Members Only

AN INFORMATIONAL BRIEF PREPARED FOR MEMBERS OF THE OHIO GENERAL ASSEMBLY BY THE LEGISLATIVE SERVICE COMMISSION STAFF

Volume 133 Issue 2
March 12, 2019

Blockchain Technology and Virtual Currency

Prepared By: Yosef Schiff, Attorney
Reviewed By: Michael J. O'Neill, Division Chief

Summary

The creation of Bitcoin in 2009 ushered in a new era of technological and financial disruption. The first successful virtual currency, Bitcoin laid the groundwork for other virtual currencies and the use of digital ledger technologies like blockchains more broadly.[1] At its heart, blockchain technology is simply a way of keeping records on a decentralized ledger. Despite this apparent simplicity, however, blockchain technology has opened the door to transforming various industries, especially finance and banking.

Since Bitcoin's inception, federal and state regulators have been taking various approaches to regulating actors in the blockchain and virtual currency space. This memorandum explains how blockchain technology works, its various applications including virtual currency and smart contracts, and the current state of regulation.

The first successful virtual currency, Bitcoin laid the groundwork for the use of blockchain technology more broadly. A blockchain is simply a type of decentralized database.

TABLE OF CONTENTS

A blockchain secures information against future alteration.

Ohio law

In 2018, the Ohio Treasurer of State launched OhioCrypto.com, reportedly making Ohio the first state to accept tax payments in virtual currency.[2] The website allows taxpayers to pay their state business taxes in virtual currency.[3] Also in 2018, the General Assembly amended the Uniform Electronic Transactions Act to specify that records secured by blockchain technology are electronic records and that signatures secured by blockchain technology are electronic signatures for the purposes of that Act.[4] There are currently no other regulations relating to virtual currency or blockchain technology on the books in Ohio.

Virtual currencies allow user anonymity and peer-to-peer transactions.

Digital ledgers and blockchains

The technology behind Bitcoin is commonly referred to as "blockchain technology." However, blockchain technology is actually one specific type of distributed ledger technology. A distributed ledger is a completely decentralized database that is shared and maintained by each individual computer on a network. Put another way, digital ledger technology is really just a very specific kind of recordkeeping technology in which every user has its own copy of the database; there is no one "official" version on some centrally located server. A distributed ledger is useful for recording certain types of information such as transactions or changes in ownership without the need for a central authority to verify the information. Various technologies have been developed that facilitate decentralization, one of which is blockchain technology.[5] In the case of Bitcoin, the information being recorded is ownership of the bitcoins transferred in a transaction.

On a distributed blockchain-based ledger, information is added to the shared ledger in "blocks." A block contains a group of transactions or messages along with additional information to aid in validating the legitimacy of the transactions or messages (with Bitcoin, the process of validating is called "mining"). Once the block is validated, it is "chained" to the most recent block in such a way as to prevent any future alteration of the information in that block, hence the moniker "blockchain." Chaining blocks together involves a mathematical process called "hashing" that allows you to link one piece of information to another such that any change to the earlier information breaks the link, making it obvious that an alteration occurred. Any attempt to cover up an alteration would require vast amounts of resources in the form of computing power or money.

Blockchains and other types of distributed ledgers have a number of actual and potential uses including virtual currency, smart contracts, and property record management.[6] The remainder of this memorandum addresses the use and regulation of blockchain technology in particular, as it is by far the most prevalent kind of decentralized ledger used for virtual currency and smart contract applications, although related technologies are on the rise. The addendum to this memorandum explains how blockchains operate in detail, using a bitcoin transaction as an example.

Virtual currency – federal regulation

Bitcoin was the first widely successful virtual currency, which is a type of digital money that is not issued by a government and that typically utilizes cryptography for security. Other features commonly associated with virtual currency include:

- The ability to mask the identities of parties to a transaction;
- A tamper-resistant record of transactions;
- The ability to transact on a completely peer-to-peer basis, i.e., without the need for a bank or other trusted third party;
- Irreversible transactions (in contrast to something like a credit card transaction, which can be reversed).[7]

Notably, despite its ostensible function as a medium of exchange, virtual currency is more often traded like an asset than used as money, and federal regulation treats it as one or the other depending on the context. Also of note is that federal regulation of blockchain technology is almost, if not entirely, concerned with its financial and investment applications.[8]

Virtual currency as money

Bitcoin was originally envisioned as a purely digital form of money that did not require banks or other trusted third parties to function. However, no virtual currency constitutes legal tender in the United States. Unlike dollars, creditors are not required to accept virtual currency as payment, although they may choose to do so. In addition, for a number of reasons including high price volatility and slow transaction speeds, virtual currency is primarily traded as an asset.[9]

This primary use raises a question: if virtual currency is only rarely used as a medium of exchange and is instead primarily traded as an asset, is it money? In 2013, the U.S. District Court for the Eastern District of Texas answered affirmatively: despite the dearth of merchants and other businesses accepting Bitcoin, it is nonetheless money because it can be and sometimes is used as a medium of exchange and can also be exchanged for conventional currencies. Consequently, Bitcoin's status as money subjected it to the federal securities laws that apply to investment contracts.[10]

However, virtual currency may also be considered a security or commodity. Its status in a particular case is important for determining what regulations apply.

Virtual currency can be regulated as money, a security, or a commodity, depending on how it is used.

Virtual currency as a security

In March 2018, the U.S. Securities and Exchange Commission (SEC) issued a public statement regarding regulations that online trading platforms must follow if the platforms allow users to buy and sell tokens issued through initial coin offerings (ICOs). An ICO is a fundraising mechanism by which a company looking to create a new virtual currency, app, service, or other product offers digital tokens in exchange for either conventional currency or virtual currency. The tokens can then be traded like traditional securities or used for purchasing goods or services from the company.[11]

Initial coin offerings (ICOs) resemble traditional initial public offerings (IPOs). ICO tokens may qualify as securities.

