Cryptoeconomics

Tyler Cowen
Alex Tabarrok

CHAPTER OUTLINE

What is bitcoin? How about ether? What are blockchains? What is DeFi? What are NFTs?

As instructors we hear these questions with increasing frequency, and we hear them not only from our students but also from our economist colleagues and from our friends and family. So we thought we would write a quick and straightforward guide.

To be clear, *none of this is intended as investment advice,* one way or the other. And if you have gotten rich, or poor, buying and selling cryptocurrency (or crypto), well, that is your business, quite literally.

This is a guide for how to understand crypto, and how to put crypto into a broader analytic and economic framework. Crypto is not a common topic in principles of economics classes. But it is one of the economics ideas that has been discussed the most over the past decade, so we thought it worth some coverage. Optional, of course!

Crypto is an application of cryptography, so we're going to talk you through some basic insights of cryptography. Don't worry, we'll be headed back to our main topics, and to economic reasoning, in due time.

If we had to sum up cryptoeconomics as it has evolved we might say that cryptoeconomics brings the invisible hand to computation.

Some Basics of Cryptography

The ancient Indian guide to the good life, the *Kama Sutra,* written around 400 BCE to 200 CE, is well known for including an uninhibited guide to good sex. Perhaps appropriately, it also recommends learning how to write in code so that two lovers can exchange secret messages. Thus, the history of cryptography is more than 2,000 years old.

One of the cryptographic techniques recommended in the *Kama Sutra* is a transposition cypher, replacing each letter in a sentence with a different letter, say, the next in the alphabet. Ordinary transposition cyphers can be broken by analysis. Ju't opu ibse up dsbdl.

There is a transposition cypher that can't be broken—one that associates each successive letter in the message with a new *randomly chosen* letter (this is also known as a one-time pad cypher). A message encrypted with a random transposition cypher can be decoded only if the receiver knows the key—which letter replaces which letter. Great for secret lovers! Let's call them Alice and Bob. But there is a problem. If Alice and Bob can't share secret messages without first sharing a key, how can they share the key in secret? It seems we are back to where we started.

Indeed, it seemed impossible that a key could ever be exchanged without in-person or trusted key exchange and that is how it seemed for thousands of years. The world could hardly believe it, therefore, when in 1976 Whitfield Diffie and Martin Hellman created a new kind of cryptography, one that allowed for secure communication of a secret key over an *insecure* network.

The remarkable Diffie-Hellman algorithm is based on the mathematics of nonreversible functions—which we won't get into—but let's be clear what the algorithm and its successors make possible. Alice and Bob can meet, let's say in a crowded bar, they can shout some words at one another—words that anyone else can hear. The words let Alice and Bob create a secret key that only they know. Using the secret key, Alice and Bob can then shout more words at one another and no one will know what they are saying. Remarkable!

Shouting in crowded bars to send secret messages might not sound very useful but what we are really talking about is sending messages across the internet. Is that starting to sound more useful? Take a look at the URL of your bank's website. It probably starts with https://. If it doesn't, get a new bank immediately! You probably know that http stands for HyperText Transfer Protocol, which is a protocol for sending data over the internet in a way that your browser recognizes as links, pictures, text, and so forth. The "s" at the end stands for secure and what it means is that before communicating messages—like bank account numbers, credit card numbers, or medical information—your bank and your browser will first exchange a key. The key will then be used to encrypt messages so that even if someone else (crowded bar, remember) hears those messages they won't be able to decode them.

In fact, the same Diffie-Hellman algorithms that let you communicate secretly with your bank also lets banks secretly communicate with one another. Every day trillions of dollars in interbank transfers are secured using these algorithms. Thus, the first lesson of cryptoeconomics is that the commercial internet as we know it would not be possible without cryptography. Message services such as WhatsApp and Signal also use Diffie-Hellman algorithms so that people across the world can communicate securely.

Diffie and Hellman revolutionized cryptography by proving that a secret key could be distributed over an insecure network. In 1978, inspired by Diffie and Hellman, computer scientists Ron Rivest and Adi Shamir and mathematician Leonard Adleman created a second revolution. Rivest, Shamir, and Adleman, henceforth and forevermore known as RSA, showed that the key used to encrypt a message did not have to be the same as the key used to decrypt a message. The implications of a two-key system are profound.

Suppose Alice wants Bob to send her a secret message. Using the RSA system, Alice creates two keys, a public key and a private key. She announced the public key to the world—perhaps she puts her public key on her webpage or in an address book like an email address. The public key is used to encrypt messages to send to Alice. Now here is the amazing part. The only way to decrypt a message sent using Alice's public key is to use Alice's private key. In other words, only Alice will be able to read messages encrypted using Alice's public key. The advantages of a public-private key system are tremendous.

The first advantage is that Alice only needs to create her public-private key pair once and she can then communicate securely with anyone in the world at any time. Not only can Bob send Alice a secret message but so can Tom, Dick, and Harry.

The system also works in "reverse." Alice can encrypt a message using her private key that can only be decrypted using Alice's public key. Why would Alice want to encrypt a message that anyone can decrypt? *To prove that she is*

Alice. To be more precise, encrypting a message that Alice's public key decrypts proves that the sender knows "Alice's" private key. Public-private key encryption thus authenticates control of the private key.

He who controls the private key controls the identity. Often this alone is quite useful. Smart cards, for example, use public-private keys for authentication. Each smart card has a unique public key known to the credit card company, say Visa, and a corresponding private key stored on the chip in the card. When the card is presented for payment, Visa sends it a random number. The chip in the card encrypts the random number using its private key and sends the encrypted message back to Visa. Visa then attempts to decrypt the message using the card's public key. If the decrypted message reveals the random number sent by Visa, then Visa knows exactly which card is being used. Of course, the card could still be stolen and used by a nonrightful owner but unlike earlier credit cards, a smart card cannot be duplicated using any transmitted information and it would be very difficult to physically duplicate a card even if it were stolen. Thus, public-private key encryption and smart cards limit the value of a stolen card and add significantly to the security of the credit card system.

Not only is a public key a type of identity, it is a powerful *new type of identity*. Writers have long used pseudonyms. *Federalist 51*, for example, was signed by Publius, a pseudonym who most historians think was James Madison.[1] The Publius pseudonym offered Madison some anonymity but what if another writer started publishing papers under the name Publius? How could Madison prove that the new Publius was a fake? He could not—but a modern Madison could. A modern Madison wishing to remain anonymous could create a public-private key pair and associate the public key with the name Publius. He could then encrypt his letters using the private Publius key. Since only Publius's public key could decrypt Publius's letters, no one else could credibly claim to be Publius.

It would be a bit of a pain to have to decrypt every new Publius letter. So Publius publishes his letters to the web and then signs them with a digital signature. A digital signature is a message that can only be decrypted using Publius's public key. The message might be as simple as "I am Publius," but then we have a problem—someone could take Publius's digital signature and attach it to a different message. To avoid this problem, we create a practically unique digital signature for every message by binding the digital signature to a cryptographic "hash" of the letter.

A cryptographic hash is like a digital fingerprint, a much shorter message that in practice can be uniquely associated with any message. The SHA256 hash algorithm, for example, hashes any input message into an output message of 256 bits, a binary number composed of 1's and 0's that is 256 digits long. In other words, we can feed any message into the SHA256 algorithm—it could be a sentence, an entire novel like *War and Peace*, or a digital picture—and the algorithm will hash it into a string of 1's and 0's that is 256 digits long.

