Blockchain 101 for Lay People

WRITTEN BY:

Celiza (Lisa) Bragança

PRESENTERS:

Celiza Bragança: @LisaBraganca

Ian Hu: @Ian_Hu_

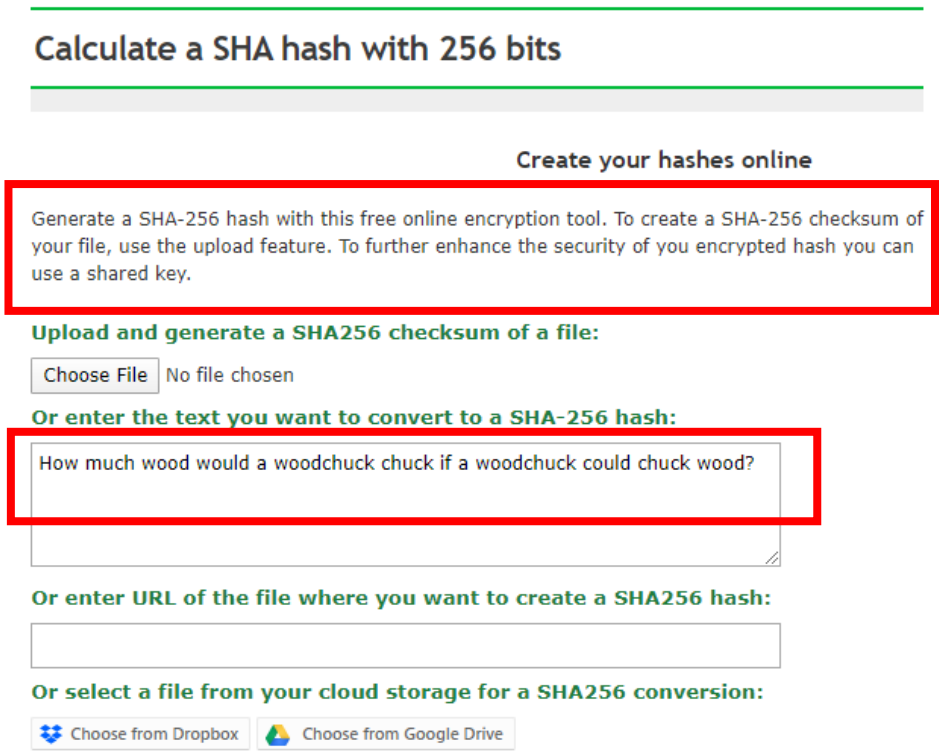
January 6, 2020

WHAT IS BLOCKCHAIN?

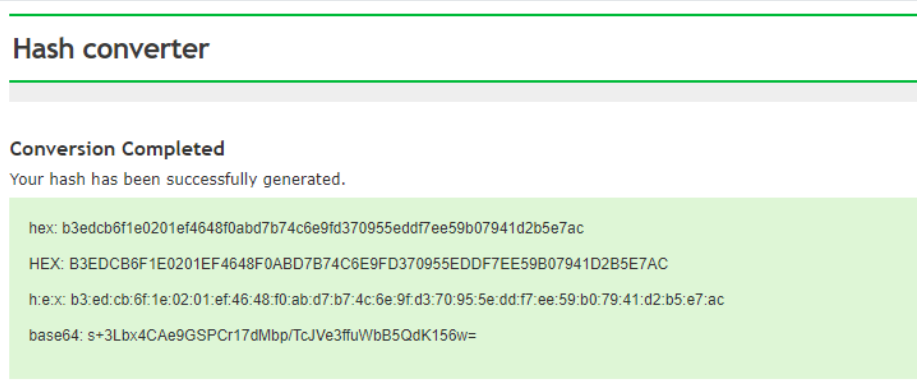
A blockchain is a special type of database that is shared across a network of computers. There are several factors that distinguish blockchain technology from the typical technology used in maintaining databases.