The IRS treats virtual currency like property for tax purposes.

Virtual currency activity may be subject to anti-money laundering laws, election laws, or various other federal laws.

In its statement, the SEC said that if digital assets are being traded on a trading platform *as if* they are securities, then they *are* securities and the trading platform and any company offering such assets must comply with the various securities laws.[12]

This holding means that an ICO is not necessarily an offering of securities. If the tokens are marketed and purchased with the expectation that they will increase in value as a result of the business's success, then the ICO is more likely to qualify as an offering of securities. If, however, the tokens are marketed solely for use on the company's platform and are actually used that way – i.e., not resold as investments that will gain value as a result of the business's success – the ICO is less likely to qualify as an offering of securities. The takeaway is that like any other offering, if an ICO meets the elements of an offering of securities, it will be treated as such.[13]

Virtual currency as a commodity

The U.S. Commodity and Futures Trading Commission (CFTC) has determined that virtual currency is a commodity in certain circumstances, giving the CFTC jurisdiction over certain virtual currency products, like virtual currency futures. In a 2015 order issued against Coinflip, Inc., an online platform for trading Bitcoin options contracts, the CFTC made two important holdings. First, the CFTC defined "virtual currency" as "a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value, but does not have legal tender status in any jurisdiction," thereby differentiating it from what the CFTC calls "real currency." And second, the CFTC held that virtual currencies are commodities under the Commodity Exchange Act of 1936,[14] and are therefore subject to the various commodity futures regulations.[15] The takeaway here is similar to the takeaway in "**Virtual currency as a security**" above: if a virtual currency is being used like a commodity, then it *is* a commodity and the CFTC has jurisdiction.

Virtual currency and taxes

The U.S. Internal Revenue Service (IRS) treats virtual currency as property for tax purposes. In a 2014 Notice, the IRS stated, "general tax principles applicable to property transactions apply to transactions using virtual currency."[16] In particular, this means three things. First, virtual currency transactions must be reported like any other payment made in property. Second, payments made in virtual currency to employees and independent contractors are taxable. And third, if a virtual currency is held as a capital asset like a stock or other investment property, it is subject to the capital gains tax rules.[17]

Virtual currency and money laundering

Under the Bank Secrecy Act of 1970, financial institutions must meet strict recordkeeping and reporting requirements that are aimed at preventing and detecting money laundering activity.[18] The regulations implementing the Act along with guidance issued by the Financial Crimes Enforcement Network (FinCEN) specify that money transmitters are financial institutions for purposes of the Act, and that persons dealing in virtual currency may qualify as money transmitters depending on the circumstances. In essence, FinCEN's guidance is similar to the SEC's and CFTC's: if a person transmits virtual currency in such a way that the person would qualify as a money transmitter had the person been transmitting conventional currency, then that person is a money transmitter and is therefore subject to the Act.[19]

In its guidance, FinCEN made two other important points. First, it stated that a person that creates a decentralized virtual currency like Bitcoin and exchanges it for real currency or its equivalent is a money transmitter for purposes of the Bank Secrecy Act. And second, although virtual currency is similar to real currency, certain provisions of the Act that contemplate legal tender currency only do not apply in the virtual currency context.[20]

Other federal laws

Various other federal laws are implicated in virtual currency activity in various ways. For instance, the Federal Election Commission held that subject to certain requirements, a political action committee may accept contributions in the form of Bitcoin.[21] And it is currently unclear whether the Stamp Payments Act of 1862,[22] which prohibits the use of certain alternative forms of money, applies to the issuance of nonphysical digital tokens.[23]

Blockchain technology in general and virtual currency in particular are continuing to develop and regulators are still in the process of understanding their implications. As the technology and markets mature, so will the regulations.

Smart contracts and other uses of blockchain technology

Blockchain technology is useful for more than just virtual currency applications. It also facilitates the use of so-called "smart contracts." A smart contract is a computer program that executes a set of instructions, often in the form of contractual terms, automatically as real-world events unfold. Because blockchains allow recordkeeping without the need for a central authority to verify those records, they provide a way for smart contracts to operate automatically and in a decentralized manner. In fact, a virtual currency transaction is actually an example of a smart contract. There are, however, other more complex examples.[24]

In addition to virtual currency, blockchain technology also facilitates the use of smart contracts. A smart contract is a computer program that executes instructions as real-world events unfold.

For instance, in the process of leasing an apartment, an agreement is executed, the tenant writes a check, and the landlord hands over a key. These actions could all be automated via a smart contract: upon affixing digital signatures to an electronic lease agreement, a virtual currency transaction is executed and a smart lock on the apartment is set to allow the tenant entry via fingerprint, code, or other method. In this case, the money transfers instantly, and presumably with less risk because no banks are involved; if the tenant has the funds, they are immediately and irrevocably transferred. If the tenant lacks the funds, they are not transferred and the remaining conditions in the smart contract remain unexecuted. There are no checks to bounce at a later date. The use of a smart lock integrated into the blockchain ensures that the landlord cannot restrict the tenant's access to the apartment or grant others access so long as the funds are transferred. Other aspects of an apartment lease could be automated in a similar manner.[25]

Smart contracts can make property transactions, financial transactions, voting, supply chain management, and other areas more efficient. But they carry risk, as well.