256 digits isn't that long—it's about the length of two to three sentences. But since each digit can be either a 0 or a 1 there are 2^{256} possible hashes and 2^{256} is a very, very big number. It's just a little bit smaller than all the atoms in the known universe.

Now here is what's amazing about these cryptographic hash algorithms—the output is "as good as random." In other words, anytime you hash something new the output could be any of 2^{256} possible outputs and there is no way to predict the output in advance. Guessing is useless since there are so many possibilities. Yet even though the output can't be guessed before hashing, the function isn't random.

Here, for example, is a hash of the entire text of *War and Peace*:

AB8257AE34CE51933B7D6F0B06A486CD1E189636C572B0723A5F
4E341B57A37A

If you are wondering why it's not a string of 256 0s and 1s, that's simply because we encoded the same date in a shorter Hexadecimal format. An "A" in this format converts to 1010, for example. Now here is *War and Peace* hashed but with just one comma missing.

F92D49FF6BF02E4B29469C8AC71A7D662E82139F0AD4EC9D027
DF1AA86B23426

You can try the SHA256 hash function yourself at websites such as: https://emn178.github.io/online-tools/sha256.html.

The two hashes look completely different and that is the sense in which a hash produces a digital fingerprint. Another important implication is that a hash function like SHA256 is said to be collision-resistant, meaning that it is infeasible to find two messages with the same hash.

Ok, now let's go back to Publius. Publius publishes his letter to the web and then he hashes the letter and encrypts the hash with his private key. Anyone who wants to be sure that Publius wrote the letter can decrypt the hash using Publius's public key and then compare the decrypted hash to the hash of the publicly posted letter. If the two hashes match, the readers know not only that Publius wrote the letter but also that the letter wasn't tampered with. Remember that if a single comma in the published letter has been altered its hash will not match the hash found in the digital signature.

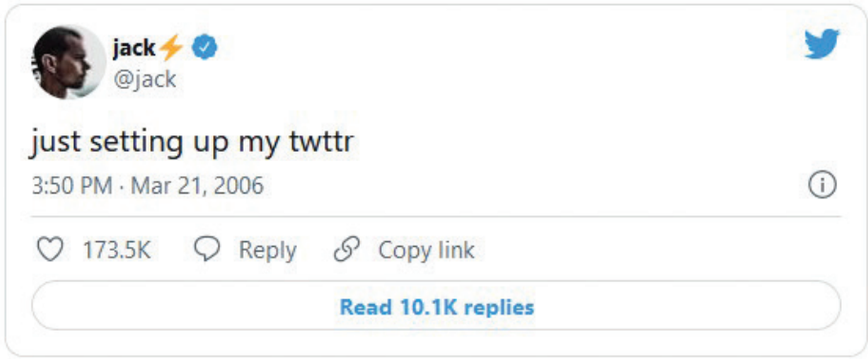
Several people have claimed to be Satoshi Nakamoto, the anonymous creator of bitcoin. None, however, have passed the acid test—sign a letter using Satoshi's digital signature.

Summarizing, digital signatures offer three key properties: authenticity, message integrity, and nonrepudiation. Authenticity means that a digital signature is strong evidence that the signer has the identity associated with the public key. The integrity of the message is provided by comparing the message hash within the signature with the hash of the message. Finally, since only the holder of the private key can sign the digital signature, the signer cannot repudiate having signed the document.

We're still going to get to bitcoin, but to clarify these cryptographic principles and to introduce the idea of a blockchain, we will first explain the simpler topic of Non-Fungible Tokens, or NFTs as they are known.

Non-Fungible Tokens

Perhaps you have heard of NFTs, digital art sold on a blockchain for what sometimes seem like astounding prices. Jack Dorsey, the co-founder of Twitter, for example, sold an NFT of his first tweet for $2.9 million dollars! Here it is:



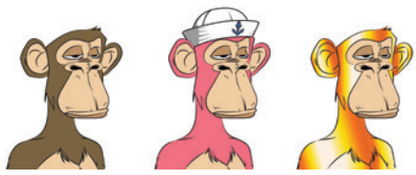
Okay, so what is an NFT? An NFT is just a cryptographic hash of an artwork (or other digital file) signed with a digital signature. Remember the letters signed by Publius with a digital signature? The signature proved that Publius wrote the letter and also that the letter is exactly what Publius wrote. Now imagine that Publius becomes famous as one of the authors of the U.S. Constitution. Maybe Publius would like to cash in on the fame by selling an NFT.

Here's how Alice can buy and Publius can sell an NFT. Alice sends Publius some crypto assets, for instance bitcoin. Publius signs one of his letters with his private key and attaches to it a message: "I sell this letter to Alice." He then encrypts the whole package with Alice's public key and sends it to Alice. Alice now "owns" Publius's letter which means that she can prove that Publius sent her a message saying "I sell this letter to Alice." So what has Alice really bought? She hasn't really bought the letter that, like Jack Dorsey's tweet, was public anyway, but she has bought Publius's digital signature. In a way, the artwork is a wrapper for the digital signature.

Is it strange to buy a digital signature? Maybe. But people buy autographs all the time. In 2021, a rookie card signed by NFL quarterback Tom Brady sold for $3.1 million. One collector said, "For me, an autograph on a card makes that card both unique and special. The autograph means that the signer came in contact with the card; therefore, owning a signed card provides a direct, physical link to its signer. That link makes the card special and forever distinguishes it from all of its unsigned cousins."[2] Many people feel the same way about digitally signed NFTs. You might be bullish or bearish about the current level of NFT prices, but we don't find it strange that a market has developed. There are markets in many kinds of collectibles, for instance a first edition of Adam Smith's *Wealth of Nations* sells for a six-figure sum, even though it has the same words as a much cheaper copy you might buy on Amazon.

NFTs have other advantages that are likely to develop over time. We haven't yet discussed blockchains but for now simply think of a blockchain as a public ledger—a place where one can easily look up who owns what. That's useful because it means that a seller of NFTs can always quickly find out who owns them (i.e., their public key address) even when the NFTs have been sold many times. NFTs, therefore, can connect brands to their most dedicated followers and can even act like membership tickets to a club.

The Bored Ape Yacht club is a limited collection of 10,000 NFTs that are signified by a picture of, well, a bored ape. The NFTs have sold for an average price of $200,000. Why would anyone pay so much for a bored ape? Well, owning one of these NFTs makes you a member of a club that includes future giveaways, invitations to real-life parties, and simply the knowledge that you belong to a club that includes Steph Curry, Jimmy Fallon, and Snoop Dogg as members. NFTs, therefore, can connect sellers to buyers but they can also help to create a community. Remember, lots of people bought memberships in yacht clubs even when they rarely sailed.



Mininyx Doodle/Alamy Stock Photo

Here are 3 of the 10,000 Bored Ape Yacht Club NFTs.

Source: https://boredapeyachtclub.com/#/home.