The first factor is a distributed network where each computer contains a complete copy of all records. There is no single centralized database. Nor is there a centralized entity that ensures the accuracy of all the data. Transactions are grouped into blocks and recorded by each computer in the network. This kind of decentralized network is only possible because of **cryptography**.

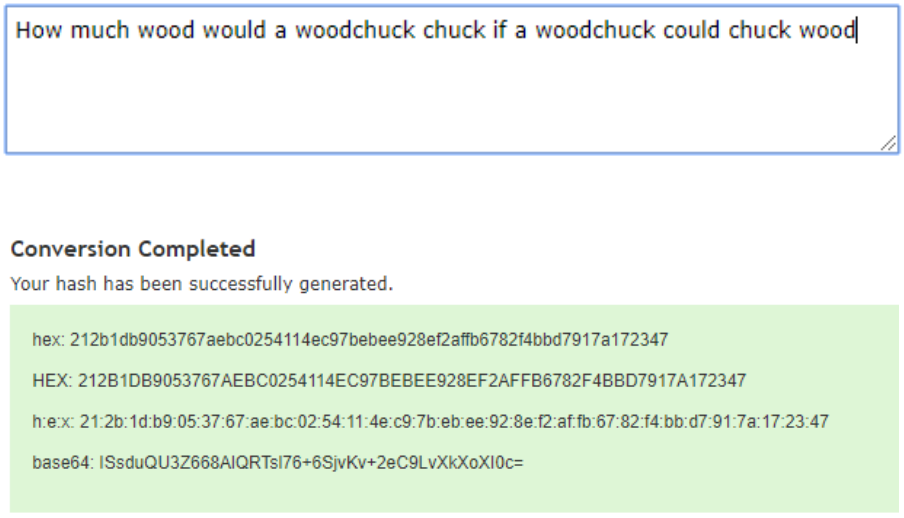
The second factor is the use of **cryptography** to ensure that transactions are recorded accurately and are unchanged. Blockchains use hashing functions (cryptography) to create a unique identifier – a hash code -- for every block of transactions. A hash code is generated by a mathematical function. You put in digital information and it generates a hash – a string of letters and numbers. Here is one website that will do this for you: https://hash.online-convert.com/sha256-generator



Put in the statement "how much wood would a woodchuck chuck if a woodchuck could chuck wood?" and it will generate the following hash:



But, if any part of the digital information (input) is changed, the hash will change. What if we take out the question mark at the end of the statement?



The mere removal of a question mark results in a completely different hash. Here is a graphical depiction of these concepts created by Reuters that you might find helpful: http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html.

The hash codes are used by the decentralized computers storing the blockchain to ensure that the information they have is accurate and unchanged. The hashes are embedded in the blocks making it ridiculously hard to go back and alter information in recorded blocks.

You may have heard about bitcoin mining. Mining is the name given to computers racing to solve complex mathematical problems in order to earn the right to record a block on the blockchain and earn bitcoin.

The winning miner records the block that is then recorded by all other computers in the network. This happens about once every ten minutes on the bitcoin blockchain. Miners also receive transaction fees from those who have transactions on the bitcoin blockchain. A really nice short description by SciShow is called *Bitcoin: How Cryptocurrencies Work*, available on YouTube at https://youtu.be/kubGCSj5y3k

There are lots of user-friendly resources to explain in detail what blockchains are and how they work. For example, Khan Academy has a course on blockchains, available at https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-what-is-it. A nice video on blockchain is *Blockchain Expert Explains Oner Concept in 5 Levels of Difficulty* (published by Wired Magazine), available at https://youtu.be/kubGCSj5y3k.

Do not be discouraged if you do not understand blockchain the first, second, or tenth time you watch a video or read about it. It can take a long time to understand these concepts. Moreover, you do not have to understand everything about blockchain to be technically competent.

WHAT IS A CRYPTOCURRENCY?