Of course, this level of automation carries other risks. For example, what if the smart contract is executed, the tenant is scheduled to take possession in one month, but the property is condemned after only a week? If this contingency is not programmed into the smart contract, it will execute nonetheless and the landlord will have the tenant's money, but the tenant will be unable to take possession. Contingencies like this would need to be programmed into the smart contract, or there would need to be a mechanism allowing human intervention.[26]

Smart contracts can also be used in the purchase of real property. The process of purchasing a home involves many parties including buyers, sellers, banks, title companies, etc. In theory, the entire transaction, which currently takes days or weeks to complete, could be completed in seconds. A virtual currency transaction can obviate the need to obtain a certified check. Utilizing blockchain-based property records might obviate the need for title insurance and even the need to examine the property's chain of title if the entire chain of title is publicly visible on the blockchain. Under the current system, title searches are conducted to ensure that the seller has the right to sell the property and that the title to the property is clean and unencumbered by liens or other title defects. If the entire chain of title, along with any encumbrances, is recorded on a publicly visible blockchain, there is effectively nothing to miss and therefore nothing to insure: in theory, the blockchain would show the true state of the property without need for further verification. And other blockchain-based processes could eliminate the need for various other steps and actors.[27]

Smart contracts are currently being used in the financial sector for more efficient trading of assets like stocks, bonds, and derivatives. Smart contracts allow for quicker settlement mechanisms and greater access to information affecting prices, as every transaction on a blockchain is immediately and publicly visible. There are also proposals to utilize the technology in issuing and processing syndicated loans (loans that are so large they require the coordination of multiple lenders).[28]

In the entertainment industry, there are proposals to utilize smart contracts to make the royalty process operate more smoothly and make the rights to access purchased content durable should the service through which the consumer purchased the content become unavailable. For example, anytime an artist's song is downloaded on a streaming service, money – likely in the form of virtual currency – can be immediately distributed to the necessary parties. Currently, the process involves a number of intermediaries and is prone to delay.[29]

In the public sector, two applications of blockchain technology drawing interest are property record management and voting. Because blockchains are often used to store information about transactions and changes of ownership, actions like selling a property interest or casting a ballot can be done on a blockchain. In fact, the Franklin County Auditor has launched an effort to utilize blockchain technology to transfer deeds.[30]

There are a number of proposals to utilize blockchain technology in the healthcare industry. For example, a pharmaceutical company – or any company with a complex supply chain – could utilize the technology to make its supply chain more efficient, e.g., by programming a smart contract to automatically order new products once a certain number of products are delivered or sold. There are also proposals to utilize blockchains to make the health insurance claims process quicker, more efficient, and less prone to fraud and error. The technology could even be used to manage patient records more efficiently, in theory allowing patients and providers instant access to the patient's complete medical record. However, it remains unclear how the Health Insurance Portability and Accountability Act of 1996,[31] commonly known as "HIPAA," would apply to records maintained on a distributed ledger.[32]

There are numerous other potential and actual uses of blockchain technology. Unlike in the area of virtual currency, however, federal law is largely silent on blockchain applications not involving virtual currency. States, however, are beginning to wade into these issues.

To learn more

This *Members Only* brief is intended as an introductory overview. The following resources explain blockchain, virtual currencies, and the law relating to them in greater detail.

Further reading

- Arvind Narayanan et al., *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (2016). Course materials including video lectures available at http://bitcoinbook.cs.princeton.edu/.
- Congressional Research Service, *Bitcoin: Questions, Answers, and Analysis of Legal Issues*, October 13, 2015, available at https://fas.org/sgp/crs/misc/R43339.pdf.
- Primavera De Filippi & Aaron Wright, *Blockchain and the Law: The Rule of Code* (2018).
- Shawn S. Amuial, Josias N. Dewey, and Jeffrey R. Seul, *The Blockchain: A Guide for Legal & Business Professionals* (2016).

Further videos

- Anders Brownworth, *Blockchain 101 - A Visual Demo* (2016), available at https://www.youtube.com/watch?v=_160oMzblY8.
- Anders Brownworth, *Blockchain 101 - Part 2 - Public / Private Keys and Signing* (2016), available at https://www.youtube.com/watch?v=xIDL_akeras.

- Bill Maurer and Donald J. Patterson, *Uses of the Blockchain* (2015), available at https://www.youtube.com/watch?v=SPyIy61Lnrw.
- Grant Sanderson, *Ever wonder how Bitcoin (and other cryptocurrencies) actually work?* (2017), available at https://www.youtube.com/watch?v=bBC-nXj3Ng4.

Endnotes

[1] As noted by legal scholar Angela Walch, the terminology used in the blockchain and virtual currency space is "notoriously confusing." Properly speaking, a blockchain is a specific type of distributed ledger, and Bitcoin is an example of a cryptocurrency, which is a specific type of virtual currency that is secured through the use of cryptography. Digital tokens offered through an initial coin offering (see "**Virtual currency as a security**") may also be considered virtual currency or cryptocurrency, although these kinds of token do not necessarily have all the attributes commonly associated with money. See Angela Walch, *The Path of the Blockchain Lexicon (and the Law)*, 36 Review of Banking & Financial Law 713 (2017). See also, Congressional Research Service, *Bitcoin: Questions, Answers, and Analysis of Legal Issues*, October 13, 2015, available at https://fas.org/sgp/crs/misc/R43339.pdf.

[2] *The Columbus Dispatch, "*Ohio to accept bitcoin for tax payments," November 26, 2018, available at https://www.dispatch.com/news/20181126/ohio-to-accept-bitcoin-for-tax-payments.