You can also see that NFTs can serve as a system of property rights for internet goods. The concept of a "membership ticket" here is quite general. A ticket might let you post in a particular internet forum or let you decide who else can post in a forum or it might give you ownership of Excalibur in the King Arthur online world and Luke Skywalker's lightsaber in a Star Wars universe. In essence you *own* those rights, and your ownership is securely validated by these cryptographic systems.

If you think that virtual reality or the internet more generally is going to be even more important in the future, plausibly its property rights will be a lot more important, too. So with NFTs we have invented a whole new type of property right. And property rights are a key economic concept, as we have explained throughout this textbook. One reason that we, Tyler and Alex, are interested in NFTs is because we are intrigued that humans have invented a new kind of artwork and a new kind of property right at the same time. Almost nobody was expecting this even 15 years ago.

There are also many experiments going on that tie NFTs to other digital and nondigital assets. Royal.io, for example, is a platform that sells song rights as NFTs. Users can buy NFTs of songs and musicians can earn royalties as their songs increase in popularity. Using NFTs in this way requires connecting NFTs and other digital assets to real-world legal institutions like copyright law and music publishers. It remains to be seen how successful such connections will be but the increased consumption of music online (streaming) does suggest that there are opportunities to use cryptoeconomics to simplify and streamline the royalty process, again helping to solve a property rights problem.

Now, let's imagine that instead of bored apes that someone created a series of NFTs with pictures of presidents much like the picture below.

nimon/Shutterstock.com

As before, each artwork is unique. The artwork shown here, for example, is artwork B03542754F. You will also note that the "artist," in this case Timothy F. Geithner, has signed his artwork.

Now let's imagine that people get bored with looking at presidents and simply just trade the serial number and the signature. Serial numbers aren't very memorable so perhaps after some time, people start to treat every serial number like any other, in other words, serial numbers become fungible. We have now created a type of digital cash.

To make digital cash work well, however, we must also solve the double-spend problem. Or in other words, how do we stop a person from using the same digital signature twice. Using the cryptographic tools we have described, Alice can send Bob a token—which we now know is just a message and a digital signature—and Bob can prove that Alice sent him the token. What Bob can't do, however, is prove that Alice didn't also send the same token to Tom, Dick, and Harry. Or what if Alice tried to use the same digital asset to buy something from both Walmart and 7–11? What is to stop this from happening?

Solving the double-spend problem is easy if Alice and Bob can trust a third party. Let's call the trusted third party, the Trust Bank. The Trust Bank keeps a

set of accounts, a ledger. Every time Alice wants to send Bob a token she routes her message to the Trust Bank. The Trust Bank checks its accounts and if Alice hasn't previously sent the token to someone else it validates the transaction and updates Alice and Bob's accounts. If Alice tries to send the token again, the Trust Bank will mark the transaction as invalid. Easy!

In fact, firms did create digital cash mechanisms similar to what we have just described and some central banks are in the process of creating digital cash along these lines.[3] But what if we don't trust the Trust Bank? We might be worried, for example, that the Trust Bank will secretly change its accounts in favor of some of its members or perhaps in favor of its owners. We can solve this problem by making the ledger public. A public ledger might look something like this:

Day One
Alice 1
Bob 2
Tyler 4
Alice -> Bob +1
Alice 0
Bob 3

Day Two
Tyler -> Alice +1
Alice 1
Bob 3
Tyler 3

Day Three
Bob -> Tyler +2
Alice 1
Bob 1
Tyler 5

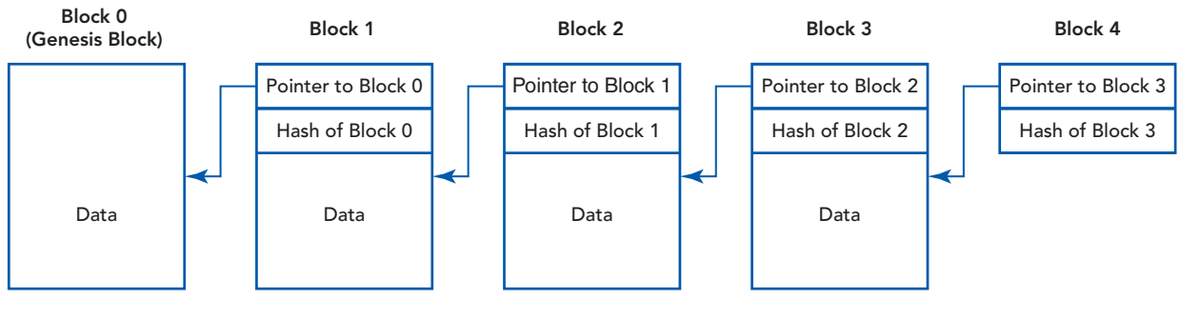
Making the ledger public makes it harder for the Trust Bank to cheat but suppose that the Trust Bank does cheat then we would have to compare their accounts with someone else's accounts, say the accounts of the Super Trust Bank. But how do we know that the Super Trust Bank isn't cheating?

Amazingly, cryptographic hash functions provide a solution to this problem. Remember that a cryptographic hash function takes any data as input and outputs a digital fingerprint of that data, an essentially unique ID such that if any piece of the data is ever changed it won't hash to the same ID. Now generalizing, let's post each day's ledger publicly except now we will call each day a block and let's link each block like the ones shown in Figure 1.[4]

We call this a blockchain. How does the blockchain make our data tamper-proof?

Suppose we are worried that some of the data in Block 1 has been tampered with. We can quickly hash the data in block 1 and compare it with the hash of Block 1 in Block 2. If the hashes match we gain some confidence that Block 1

FIGURE 1



was not tampered with, but how do we know that Block 1 and Block 2 weren't both tampered with? Well, we can hash Block 2 and compare that hash with the hash of Block 2 in Block 3. If those hashes match, that give us confidence that neither Block 1 nor Block 2 have been tampered with (since the hash of Block 2 also contains the hash of Block 1). By the same logic, if the hash of the most recent block matches the hash listed then we can be quite confident that *none* of the previous blocks have been tampered with.

Wait. Did you notice the one way to tamper with a blockchain? Yes, it would be possible to change one piece of data if you replaced *every* subsequent block. Security is never perfect. Nevertheless, what we have shown is that using a blockchain we can create a database that is highly immutable—changing any element in any block requires making changes to *every* subsequent block and that is much more difficult than changing one element of a block. Blockchains, therefore, greatly increase the security of databases and the more blocks subsequent to a given block, the greater the security.

To review briefly. Our digital cash mechanism now works reasonably well. Alice and Bob can send secure messages. Trust Bank can verify their accounts so that double-spends don't happen, and we can verify Trust Bank's accounts using a secure public blockchain.

But notice that we are still relying on the Trust Bank to post the ledger's data to the blockchain and to validate transactions. That gives Trust Bank a lot of power. Even if Trust Bank can be trusted not to fake data, maybe they can't be trusted not to abuse their monopoly. And what happens if the Trust Bank goes bankrupt?

This is where bitcoin comes in. Bitcoin replaces trust in institutions with trust in the invisible hand. Let's see how it works.

Bitcoin

All of the cryptographic tools that we have described, most notably, public-private key cryptography, cryptographic hashes, and blockchains, preceded bitcoin. But Satoshi Nakamoto, the pseudonymous creator of bitcoin, assembled these tools in a new and remarkable way.