Cryptocurrency (or virtual currency) is a specific type of digital coin that is used as currency. Bitcoin is just one type of cryptocurrency. Use as currency means that a digital coin "functions as a medium of exchange, a unit of account, and/or a store of value." CFTC Primer on Cryptocurrencies, available at https://www.cftc.gov/sites/default/files/idc/groups/public/documents/file/labcftc_primercurrencies100417.pdf. A comprehensive definition of cryptocurrency by The Financial Action Task Force is:

> a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued or guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency. Virtual currency is distinguished from fiat currency (a.k.a. "real currency," "real money," or "national currency"), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and

> accepted as a medium of exchange in the issuing country. It is distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency.

Fin. Action Task Force, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks* 4 (2014), https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

What does this mean? It means you can use a digital coin – cryptocurrency – to purchase something, to value something, and/or a way to save for later consumption.

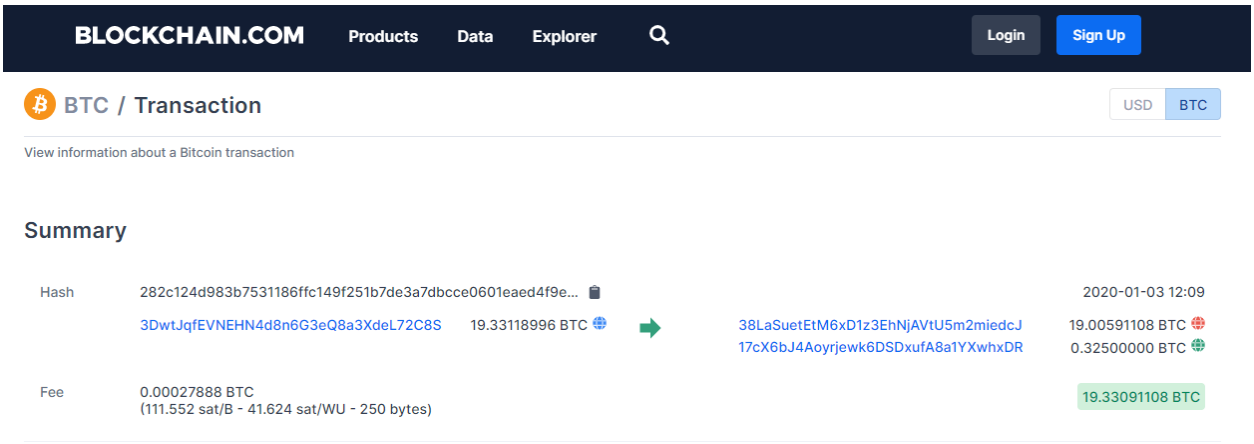
WHAT IS BITCOIN?

Bitcoin is the most popular of the cryptocurrencies in use today. The creation of bitcoin and the blockchain came on the heels of the Great Recession, when many people lost faith in the banking system and banking regulators. The first digital coin, bitcoin, was created in 2009 by Satoshi Nakamoto. Nobody knows who Nakamoto is or whether he is one person or a group.

Nakamoto published a nine-page white paper called *Bitcoin: A Peer-to-Peer Electronic Cash System*. In the paper Nakamoto proposed an alternative to the existing financial system, which had recently failed so spectacularly. He proposed a system that would cut out governments, banks and other financial institutions, a system that would allow "two willing parties to transact directly with each other without the need for a trusted third party." The goal was a peer-to-peer financial system that offered privacy, was independent of governments and eliminated the transactional expenses imposed by, and the interference of, banks and other financial intermediaries.

What does bitcoin look like?

Now that you have some idea of what bitcoin is, let's look at a bitcoin transaction. Because bitcoin are bits of computer code, you need a computer program to show them to you. One such program is called the Blockchain Explorer, available at https://www.blockchain.com/explorer. This program reads bitcoin transactions that exist on the blockchain and translates them into a readable format like the following:



This is the most important of the information available about a transaction available on the Blockchain Explorer. There is much more, including the identification of the "block" on which this transaction is recorded.