[3] Bitcoin is the only virtual currency currently being accepted, although the Treasurer's Office plans to allow others in the future. OhioCrypto.com: Cryptocurrency Tax Payment Portal, FAQ page, available at https://ohiocrypto.com/faq.

[4] R.C. 1306.01.

[5] Shawn S. Amuial, Josias N. Dewey, and Jeffrey R. Seul, *The Blockchain: A Guide for Legal & Business Professionals* § 1:2 (2016).

[6] Shawn S. Amuial, Josias N. Dewey, and Jeffrey R. Seul, *The Blockchain: A Guide for Legal & Business Professionals* (2016); Congressional Research Service, *Bitcoin: Questions, Answers, and Analysis of Legal Issues*, October 13, 2015, available at https://fas.org/sgp/crs/misc/R43339.pdf; Anders Brownworth, *Blockchain 101 - A Visual Demo* (2016), available at https://www.youtube.com/watch?v=_160oMzblY8; Anders Brownworth, *Blockchain 101 - Part 2 – Public / Private Keys and Signing* (2016), available at https://www.youtube.com/watch?v=xIDL_akeras; Grant Sanderson, *Ever wonder how Bitcoin (and other cryptocurrencies) actually work?* (2017), available at https://www.youtube.com/watch?v=bBC-nXj3Ng4.

[7] Primavera De Filippi & Aaron Wright, *Blockchain and the Law: The Rule of Code* 33-45 (2018). While these features, especially the privacy feature, are appealing to many users, they also create opportunities for criminals. Everything from money laundering to sex trafficking is more difficult to control when the parties use virtual currency. While cash is equally difficult to track, using virtual currency rather than cash makes transactions less risky for criminals because the transaction can be completed remotely rather than in person.

[8] Congressional Research Service, *Bitcoin: Questions, Answers, and Analysis of Legal Issues*, October 13, 2015, available at https://fas.org/sgp/crs/misc/R43339.pdf; Primavera De Filippi & Aaron Wright, *Blockchain and the Law: The Rule of Code* 61-66 (2018); and Angela Walch, *The Path of the Blockchain Lexicon (and the Law)*, 36 Rev.Bank&Fin.L. 713 (2017).

[9] Jon Swartz and Avi Salzman, *Bitcoin Is the Hottest Thing Around. So Why Is It So Hard to Use?*, Barron's, December 15, 2017, available at https://www.barrons.com/articles/bitcoin-is-the-hottest-thing-around-so-why-is-it-so-hard-to-use-1513347597?mod=article_inline.

[10] *SEC v. Shavers*, 2013 U.S. Dist. LEXIS 110018.

[11] Primavera De Filippi & Aaron Wright, *Blockchain and the Law: The Rule of Code*, pp. 98-104 (2018).

[12] U.S. Securities and Exchange Commission, *Public Statement: Statement on Potentially Unlawful Online Platforms for Trading Digital Assets*, March 7, 2018, available at https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading.

[13] To determine whether a scheme qualifies as an offering of securities, courts utilize the three-part *Howey* test, under which a scheme is an offering of securities if it (1) "involves and investment of money," (2) "in a common enterprise," (3) "with profits to come solely from the efforts of others." *SEC v. W. J. Howey Co.*, 328 U.S. 293, 301.

[14] 49 Stat. 1491, 7 U.S.C. 1.

[15] *In the Matter of Coinflip, Inc. and Francisco Riordan*, CFTC Docket No. 15-29, fn. 2 and pg. 3.

[16] Internal Revenue Service, Notice 2014-21.

[17] Internal Revenue Service, Notice 2014-21.

[18] *Bank Secrecy Act of 1970*, 84 Stat. 1114, 31 U.S.C. 5311 to 5332.

[19] 31 C.F.R. 1010.100(ff)(5); Financial Crimes Enforcement Network (FinCEN), *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001, issued March 18, 2013. Under this and other guidance, the key factor in determining whether a party is acting as a money transmitter is how closely related the transfer of funds is to another purchase or sale.

[20] Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001, issued March 18, 2013.

[21] Federal Election Commission, Advisory Opinion 2014-02, May 8, 2014, http://saos.fec.gov/aodocs/2014-02.pdf.

[22] 12 Stat. 592, 18 U.S.C. 336.

[23] Congressional Research Service, *Bitcoin: Questions, Answers, and Analysis of Legal Issues*, October 13, 2015, available at https://fas.org/sgp/crs/misc/R43339.pdf.

[24] Shawn S. Amuial, Josias N. Dewey, and Jeffrey R. Seul, *The Blockchain: A Guide for Legal & Business Professionals* §§ 2:2-2:3 (2016).

[25] Blockgeeks, *Smart Contracts: The Blockchain Technology That Will Replace Lawyers*, available at https://blockgeeks.com/guides/smart-contracts/.

[26] Blockgeeks, *Smart Contracts: The Blockchain Technology That Will Replace Lawyers*, available at https://blockgeeks.com/guides/smart-contracts/.

[27] Avi Spielman, *Blockchain: Digitally Rebuilding the Real Estate Industry*, Master's thesis, Massachusetts Institute of Technology, 2016, available at https://dspace.mit.edu/bitstream/handle/1721.1/106753/969450770-MIT.pdf?sequence=1.

[28] Primavera De Filippi & Aaron Wright, *Blockchain and the Law: The Rule of Code* 90-92 (2018).

[29] Sherman Lee, *Embracing Blockchain Could Completely Change The Way Artists Sell Music And Interact With Fans*, Forbes, April 25, 2018, available at https://www.forbes.com/sites/shermanlee/2018/04/25/embracing-blockchain-could-completely-change-the-way-artists-sell-music-and-interact-with-fans/#6fc1ab0e1a25; James Rinaldi, *Peer to Peer Digital Rights Management using Blockchain*, Master's thesis, University of the Pacific, 2018, available at https://scholarlycommons.pacific.edu/cgi/viewcontent.cgi?article=4135&context=uop_etds.