In our previous example the Trust Bank validates transactions and assembles them into a publicly verifiable blockchain. Satoshi didn't trust banks, not even Trust Bank. So Satoshi created a mechanism that incentivized individuals and firms all over the world to validate and assemble blocks, thereby maintaining the bitcoin network, and to do so based on self-interest without the intervention of any central guiding hand or authority. In Adam Smith's words, individuals are incentivized to maintain the bitcoin network "as if guided by an invisible hand."

The big picture looks like this. When Alice wants to send Bob a bitcoin she doesn't contact her bank or Visa or Stripe. Instead she broadcasts a message to the bitcoin network that says "I authorize a transfer of bitcoin to Bob. Here's my digital signature." Bitcoin "miners" listen for transaction messages, verify that the transactions are valid and compile them into blocks. In about 10 minutes (we explain why it takes 10 minutes further below) a block with Alice's new transaction will be added to the blockchain. Anyone in the world can then verify that Alice transferred a bitcoin to Bob and if Bob wants to make a subsequent transaction with Tom anyone can verify that he has the funds to do so. Alice has no contract with the miners and they are not obligated to produce blocks. Nevertheless, when Alice broadcasts her message many thousands

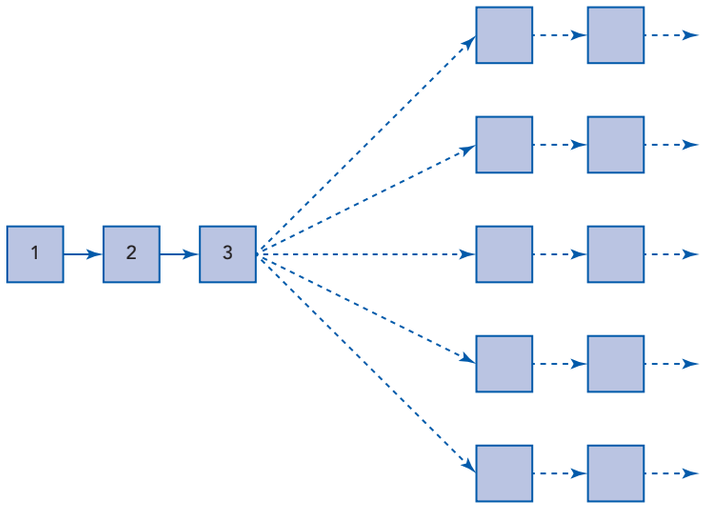
of miners—no one knows precisely how many or who they are—compete to help Alice fulfill her request. Alice doesn't need to trust any bank or intermediary she just needs to trust the invisible hand. Amazing.

Okay, so now let's fill in some of the pieces behind that bigger picture. Validating transactions and assembling them into blocks isn't technically difficult, but it takes some computational resources so Satoshi had to pay the "miners" to perform these services. He couldn't pay miners in dollars—where would the dollars come from?—so he made a leap of faith and paid them in bitcoins. Satoshi programmed the bitcoin code so that each new block in the blockchain created 50 new bitcoins that could be claimed by the miner of that block. (Per the original bitcoin program, the rate diminishes over time—it is currently 6.25 bitcoin per block which will halve to 3.125 bitcoin per block around 2024. The rate will keep halving so that the total supply of bitcoins will never exceed 21 million bitcoins. Bitcoin miners can also earn transaction fees.)

Paying bitcoin miners in bitcoin was a leap of faith because why would anyone want bitcoins? Satoshi gambled that people might be willing to perform services for the bitcoin network as a temporary experiment long enough for the system to take off. The gamble worked. In 2010 bitcoins traded for less than a penny but by 2012 the price had rocketed up to $10, which might not sound like much but that's a phenomenal percentage increase. In November 2021 the price of a bitcoin hit $68,000. You can google "BTC price" to find out the current price, but don't be surprised if it is much higher or much lower.

To earn bitcoins, bitcoin miners race to validate transactions, making sure there are no double-spends, and add blocks of transactions to the chain. In fact, they race too fast. Validating transactions is computationally quick, which leads to situations with many competing blocks as shown in Figure 2. How does the bitcoin network decide which chain is the valid chain? You might think that we could simply use a first to arrive rule but the bitcoin system is decentralized,

FIGURE 2



The blockchain is in consensus up to Block 3 but then five miners offer competing blocks. Which blockchain is definitive?

it lives in computers that are distributed all over the world, so there is no single place where the blockchain is kept, no center to the network, and no single measure of which block was mined "first."

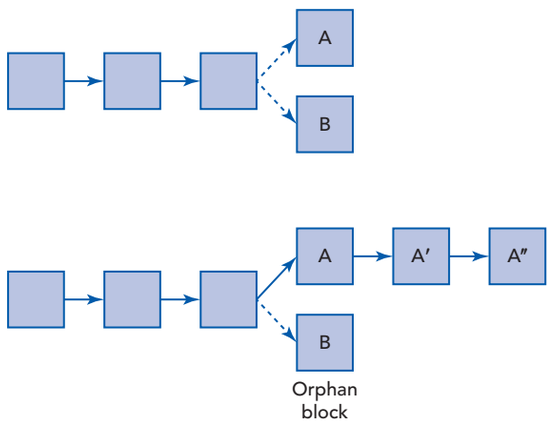
To slow down mining and reduce the potential for competing blocks, Satoshi required that in addition to validating transactions and preparing blocks, miners must also win a lottery. To create the lottery Satoshi used a familiar tool, cryptographic hashes. Recall that cryptographic hashes are as good as random; that is, each input is equally likely to produce any of the possible outputs, numbers running from 0 to 2^{256}. The way to win Satoshi's lottery is simple—hash the data in the block plus a bit of extra text that the miners can adjust to find a "rare" hash.[5] For example, one that starts with many 0's. Each hash is thus a lottery ticket—more hashes, more chances to win the lottery. The first miner to find the rare hash wins the new bitcoins and writes their block to the chain.

In practice, bitcoin miners must try *trillions* of hashes to find the rare hash that wins Satoshi's lottery. It is a part of the system that how rare a winning ticket has to be adjusts over time so that on average it always takes about 10 minutes to find a winning hash and mine a new block. If computers get faster, for example, blocks will temporarily be discovered more quickly but very soon the lottery will become more difficult to win (more 0's will be required in the hash) and the block discovery rate will return to an average of one block every 10 minutes. All of this was built into the original bitcoin "rules of the game," as developed by the ingenious Satoshi.

Adjudicating Competing Blocks?

Before we move on, here is one final complication that is a bit technical but helps explains exactly how the system works. Slowing down block creation makes situations like Figure 2, in which there are three or more competing blockchains, very unlikely but winning the Satoshi lottery is random and it sometimes does happen that two lottery tickets are won in quick succession so that there are two competing blockchains as shown in Figure 3. Which blockchain is the definitive and valid blockchain?

FIGURE 3



A situation in which there are two competing blocks such as A and B in the top panel is soon resolved. The miner who solves the next block must choose whether to build on chain A or B. Suppose they choose A so the new block is A′. Now the chain with A′ is the longest chain and further blocks will build on that chain. Block B becomes an orphan block and transactions in that block are treated as invalid.

The dilemma is resolved by the longest chain norm. The longest chain norm simply states that miners should build on top of the longest chain (technically the chain that required the most hash power to build but longest is close enough).

