboard and click the Send button on the menu bar (see Figure 1-4).

Figure 1-4: The Send screen in Bitcoin Core.

9. Paste the new address into the Pay To box, choose how much Bitcoin to send, and click the Send button (see Figure 1-5).

   You have just sent yourself some Bitcoin. Congratulations.

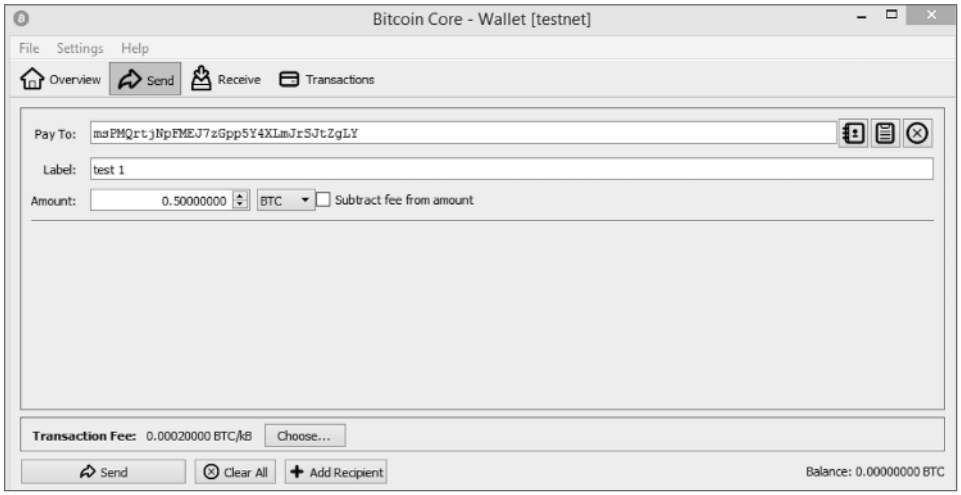


Figure 1-5: The Send screen with send address filled in.

10. In the Transactions dialog box, you will be able to see the transaction you just did. Double-click the transaction line, and a box will open that includes a long string titled `Transaction ID`. Copy this long value onto the clipboard.
11. Browse to `http://bit.ly/2jKBPso_` and paste the value into the Address search box at the top of the screen.

    You should see a representation of your transaction taken from the blockchain (see Figure 1-6). Again, congratulations.

Figure 1-6: Blockchain viewer showing a transaction.

I will explain every aspect of what you can see on this screen in a future chapter, but for the time being, you now know how to send bitcoin and find your transaction on the blockchain.

Summary

In this chapter, you learned what a cryptocurrency is, how the generated coins can have a perceived value, and how the concept of the blockchain can be used for many differing applications. The history of the stone coins of Yap helped to explain how a decentralized ledger can work in a community setting and how this concept is used in the distributed ledgers of a global blockchain. You learned how to set up a Bitcoin Core full node and how to practice coin transactions without costing anything by using the Bitcoin Testnet. The chapter introduced you to concepts that you need to understand in much more detail, such as cryptography, blocks, and transactions, which we will delve into in the coming chapters.