[30] *The Columbus Dispatch,* "Auditor's use of blockchain technology touted as more than way to transfer records," August 23, 2018, available at http://www.dispatch.com/news/20180823/auditors-use-of-blockchain-technology-touted-as-more-than-way-to-transfer-records.

[31] 110 Stat. 1936.

[32] Shawn S. Amuial, Josias N. Dewey, and Jeffrey R. Seul, *The Blockchain: A Guide for Legal & Business Professionals* §§ 2:12 and 2:14 (2016).

Published by the Ohio Legislative Service Commission Staff

9th Floor
Vern Riffe Center
Columbus, Ohio
(614) 466-3615

Director, Office of Research and Drafting
Jim Kelly

Author
Yosef Schiff
Attorney

Reviewer
Michael J. O'Neill
Division Chief

Layout & Design
Linda Bayer

Addendum: Anatomy of a Bitcoin Transaction

This Addendum describes in detail how blockchain technology works in the context of a Bitcoin transaction. Note that while other virtual currencies and blockchain applications, like property record management, operate differently, these various technologies share the basic property of linking "blocks" of information together through the process of "hashing" as explained below. Also note that the information presented here is a simplification of the Bitcoin protocol; some details are left out and others are imprecisely stated. The point of this Addendum is to communicate the basic idea of how one type of blockchain works.[i]

Step 1: Record and sign a transaction

Say that Alice wants to send 10 bitcoins to Bob. This is done by recording the individuals' account numbers, the amount to be transferred, and other relevant information. To ensure that it really is Alice sending the money and not an imposter, Alice applies a digital signature to the transaction. Then all of this information (the account numbers, amount, digital signature, etc.) is added to a block containing other pending transactions. Once that block contains enough transactions, it can be validated and added to the blockchain.[ii]

Step 2: Validation

Hashing

To understand the validation process, it is first vital to understand what a hashing algorithm is. Although the details can get complicated, the concept is actually quite simple. Hashing is the process of applying certain operations to a piece of code, changing it so it appears like a long, random string of characters. The most prominent hashing algorithm is SHA-256 (Secure Hash Algorithm 256), and there are three important things to understand about it. The first is that no matter how large or small the input, the output is always the same length: 256 bits, or 64 characters. Second, even if you know how the algorithm works at a detailed level, you cannot reverse it; you cannot take an output (the random-looking string of characters) and figure out what the input was.[iii] And third, SHA-256 is extremely sensitive in that even the tiniest change to the input, such as replacing a single letter, produces an entirely different output. Thus, a hash can be thought of as a fingerprint of the thing being hashed; it is a way to verify that a piece of information has not been changed, since even the smallest change results in an entirely different hash. You may not know what has changed, but you will know a change has occurred.

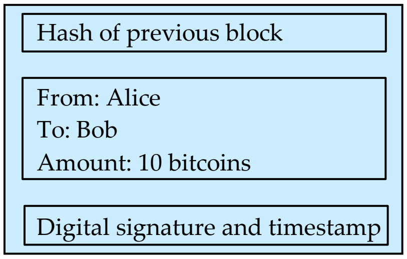
Creating a hash is very easy. In fact, SHA-256 generators are freely available on the Internet. All you do is enter text of any length and it quickly displays a hash of that text. For example, the hash of the word "hello" is 2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa 7425e73043362938b9824. And the hash of Herman Melville's *Moby Dick* (the entire book copied and pasted into a SHA-256 generator) is 5c36160a5d1a666d5c509ac445ae171b1ba 23e6f6c50d7a93831ee384faab530. But you cannot reverse the process; if you were given these very hashes but did not know that they were produced from the word "hello" and the book *Moby Dick,* there would be no way to figure out that the inputs were "hello" and *Moby Dick*.

And if you were to delete a single word from *Moby Dick,* the hash would be completely different. As will become clear below, this irreversibility and sensitivity help secure the transaction.

Race to find the nonce

So what does hashing have to do with validation? To validate a block, so-called "miners" start searching for something called a "nonce" or "number used only once." This is a number that, when added to all the other information in a block, results in the block having a very specific hash, i.e., one that begins with 20 zeros.[iv] Finding a nonce involves guessing and checking quadrillions of times. This process is illustrated in the figures below. A miner is someone who uses a computer[v] to find nonces in hopes of obtaining a mining reward.[vi] When a miner finds the nonce, the miner broadcasts that number to the network so others can verify that it is correct. Again, this process is illustrated below.

For the sake of simplicity, let us assume the block only contains a single transaction, the one between Alice and Bob. At this point, the block looks like this:



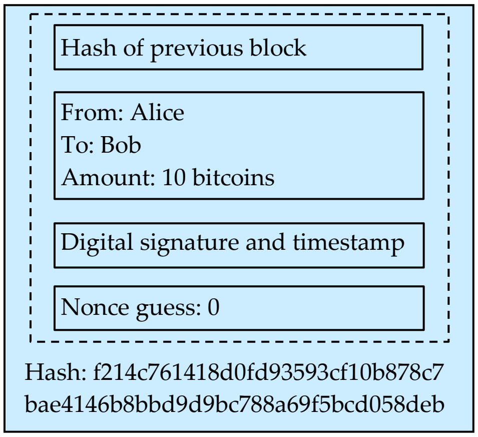
Hash of previous block

From: Alice
To: Bob
Amount: 10 bitcoins

Digital signature and timestamp

As you can see, the block contains the transaction and a few other pieces of information, including a digital signature and timestamp, which ensure a transaction is not fraudulent and help order transactions chronologically. Importantly, the block also contains the hash of the previous block.[vii] As we will see below, this is how blocks get "chained" together.