In Figure 3 for example the top panel shows two potential blockchains with top Blocks A and B. In about 10 minutes a new block will be created. The miner of the new block must decide whether to build on top of A or B. Since the two potential chains are equally long it doesn't matter which. Assume they build on top of A with new Block A′. The key is that now the A′ blockchain is the longest chain and so the next block, A″, will build on that chain. Block B then becomes an "orphan block" and its transactions are regarded as invalid.

But wait. Couldn't the Block B miners get lucky and solve two puzzles in a row and in this way overtake

the A′ chain? Yes. It's possible. But if most miners follow the longest chain norm then the longest chain will soon become longer than any competing chain. Why? Computing lottery tickets (trying new hashes) requires a lot of computing power. If most miners are following the longest chain norm then most of the computing power is following the longest chain norm and so that group will create the longest chain. A group with less computing power might get lucky once or even twice, but over time the group with the most computing power will produce the longest chain.

The bottom line is that there are occasional "orphaned" blocks on the bitcoin blockchain, so if you are making a big transaction you want to wait until the block with your transaction is say six levels deep into the blockchain. A block six or more levels deep is very safe, in essence the data on those blocks is immutable, because the computing power necessary to rewrite six or more blocks is immense. Do you recall earlier when we said a blockchain makes data more secure because tampering with one element requires changing every subsequent block? That is exactly what is going on with the bitcoin blockchain except now we are also making clear that changing a block requires a costly expenditure of computing power.

We need to answer just one more question: Why do miners follow the longest chain norm? The answer is that the longest chain norm is self-sustaining—if other people follow the norm then it is in your self-interest to follow the norm.[6] Miners want to earn the block reward of more bitcoin but miners who mine an orphan block earn nothing. In fact, miners aren't able to spend their rewards until their block is 100 deep into the blockchain. So to earn the block reward, miners must create a block that future miners build upon. If future miners will build upon the longest chain then the best bet for a miner today is to build on the longest chain. It's a subtle argument but in practice quite powerful. It's a bit like driving on the right side of the road or the left. There is no strong reason to favor one rule or the other but there is a very strong reason to follow the rule that other people follow.

Weaknesses of the Bitcoin Protocol

Satoshi combined cryptography with economics to produce a remarkable mechanism that achieves something new, namely *decentralized consensus*. The bitcoin system, taken as a whole, lets everyone in the world come to a consensus about the blockchain, which means everyone can agree about who owns what, or more generally about the data.

These new crypto innovations add to our understanding of decentralized systems. Markets are one kind of decentralized or "invisible hand" system, the economics of unowned natural resources, such as the ocean or the quality of the air can be thought of as another kind of decentralized system, even some aspects of politics are best thought of as a decentralized system. The startling truth behind crypto is that an entirely new kind of decentralized system involving both economics and computer science has been invented, and it dates from as recently as 2009.

At this point it is worth considering a few issues or potential problems with bitcoin:

Is Bitcoin a Bubble?

Some critics have charged that high bitcoin prices reflect bitcoin as a bubble or even a kind of fraud. But bitcoin prices have been high now for years, and they

have bounced back repeatedly from major downward swings. Usually once a true bubble bursts, it doesn't come back at all. At the very least, bitcoin seems to be proving itself as a store of value, thereby giving some backing to its market price.

It is estimated there is about $8 trillion worth of gold in the world, and most of that is held for purposes of investment and speculation, rather than it all going into tooth fillings.[7] It doesn't seem crazy for the stock of bitcoin to have some percentage of gold's value; after all, bitcoin is a kind of digital gold because of its limited supply and it has become a well-known, focal asset, just as gold is. Bitcoin bulls, of course, think bitcoin is likely to displace more of the gold market as a store of value, while bitcoin bears hold the opposite view.

Slow Processing Speed and High Transaction Costs

Satoshi wanted bitcoin to be used for ordinary payments, such as buying a coffee, but it's now clear that the current network is too slow and expensive for small payments. The 10-minute average time it takes to find a new block helps the network to achieve consensus, but it has come at a price. Satoshi limited blocks to 1 megabyte (mb) in size and transactions take about 500 bytes each so a block is limited to about 2,000 transactions. Bitcoin, therefore, can process about 2,000 transactions in 10 minutes or 3.3 transactions per second. You can't run Christmas on 3.3 transactions per second! In comparison, credit card networks like Visa and MasterCard regularly handle 5,000 or more transactions per second.

Other networks, sometimes called Layer 2 networks, are working to increase the speed and scale of transactions while still using bitcoin as the ultimate settlement layer, but it remains to be seen whether it will be better to extend bitcoin or use another network built explicitly for payments.

Energy Cost

At a bitcoin price of around $40,000, the bitcoin network computes about 200 million trillion hashes per second or 200 quintillion hashes per second! That's a lot of computing power and no one wants the results of these quintillions of hash computations. The computations are wasted or least not used for any purpose other than securing the bitcoin network.

You will sometimes read that bitcoin uses as much electricity as a small country. That's true but it's mostly a reflection of how cheap electricity is. At a price of $40,000, bitcoin spends on the order of $10 billion on electricity annually. $10 billion in spending is less than the world spends on toothpaste ($30 billion), much less than the United States spends on cigarettes ($80 billion), and considerably less than the U.S. federal government spends in one day ($18.65 billion). $10 billion is about the same as the United States spends on Halloween costumes every year. $10 billion isn't negligible and bitcoin's resource cost rises with the price of bitcoin, but $10 billion isn't earthshaking.

MARK FELIX/AFP/Getty Images

The Whinstone bitcoin mine in Rockdale, Texas, is the largest bitcoin mine in North America.

Even though the total resource cost of bitcoin isn't enormous, the per transaction cost is high relative to other payment systems. Visa, for example, can process transactions for about 16 cents per transaction. In contrast, as we write this chapter, the typical bitcoin transaction has a social cost of about $130.[8]

The 51% Attack Problem

Finally, let's discuss a more technical problem. A bitcoin miner that controls 51% of the computing power can execute a double-spend attack. In a double-spend attack, the attacker sells bitcoins for dollars. As soon as the attacker has received the dollars and the bitcoin transfer has been registered in a block—call this Block B—the attacker creates a competing block that does *not* include the bitcoin transfer, call this block A for "attacking." If the attacking miners get lucky and are able to mine the next block then they will follow block A with block A′ which makes their chain the longest. Block B containing the transfer of bitcoins is then orphaned—it's as if the transfer never happened. This is exactly what is shown in Figure 3 from earlier except now the competing block wasn't an accident of timing but was planted on purpose by the attackers.

Remember when we said that someone who receives a lot of bitcoins should wait at least six blocks to be secure? Well that's true because it means that an attacker must replace at least six blocks and probably many more before the attacking chain becomes the longest chain but if the attacker does have 51% of the computing power it's only a matter of time before that happens. It's actually somewhat surprising that there haven't been more double-spend attacks on the bitcoin blockchain.

One thing to keep in mind is that a double-spend attack can make it as if a transaction never happened but it can't otherwise steal bitcoins or transfer them. Only someone with the private key can transfer the bitcoins associated with that account. Another reason why bitcoin might not be attacked is that a double-spend attack might cause the value of bitcoin to fall precipitously, leaving the thieves with much less than they expected.