This is not the friendliest format, but this is what a bitcoin transaction looks like. The "hash" is the transaction identifier. The long blue number below the hash starting with "3Dw" is the address of the wallet from which bitcoin was transferred (the "From" wallet). The two long blue numbers to the right of the green arrow starting with "38L" and "17c" are the addresses of the wallets into which the bitcoin was transferred (the "To" wallets). At the bottom left, the fee for processing the transaction is reported.

WHO SHOULD CARE ABOUT BLOCKCHAIN AND DIGITAL COINS?

All lawyers should have some familiarity with the legal and regulatory issues concerning blockchain and digital coins. More individuals and businesses are choosing to acquire and hold digital assets that exist on blockchains. This means lawyers must be familiar with, and inquire about, digital coins in many types of matters such as litigation, tax, divorce, estate planning, probate, bankruptcy and business transactions, to name just a few. For example, if you are representing one party in a divorce, you should be seeking information about bitcoin or other digital assets that your client and the other party may possess. It would be a mistake to assume that only criminals use digital assets.

Moreover, as clients experience problems with bitcoin and other digital assets, their first call is likely to be to their lawyer – you. It is important that you are able to give them the kind of "first aid" advice that will preserve whatever chance they may have of recovering their losses. A fundamental legal skill is

identifying potential legal problems whether an attorney has the skill and knowledge to address those issues or not:

> Perhaps the most fundamental legal skill consists of determining what kind of legal problems a situation may involve, a skill that necessarily transcends any particular specialized knowledge. A lawyer can provide adequate representation in a wholly novel field through necessary study. Competent representation can also be provided through the association of a lawyer of established competence in the field in question.

ABA Model Rule 1.1, Competence – Comments (Legal Knowledge and Skill), at Comment 2, available at https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1/.

REGULATION OF DIGITAL ASSETS

Digital assets as currency

Digital assets like bitcoin are regulated by banking regulators and state money transmission regulation. Banking regulators require businesses selling virtual currencies like bitcoin to comply with anti–money laundering and "know your customer" regulations. At the federal level the Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Treasury Department, oversees registration and regulation of money transmitting businesses. FinCEN issued guidance in March 2013 on the regulatory responsibilities of money transmitter businesses in a document entitled Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, which can be found online. There are also numerous state regulations of money transmitters.

Digital assets as commodities

Bitcoin is also considered a commodity by the Commodities Futures Trading Commission (CFTC). While the CFTC does not directly regulate the sale of commodities—such as gold, silver and pork bellies—it does regulate derivatives that are based upon the value of commodities, such as swaps, futures contracts and options contracts.

The CFTC has allowed two of the exchanges it oversees to begin trading bitcoin futures. The Chicago Mercantile Exchange and the Chicago Board Options Exchange used a self-certification process to

approve and begin trading these contracts, so the CFTC did not have to expressly approve the trading of bitcoin futures contracts.

Digital assets as securities

Federal and state securities laws apply to those digital coins that are securities. The determination of whether a digital coin is a security is not always clear-cut. There is no simple formula. The SEC looks at the economic reality of a particular transaction: if it walks like a duck and quacks like a duck, it is a duck.

The Howey test is the long-established test used by the SEC to determine whether an offering is subject to federal securities laws. The Howey test applies to digital coins as well as other offerings. In the *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO* (the DAO Report), available at https://www.sec.gov/litigation/investreport/34-81207.pdf, the SEC issued an authoritative statement of how it applied the Howey test to conclude that digital coins issued by the DAO, an unincorporated organization, were securities:

> An investment contract is an investment of money in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others . . . . In analyzing whether something is a security, form should be disregarded for substance, and the emphasis should be on economic realities underlying a transaction, and not on the name appended thereto (citations omitted).

Because the DAO digital coins, called tokens, offered investors the prospect of earning profits that would be generated through the managerial and entrepreneurial efforts of the issuers and others, the SEC considered the coins securities.