This is where the validation process begins. Miners start adding numbers to the block hoping to find the nonce. Again, this is the number that makes the hash begin with 20 zeros. Miners begin with 0, then 1, then 2, and so on. The process looks something like this:



Hash of previous block

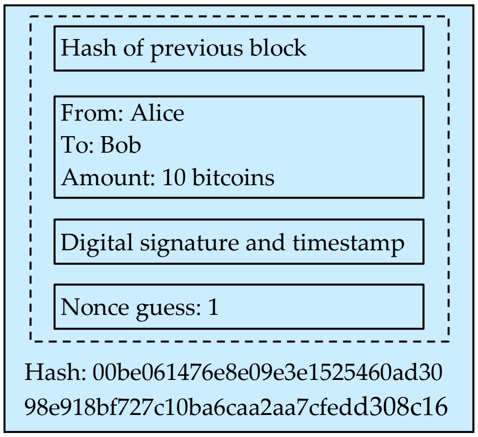
From: Alice
To: Bob
Amount: 10 bitcoins

Digital signature and timestamp

Nonce guess: 0

Hash: f214c761418d0fd93593cf10b878c7
bae4146b8bbd9d9bc788a69f5bcd058deb

We know the nonce is not 0 since the hash does not begin with 20 zeros. What about 1?


Hash of previous block

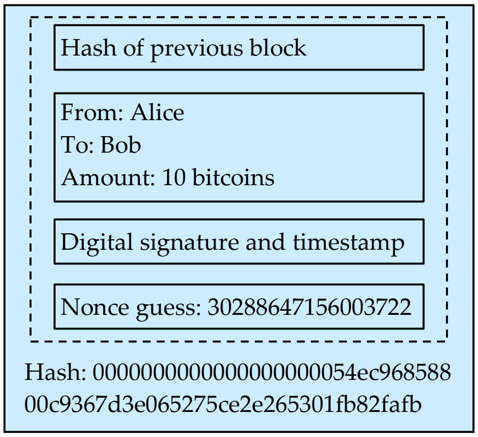
From: Alice
To: Bob
Amount: 10 bitcoins

Digital signature and timestamp

Nonce guess: 1

Hash: 00be061476e8e09e3e1525460ad30
98e918bf727c10ba6caa2aa7cfedd308c16

The nonce is also not 1. Let us assume that all the miners on the network made quadrillions of attempts before finding the nonce, which we will say is 30,288,647,156,003,722. This means our block and hash now look like this:


Hash of previous block

From: Alice
To: Bob
Amount: 10 bitcoins

Digital signature and timestamp

Nonce guess: 30288647156003722

Hash: 0000000000000000000054ec968588
00c9367d3e065275ce2e265301fb82fafb

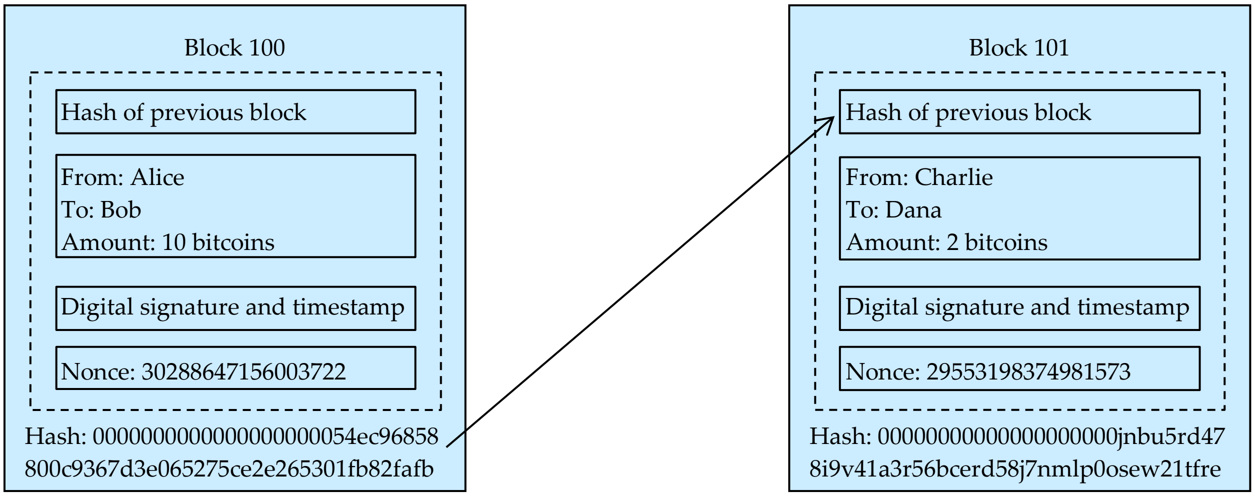
The first miner to find this nonce broadcasts it to the network so others can check it. All the other miners need to do is enter “30288647156003722” in the nonce field and hash the block to make sure it really does produce the hash 00000000000000000000 54ec96858800c9367d3e065275ce2e265301fb82fafb.

It takes *a lot* of guessing and checking to find a nonce. As of February 2019, it takes approximately 25 quadrillion guesses on average to find a nonce, or about ten minutes with all miners on the Bitcoin network searching.[viii] Although this process might seem very strange at first, the difficulty in finding the nonce is central to the operation of Bitcoin; it forms the heart of Bitcoin’s so-called “proof-of-work” consensus mechanism. The nature of that mechanism and the role of the previous block’s hash should become clear in “**Step 3: Chain the blocks together**” below.