It's also unlikely that any one person could ever control 51% of the bitcoin computing power. A group of miners could collude to form a mining cartel but the cartel would then have to agree on who gets how much from any attack and that might prove difficult (no honor amongst thieves!) as we describe for cartels more generally in Chapter 15.

Even though 51% attacks are rare on the bitcoin network they have happened on other networks.

Governing Cryptocurrencies

One of the advantages of decentralized networks like bitcoin and Ethereum is that they aren't owned by anyone, not even a big corporation. But this also raises the issue of how these networks are to be governed and improved over time and, as of yet, that is mostly an unsolved problem with lots of experimentation going on.

Blockchains do have methods for voicing disagreements and changing rules but those methods are fairly "crude". Satoshi Nakamoto famously disappeared shortly after creating bitcoin, which emphasized bitcoin's decentralized and fixed nature: It worked more or less the way Satoshi designed even with no one in charge. Other cryptocurrencies have more procedures for evolving. Vitalik Buterin is the co-founder of the Ethereum protocol and he is commonly regarded as the movement's intellectual leader. Unlike Satoshi, Vitalik is his real-world name and he hasn't disappeared.

As a result, the Ethereum protocol continues to evolve under the guidance of Buterin and others, especially the Ethereum Foundation. The Ethereum Foundation coordinates the Ethereum community around new rules and standards

and it updates those rules on a regular basis and tries to improve them. The Ethereum platform is thus more of a "moving target" than is bitcoin when it comes to explaining it. For instance, the Ethereum chain currently uses a fairly high-cost "proof of work" algorithm just as does bitcoin, but there are plans (not yet realized at the moment of writing) to move it to a very different system known as "Proof of Stake." We'll see when that happens, but odds are that Ethereum will change more than bitcoin over time.

Some observers prefer the fact that the Ethereum platform can adapt and change to new developments under the guidance of the Ethereum Foundation while others prefer the more difficult to change bitcoin. Bitcoin can and has improved over time but it's a slower and more decentralized process than with Ethereum, making bitcoin a more conservative platform.

When disagreements cannot be resolved by voice they may be resolved by exit. A sufficiently large group of miners who think a change in the rules would be beneficial may copy the blockchain code, change it, and then branch or "fork" into a new blockchain. For instance, Bitcoin Cash split off from bitcoin proper, under the premise that different rules would make it easier to use for smaller retail transactions. So now we have both Bitcoin Cash and original bitcoin. Bitcoin Cash hasn't been that successful in either being used for transactions, or for that matter in attracting general interest and support. Nonetheless it still exists, and so a single crypto asset may split into multiple assets. Forking is like dissidents leaving for a new country and it's a one reason why blockchains evolve rapidly. How easy should it be to create a new country or a new blockchain? The potential to fork a blockchain can be a check on monopoly power but it may also be a threat to stability.

Beyond Bitcoin

The success of bitcoin spurred on the creation of other faster, more capable, and less energy-intensive blockchains such as Ethereum, Solana, Elrond[9], and Avalanche, among others. Now let's turn to some of the economic innovations that new blockchains make possible.

Ken Howard/Alamy Stock Photo

A smart contract is like a vending machine. Insert your money ("gas") and it will automatically perform many wonderful and amazing feats and maybe even make you a fortune.

The Rise of Smart Contracts

If bitcoin can be thought of as an invisible hand process for transferring money, the new blockchains are invisible hand processes for performing more general forms of computation. The new blockchains are like having "a giant computer in the sky," and one that anyone can access, as computer scientist Tim Roughgarden put it.[10]

Anyone in the world can write a smart contract and deploy it to one of the newer blockchains like Ethereum. Once deployed, anyone can then interact with that smart contract by paying the "gas" required for computation. Interacting with a smart contract is something like using a vending machine—put your money in and the vending machine will operate automatically.

A smart contract is a kind of contract where the performance is guaranteed by software instead of by lawyers and judges. For example, consider a simple insurance contract: Alice pays Bob 1 ETH [the cryptocurrency ether] today, but if the temperature in Washington, DC, falls below 15°F for five days in a row in March 2025, then Bob pays Alice 4 ETH.

One virtue of this contract is that the funds can be held by the smart contract in the form of collateral so there is no question that Bob will pay if he is

supposed to. Once the contract has been entered into it is self-enforcing and executed by the software. On the other hand, if the contract is made in Fahrenheit when Alice and Bob meant Celsius, it will still execute regardless of what the parties originally may have wanted.

Smart contracts need to be written very carefully! It's also not as easy as it sounds to prove what the temperature was in March 2025 in Washington, DC. Sure, it's easy for a human to look that information up, but it's more difficult for a software-based smart contract to be able to access that information and know that it is valid and hasn't been tampered with. In the blockchain world this is known as the Oracle problem and it is an active area of research and also a potential obstacle for the growth of smart contracts.

It is true that insurance companies, or other intermediaries, can perform the same functions as smart contracts but the hope is that smart contracts can work more reliably and at lower cost. Furthermore, these smart contracts can be made across international borders without tariffs or other trade restrictions. At least as it stands at the time of writing, smart contracts are bringing a form of automatic free trade and free capital movements to many financial services.

Smart contracts have made especially significant inroads into decentralized finance or DeFi, so let us now turn to that topic.

An Introduction to Decentralized Finance (DeFi)

Decentralized Exchanges

Traditional, centralized exchanges like the New York Stock Exchange (NYSE) trade securities using order books. In an order book, buyers post *bids* indicating the price and quantity at which they are willing to buy and sellers post *asks* indicating the price and quantity they are willing to sell. When a bid exceeds an ask there is a sale.

Order books can be run on blockchains but for a variety of reasons decentralized finance has pursued an innovative and surprising alternative method of trading securities. On a decentralized exchange like Uniswap or Curve, traders trade not with each other but with a smart contract known as an Automated Market Maker (AMM). We'll explain the details in a moment, but the general point is that blockchains have become a platform to support new market innovations, just as the internet served as such a platform to support innovations such as Amazon and Facebook and eBay.

AMMs come in different forms but we will focus on the simplest, the constant product AMM. The constant product AMM for assets X and Y holds reserves of the two assets, R_x and R_y, and it allows any trade on a curve such that:

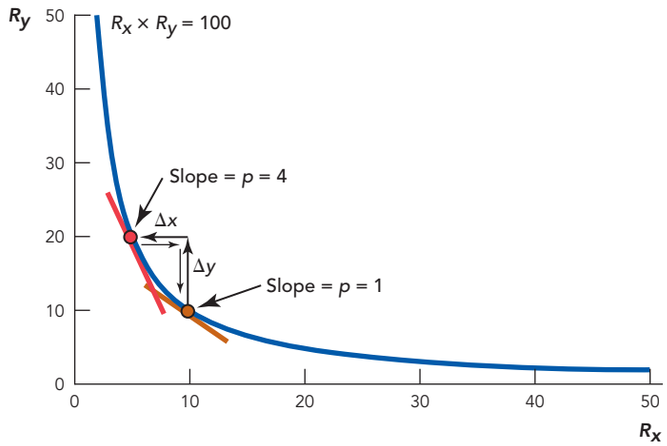
$$R_x \times R_y = c$$

where c is a constant.