More recently, the SEC expanded on the DAO Report in specific guidance to those considering "initial coin offerings" or ICOs. *Framework for "Investment Contract" Analysis of Digital Assets*, available at https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets. The SEC also created a "Strategic Hub for Innovation and Financial Technology" which it calls "FinHub." https://www.sec.gov/finhub. FinHub is intended to, among other things, collect and publish in a central location the SEC's activities and initiatives involving blockchain and other "FinTech." This includes providing continuing guidance concerning the application of federal securities laws to FinTech activities.

In 2019, the SEC issued several no-action letters that provided further guidance on the application of federal securities laws to digital assets. In one no-action letter, the SEC Division of Corporation Finance stated that it did not consider the digital tokens that a corporate charter service proposed having customers use to purchase air charter services to be securities. *In re Turnkey Jet, Inc.*, April 3, 2019, available at https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm. In another no-action letter, the SEC Division of Corporation Finance similarly stated that it did not consider digital tokens that a gaming company proposed to allow gamers who purchase or earn in-game currency in one game to transfer it to other participating games. *In re Pocketful of Quarters, Inc.*, July 25, 2019, available at https://www.sec.gov/corpfin/pocketful-quarters-inc-072519-2a1. In both cases, the SEC Division of Corporate Finance noted the issuers would not use the proceeds of the sale of the digital tokens to develop the operational platform and the tokens would only be used for consumption purposes.

TAXATION OF DIGITAL ASSETS

Another important consideration is how the IRS and other taxing authorities treat digital assets like bitcoin. The IRS treats cryptocurrencies like bitcoin as property, not like a foreign currency. IRS Notice 2014-21, available at https://www.irs.gov/pub/irs-drop/n-14-21.pdf. The IRS requires that any cryptocurrency that a taxpayer receives as payment for goods or services be reported at its fair market value on the date of receipt. The type of gain or loss recognized on the cryptocurrency is subject to IRS rules. Taxpayers may be required to issue a Form 1099-MISC for payments made in cryptocurrency and may be required to withhold taxes. Additional information on taxation of digital assets is available here: https://www.irs.gov/pub/irs-utl/2018ntf-bitcoin-cryptocurrency-an-introduction-and-tax-consequences.pdf

BEFORE YOU DECIDE TO ACCEPT PAYMENT IN CRYPTOCURRENCY

Cryptocurrencies like bitcoin and ether are gaining wide acceptance as currency. But there are a number of things to consider before you start accepting cryptocurrency as payment for legal services. For example, what is your state's attorney regulatory agency position on how you going to process the payments. Is your accountant prepared to handle cryptocurrency transactions? What steps will you take to ensure you are safely handling cryptocurrency?

The only state attorney regulatory agency to expressly authorize attorneys to accept bitcoin as payment is Nebraska's. If a Nebraska attorney receives bitcoin in payment, they are required to convert the bitcoin immediately to U.S. currency. If you do not live in Nebraska, then you could request an opinion from your state's agency.

You should make sure that your accounting software and your accountant are able to handle cryptocurrency transactions. This is a relatively new area and not every accountant is excited about having to deal with cryptocurrency transactions. Make sure that your accounting software is capable of reporting the information that you accountant will need to file your tax returns. It is better to work this all out ahead of time than to be scrambling at tax time.

Finally, be aware of all the ways that cryptocurrency can be stolen. Even Apple co-founder Steve Wozniak has had bitcoin stolen. Common ways that cryptocurrencies may be stolen are through phishing schemes, fake exchanges and clipboard hijacking. Fake exchanges have websites and addresses that masquerade as legitimate digital coin exchanges. Clipboard hijacking is accomplished by computer viruses that remain dormant until they detect a digital coin address copied onto a clipboard, which is the way most people enter online wallet addresses for digital coin transactions. The virus changes the receiving online wallet address to steal the digital coins. If you decide to accept bitcoin or other cryptocurrency as payment, you should take precautions and stay abreast of the latest scams.