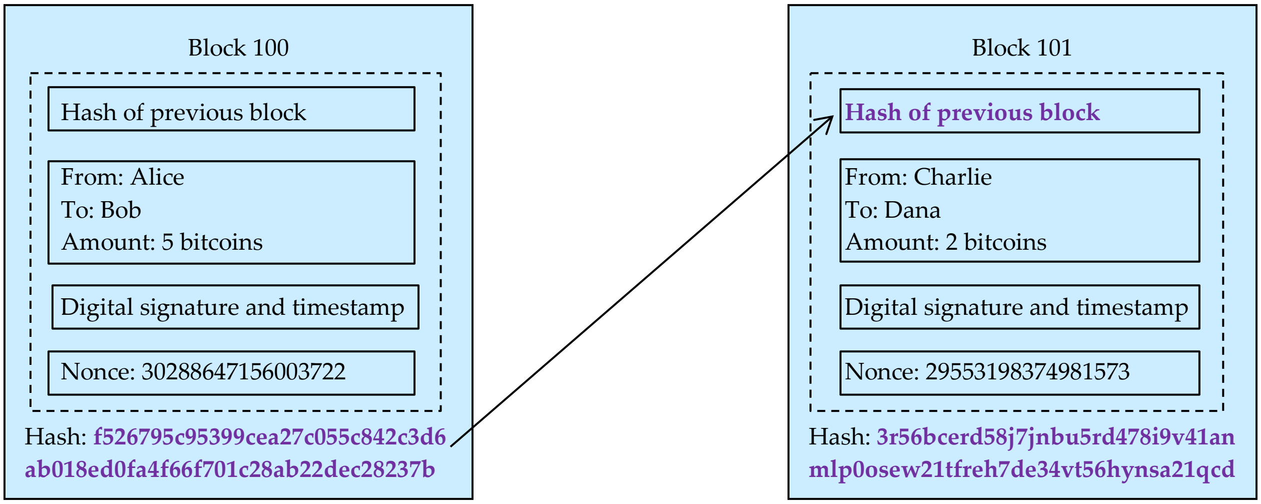
Step 3: Chain the blocks together

Once a block is validated, the existing blockchain is updated to include the new block, and the process starts all over again for the next block. Critically, though, the hash that was produced above (0000000000000000000054ec96858800c9367d3e065275ce2e265301fb82fafb) is inserted into the incoming block before the incoming block is validated with its own hash. In this way, the hash of the next block is partially based on the hash of the block that was just validated.

This means that any change to a previous block "breaks" the chain by changing the hash; if someone wishes to go back in time and fraudulently alter or undo a transaction, the hash of the block in which that transaction sits would no longer have the required number of leading zeros. Instead, it would look random. And because the hashes of all subsequent blocks are linked to the hash of that block, their hashes would change as well and each one would need to have a new nonce in order to begin with 20 zeros. Prior to such an attempted alteration, the blockchain might look like this (note that the blocks are numbered 100 and 101 to illustrate the idea that the block containing Alice and Bob's transaction is just one of many on the blockchain):


Block 100
Hash of previous block
From: Alice
To: Bob
Amount: 10 bitcoins
Digital signature and timestamp
Nonce: 30288647156003722
Hash: 0000000000000000000054ec96858
800c9367d3e065275ce2e265301fb82fafb
Block 101
Hash of previous block
From: Charlie
To: Dana
Amount: 2 bitcoins
Digital signature and timestamp
Nonce: 29553198374981573
Hash: 00000000000000000000jnbu5rd47
8i9v41a3r56bcerd58j7nmlp0osew21tfre

If Alice attempted to alter her transaction to Bob to make it look like she only sent him 5 bitcoins, you would have something like the following:


Block 100
Hash of previous block
From: Alice
To: Bob
Amount: 5 bitcoins
Digital signature and timestamp
Nonce: 30288647156003722
Hash: f526795c95399cea27c055c842c3d6 ab018ed0fa4f66f701c28ab22dec28237b
Block 101
Hash of previous block
From: Charlie
To: Dana
Amount: 2 bitcoins
Digital signature and timestamp
Nonce: 29553198374981573
Hash: 3r56bcerd58j7jnbu5rd478i9v41an mlp0osew21tfreh7de34vt56hynsa21qcd

The hash is different now because the input is different: instead of 10 bitcoins in the amount field, it now says 5 bitcoins. Remember, even the smallest change to an input results in an entirely different hash. In order to make the new hashes work, Alice would need to find new nonces. Using 30288647156003722 would no longer work for Block 100, 29553198374981573 would no longer work for Block 101, and so on, because the input that produced the hash in Block 100 is now different, and therefore produces a different hash in that block and all subsequent blocks. In order to successfully go back and alter her transaction, Alice would need to find new nonces for that block and every single subsequent block and broadcast these to the network herself. And she would need to do this quickly enough to outpace all the incoming transactions and block validations. This is a practically impossible feat of computation; remember, it takes quadrillions of guesses to find just one nonce, an enormous number of guesses and beyond the computational resources of any single actor. It is simply not feasible to successfully alter previous transactions in this manner.[ix]

Where do bitcoins come from?

All of this raises a question: although Alice cannot go back and alter a previous transaction, how do we know that the transaction was valid in the first place? In other words, how do we know that Alice really had those 10 bitcoins to begin with and is not just doing a complicated version of bouncing a check, thus spending money she does not really have? In short, because of how the software works and because all transactions are publicly visible on the blockchain, there is no way for Alice to do this. If she did not have 10 bitcoins, there would be no way for her to initiate a transaction for that amount in the first place; the software only lets you spend what you have and it knows what you have because all transactions to and from everyone are visible on the blockchain.