Suppose, for example, that the AMM starts with equal values of the two assets so that say $R_x = \$10$, $R_y = \$10$ and thus $R_x \times R_y = c = \$100$. Then the AMM offers trades along the curve shown in Figure 4. If a trader sends Δy to the smart contract they receive Δx in return or vice versa. Any trade is allowed so long as the trade begins and ends on the curve.

Now at first trading using an AMM seems ridiculous. The price on an AMM is a simple function of math. In Figure 4, buyers send Δy to the AMM and receive Δx so the price of x is just the slope of the curve, $\frac{\Delta y}{\Delta x}$. Notice that as

FIGURE 4



A constant product automated market maker lets traders make any trade along a given curve such as $R_x \times R_y = \$100$. As they do so, the implicit price changes.

people buy x by sending y to the smart contract the price of x goes up which makes some sense but the relationship is purely mechanical. Shouldn't prices be set by supply and demand?

The puzzle is resolved by arbitrage. Arbitrage keeps AMM prices close to market prices. If traders start purchasing lots of x, thus increasing the price of x on the AMM and perhaps exceeding the "market" price, arbitrageurs will step in and send x to the AMM and receive lots of y in return. Thus, there are profits to be made from trading with an AMM to bring it closer to the "true" price.

Arbitrage in DeFi works especially well because in DeFi it's possible for anyone in the world to borrow millions of dollars without any collateral. Now to be sure, anyone can't borrow money to fund a vacation but it is possible to borrow millions of dollars for arbitrage in what is called a flash loan. Flash loans are another innovation that DeFi has brought to the world.

You might wonder where the initial reserves for the AMM, R_x and R_y, come from and why anyone provides those reserves. The people who provide reserves are called *liquidity providers* and the AMM is coded so that providers get a percentage of every trade. Anyone in the world can trade with an AMM and anyone with funds on a blockchain can be a liquidity provider. Notice, that once the smart contract has been deployed to the blockchain it runs essentially by itself—attracting traders and liquidity providers in a decentralized manner.

Using AMMs to trade securities is very new and strange but it does have several advantages. Order books require thick markets which is one reason why the NYSE is only open from 9:30 AM to 4 PM daily and not on weekends or holidays. By restricting its hours, the NYSE concentrates traders making the market thicker. In contrast, since AMMs are run by smart contracts they can be available 24 hours a day, 365 days a year, and from anywhere in the world.

Another big advantage of AMMs and smart contracts (SC) is that they are "composable"—meaning one SC can call another SC. Here's a simple example, if we have a \$/BTC AMM and a BTC/Egld AMM then by sequential trade we

have a $/Egld AMM. A more complex example is a smart contract mutual fund that invests and trades in multiple assets according to a fixed set of rules. Composability makes it possible to create sophisticated financial contracts by putting together smart contracts like Lego blocks. More generally, since code uploaded to a blockchain doesn't go away each new smart contract added to the system adds to the potential capabilities of every other smart contract.

AMMs are very new. Buterin sketched the idea in a Reddit post in 2017 (based in part on earlier ideas from our colleague Robin Hanson). Uniswap, the quantum leap in this field, launched in November 2018. Not only is the field new, it is changing rapidly. The rapid pace is not an accident. Anyone in the world can launch a Uniswap competitor and many people have, bringing new ideas to the field. Uniswap responded by creating more powerful method of liquidity staking in Uniswap3. By the time you read this, there will be more innovations.

The DeFi markets are still small relative to traditional markets, which trade trillions of dollars' worth of securities every day. But in just a few years, AMMs went from nothing to more than a hundred billion dollars in liquidity provided. DeFi is a field dominated by creative destruction, namely that new products displace older products at a high rate. The future will be interesting.

DeFi Borrowing and Lending

Traditionally you apply for a loan by filling out some forms and meeting with a loan officer. The loan officer will check your identification, your credit score, your bank statements, your tax payments—maybe even your SAT scores. If all goes well, and if you can post some collateral and agree to further conditions giving the bank certain rights, you might sign a contract and get a loan—see Chapter 31 on financial intermediation.

That's the traditional world. In the new DeFi world, every day anonymous people and organizations borrow and lend billions of dollars on decentralized blockchains *without any paperwork*. MakerDAO, for example, is a decentralized autonomous organization (DAO) built on the Ethereum blockchain that lets *anyone* in the world borrow DAI, a stablecoin that is tied to the U.S. dollar.[11] How is this possible?

Well, there is a catch. To borrow DAI you must put up other cryptocurrencies as collateral and you must put up a greater value of collateral than you borrow. In other words, you need say $300 of collateral in order to borrow $100 worth of DAI. That's a limitation but people still want to borrow because they want to increase their leverage or because their collateral might not be as liquid or as convenient as using a stablecoin like DAI. Moreover, the borrowing and lending are entirely run by a smart contract so there's no paperwork or loan officers.

Notice that once the smart contract has been deployed to the blockchain it runs on essentially the same general principles that enforce the integrity of blockchains for bitcoin transfers. For instance, if you do not repay your loan on time, a message will be sent transferring some or all of your collateral to the lender, the miners in the system will validate that message, new blocks will be created in the blockchain, and in those new blocks the delinquent borrowers have lost some resources. If you want to pick up the phone and cry and complain to somebody, good luck!

Borrowing and lending without any paperwork or identification is remarkable, but how about borrowing millions without any collateral? As we

mentioned earlier, this is also possible in the DeFi world but you must borrow and lend quickly. Flash loans are loans that are made and repaid in one combined transaction so that if the loan can't be repaid then it is never made. Flash loans are an entirely new financial innovation.

DeFi and Development Economics

Traditional finance relies on legal documents like contracts, titles, and personal identification and thus it ultimately relies on a legal system that can enforce those contracts quickly, reliably, and at low cost. Relatively few countries in the world have all the required abilities, which is why traditional finance clusters in a handful of places like New York, London, Singapore, and Zurich.

Decentralized finance, in contrast, relies on smart contracts and cryptographic identification that work exactly the same way everywhere. Decentralized finance, therefore, could be broader based and more open than traditional finance. Indeed, decentralized finance could prosper in precisely those regions of the world that do not have reliable legal systems or governments with the power to regulate heavily.

Decentralized finance, especially lending and borrowing, may also connect the world at lower cost than traditional finance, offering opportunities for both borrowers and lenders. DeFi borrowing and lending has mostly been lending one cryptocurrency for another, often for speculative purposes. But the idea of software replacing more expensive and slower human beings is a general one and DeFi lending is starting to be applied more globally.

Here is one simple way to look at it. Many higher-income Americans have a lot of money just sitting around in their bank accounts, basically earning zero interest or even paying fees to the bank. Now look abroad to poorer parts of the world, where poorer people typically are borrowing funds through microcredit and paying annualized interest rates often ranging from 50% to 100%. Wouldn't some of those Americans, at least in principle, like to lend a modest percentage of their funds to much poorer borrowers, say in Latin America or Africa? Those loans might be riskier, but in fact most microcredit loans, often more than 95%, are paid off in a timely manner.[12] If you staked 5% of your checking account on such a venture, that might seem attractive to many Americans.