But this raises yet another question: where do the bitcoins come from in the first place? The answer is that bitcoins are created by the software as a mining reward. So bitcoins come into existence when a block is validated and those bitcoins can then be spent and tracked forever on the blockchain.

Other uses of a blockchain

Blockchains are useful for more than just monetary transactions. They can be used for everything from property record management to smart contracts. In fact, the Bitcoin blockchain itself can be used in some of these nonmonetary cases. In essence, rather than Alice sending Bob 10 bitcoins, Alice could transfer a piece of property to Bob. The only real difference is that instead of "Alice sends Bob 10 bitcoins," the message would read something more like "Alice transfers ownership of Property X to Bob." This nonmonetary transaction would be added to a block and validated on the blockchain just like any other transaction and the miner who finds the nonce for that block would receive the same reward as in the case of any other transaction.

Blockchain Addendum.docx/lb

[i] This Addendum is an aggregation of information from the following sources:

- Anders Brownworth, *Blockchain 101 - A Visual Demo* (2016), available at https://www.youtube.com/watch?v=_160oMzblY8.
- Anders Brownworth, *Blockchain 101 - Part 2 - Public / Private Keys and Signing* (2016), available at https://www.youtube.com/watch?v=xIDL_akeras.
- Arvind Narayanan et al., *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (2016). Course materials including video lectures available at http://bitcoinbook.cs.princeton.edu/.
- Congressional Research Service, *Bitcoin: Questions, Answers, and Analysis of Legal Issues,* October 13, 2015, available at https://fas.org/sgp/crs/misc/R43339.pdf.
- Grant Sanderson, *Ever wonder how Bitcoin (and other cryptocurrencies) actually work?* (2017), available at https://www.youtube.com/watch?v=bBC-nXj3Ng4.
- Primavera De Filippi & Aaron Wright, *Blockchain and the Law: The Rule of Code* (2018).
- Shawn S. Amuial, Josias N. Dewey, and Jeffrey R. Seul, *The Blockchain: A Guide for Legal & Business Professionals* (2016).
- Bill Maurer and Donald J. Patterson, *Uses of the Blockchain* (2015), available at https://www.youtube.com/watch?v=SPyIy61Lnrw.

[ii] For various reasons, the creator of Bitcoin set a one megabyte limit on block size. Bitcoin Magazine, *Why the Bitcoin Block Size Debate Matters,* July 7, 2016, available at https://www.nasdaq.com/article/why-the-bitcoin-block-size-debate-matters-cm645644. As of February 2019, each block contains an average of approximately 2,000 transactions, although this number varies. See, e.g., Blockchain (company), *Average Number Of Transactions Per Block Chart*, available at https://www.blockchain.com/en/charts/n-transactions-per-block; Patrick Thompson, *The Current State of the Bitcoin Network and Its Biggest Block,* Cointelegraph, September 26, 2018, available at https://cointelegraph.com/news/the-current-state-of-the-bitcoin-network-and-its-biggest-block.

[iii] SHA-256 cannot be run in reverse because it removes information from the input as it produces an output. However, the details of how the algorithm works are not important for the purposes of this memorandum.

[iv] The number of required leading zeros fluctuates depending on a number of factors, but tends to increase over time. The goal is to have one block validated every 10 minutes, meaning that more miners results in more leading zeros. Primavera De Filippi & Aaron Wright, *Blockchain and the Law: The Rule of Code* 23-24 (2018).

[v] Although home computer users were able to mine bitcoins in the virtual currency's early days, only groups of people with massive computing power can profitably do so now (Primavera De Filippi & Aaron Wright, *Blockchain and the Law: The Rule of Code* 40 (2018)).

[vi] As of 2018, the reward for successfully finding a nonce was 12.5 bitcoins, equivalent to approximately $45,000 as of February 2019. Billy Bambrough, *A Bitcoin Halvening Is Two Years Away – Here's What'll Happen To The Bitcoin Price,* Forbes, May 29, 2018, available at https://www.forbes.com/sites/billybambrough/2018/05/29/a-bitcoin-halvening-is-two-years-away-heres-whatll-happen-to-the-bitcoin-price/#14dc90e85286; Google Finance, BTC to USD Chart, available at https://www.google.com/search?q=BTC+to+USD.

[vii] By definition, the first block on the Bitcoin blockchain has no previous block. It is therefore structured differently than all subsequent blocks. Ittay Eyal, et al., *Bitcoin-NG: A Scalable Blockchain Protocol* 47, available at https://www.usenix.org/system/files/conference/nsdi16/nsdi16-paper-eyal.pdf.

[viii] Blockchain (company), *Hash Rate*, available at https://www.blockchain.com/en/charts/hash-rate; Primavera De Filippi & Aaron Wright, *Blockchain and the Law: The Rule of Code* 56 (2018). This number was calculated by taking the hash rate rounded to 50 terahashes per second and multiplying that by 600 seconds (600 seconds = 10 minutes). The result is 30 quadrillion hashes every 10 minutes.

[ix] This does not mean the Bitcoin network is completely immune from any kind of attack. If an actor were to gain more than half the computing power of the entire Bitcoin network, a truly enormous amount, that attacker could launch a so-called "51 percent attack," wreaking havoc on the network. However, such an attack is unlikely on a network as large as Bitcoin. Moreover, the value of a bitcoin would likely fall as an actor came close to acquiring that much computing power, thus disincentivizing the attack. Arvind Narayanan et al., *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* 48-49 (2016).