Under the status quo, lending out those funds globally to the poor is not easy. For one thing, your bank probably is not in touch with the potential borrowers. Your bank also might have a hard time getting a legal license to lend in those countries, and there would be numerous other obstacles of distance, language, bureaucracy, monitoring, and so on. It's probably just not going to happen.

But blockchains and crypto hold some promise here. It is true that most of the world's poorer individuals, especially those who need to borrow money, are not actively trading on blockchains. But it may be possible to introduce software-based intermediaries to make indirect blockchain access easier. For instance, most of Kenya already is connected to a system of electronic "mobile money," using their smart phones. That mobile money is regular money rather than blockchain money, but is it so impossible to imagine a new intermediary that connects Kenyan mobile money to a blockchain? Of course, the more intermediaries enter the picture, the lower your rates of return as a lender. Still, there is a large gap between the near zero rate Americans earn on their bank

accounts, and the 50% to 100% rates paid by many borrowers. It seems that there are large additional gains from trade if blockchains can reduce transaction costs.

In short, one of the major promises of the blockchain revolution is a reallocation of capital to the parts of the world with higher yields and higher rates of return. This has not yet happened, but it is one reason why blockchains have at least the potential to tie into a central concern of macroeconomics, namely boosting economic growth and increasing gains from trade. Most generally, cryptocurrencies span countries so the concept of cross-border capital flows makes less sense the more that we come to live in the "metaverse."

Takeaway

The technologist Marc Andreessen has argued that "software is eating the world" and that includes software written to a blockchain. If blockchains and smart contracts can reduce transaction costs in payments, borrowing and lending, and buying and selling securities then they can have a big effect on money, banking, and finance. It's possible that most assets—stocks, bonds, real estate, and more—will move online and be represented by a token ("coin") on a blockchain and traded on an AMM or something similar—this trend is sometimes called the "tokenization of everything."

Cryptoeconomics combines cryptography and economics to produce new methods of communication, cooperation, and organization. Without the security of public key exchange, the modern internet would not be possible. Satoshi Nakamoto showed how cryptographic primitives like cryptographic hash functions and digital signatures could be combined to produce something new, namely a reliable form of decentralized consensus. Satoshi used decentralized consensus to create bitcoin, which is in essence an invisible hand process for transferring money.

Bitcoin hasn't fulfilled Satoshi's original goal of creating a money for "small casual transactions," but it has become a tremendous store of wealth with a market capitalization circa 2022 of about $700 billion. Even more importantly, bitcoin led to new blockchains capable of executing smart contracts, invisible hand processes for computation. Smart contracts hold the potential of replacing costly intermediaries with less costly code. Integrating smart contracts on a blockchain with legal contracts and regulation will be an important step in making these technologies widespread and more useful.

In all of these crypto and blockchain areas, there are at least two kinds of uncertainty. The first is how effectively crypto and blockchain innovators will be able to capture additional gains from trade. The second question is how the authorities will regulate these markets. Cryptocurrencies and decentralized finance are not immune to problems of traditional finance including bubbles, excess leverage, and bank runs. Thus, as these markets get bigger, we may expect more regulation. As regulation increases on crypto innovations that may slow their future growth and also make traditional and decentralized finance more similar. Governments may also create new digital currencies of their own, sometimes called central bank digital currencies (CBDCs), which will be convenient but won't necessarily have the privacy or security of an unregulated digital currency like bitcoin or ZCash.

Most of all, we would stress the point that these markets are changing rapidly. We've given you some basics, but the latest innovations require you to pay close attention to the markets as they are evolving.

FURTHER READING

A good introduction to cryptoeconomics is:

Schar, Fabian and Aleksander Berentsen. 2020. *Bitcoin, Blockchain, and Cryptoassets: A Comprehensive Introduction*. Cambridge, MA: MIT Press.

More details and cryptography can be found in:

Narayanan, Arvind, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. 2016. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton, NJ: Princeton University Press.

A useful history of key cryptographic primitives is:

Narayanan, Arvind, and Jeremy Clark. 2017. "Bitcoin's Academic Pedigree." *Communications of the ACM* 60(12): 36–45. https://doi.org/10.1145/3132259.

A game theoretic discussion of the long chain norm and whether it is a Nash equilibrium can be found here:

Eyal, Ittay, and Emin Gun Sirer. 2013. "Majority Is Not Enough: Bitcoin Mining Is Vulnerable." *ArXiv:1311.0243 [Cs]*, November. http://arxiv.org/abs/1311.0243.

Many of the original papers on cryptoeconomics are technical but well worth reading including:

Adams, Hyden, Noah Zinsmeister, Moody Salem, River Keefer, and Dan Robinson. n.d. "Uniswap v3 Core." https://uniswap.org/whitepaper-v3.pdf.

Buterin, Vitalik. 2013. "Ethereum Whitepaper." Ethereum.org. 2013. https://ethereum.org.

Diffie, Whitfield, and Martin Hellman. 1976. "New Directions in Cryptography." *IEEE Transactions on Information Theory* 22(6): 644–654. https://doi.org/10.1109/TIT.1976.1055638.

Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." October 31, 2008. https://bitcoin.org/en/bitcoin-paper.

Rivest, Ron L., Adi Shamir, and Leonard Adleman. 1978. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." *Communications of the ACM* 21(2): 120–126. https://doi.org/10.1145/359340.359342.

To follow new developments in crypto, it is often necessary to camp out on Twitter and follow whoever are the most interesting people in the crypto space at the time. You can type crypto terms into Twitter search to get an idea of what is going on at any moment, and to see who is generated the most interesting comments.

Notes

1. Publius was used by Madison, Alexander Hamilton, and John Jay. Most historians think that *Federalist 51* was written by Madison. To simplify the story we proceed as if only Madison used the Publius pseudonym.
2. https://blog.psacard.com/2019/09/17/do-player-autographs-add-value-to-a-card/.
3. See Chaum et al. 1990; Wirdum 2018; and Bech and Garratt 2017.
4. Source: https://medium.com/@zhaohuabing/hash-pointers-and-data-structures-f85d5fe91659.
5. Remember that changing just a comma in *War and Peace* changes the entire hash. Thus, each block also includes a bit of empty space that is included in the hash. The miners fill the empty space with random data until they find a hash that satisfies the rare condition. A bit of random data added to data that you want to hash is called a nonce or salt.
6. Thus, the longest chain rule is a Nash equilibrium (see Chapter 15) or at least close to one. It's possible that some sophisticated strategies are better than following the longest chain rule but in practice these do not appear to be important (Ittay and Sirer 2018).
7. https://www.statista.com/statistics/1125923/global-market-value-of-gold/#:~:text=The%20total%20market%20value%20of,global%20market%20value%20of%20gold.
8. The social cost is the cost to society of making the transaction, which includes the costs of electricity and computers that the miners use. The cost to a user of bitcoin can be quite low, say, $4 per transaction.
9. One of the authors, Alex Tabarrok, is an advisor to the Elrond blockchain.
10. https://twitter.com/algo_class/status/1487075264828002307.
11. In case you are wondering, a stable coin is a coin that by design trades 1 for 1 with the dollar, and a DAO is itself a new form or organizational structure that lets people run a firm or organization without a CEO or large bureaucratic structure.
12. See https://www.vox.com/future-perfect/2019/1/15/18182167/microcredit-microfinance-poverty-grameen-bank-yunus, on repayment rates.