A FINANCIAL ADVISOR'S GUIDE TO BLOCKCHAIN, BITCOIN, AND CRYPTOCURRENCIES

Cetera®
FINANCIAL GROUP

Bitcoin and its overnight success have all the trappings of a fad.

Its value skyrocketed, seemingly out of nowhere, and it dominated headlines as prices soared. People scrambled for Bitcoin and all things cryptocurrency in late 2017, despite calls for caution, and in early 2018, the bubble burst.

Prices crashed, and people as prominent as World Bank Group President Jim Yong Kim unabashedly called cryptocurrencies "Ponzi schemes."[1] Almost as fast as the frenzy hit, sentiment began to turn against cryptocurrency. To the casual observer, the Bitcoin mania may appear to have been a flash-in-the-pan fad that can be ignored—but that could prove to be a mistake.

Excitement over Bitcoin and other cryptocurrencies has as much, if not more, to do with the blockchain technology underpinning it as it does to do with a new kind of payment method. Blockchain holds the promise of applications beyond currency, and enthusiasts are exploring projects that expand on this potential. In fact, as of early February 2018, the second-most-valuable cryptocurrency, Ethereum, is a project aimed at using blockchain for social contracts.

As more such projects and applications emerge, the world of blockchain and the complex technology fueling it are likely to continue capturing attention. Taking the time to understand the enthusiasm and technology behind this latest craze will not only help you answer client questions, but also prepare you for the future.

[1] *https://www.bloomberg.com/news/articles/2018-02-07/cryptocurrencies-are-like-ponzi-schemes-world-bank-chief-says*

WHAT IS BLOCKCHAIN?

In the simplest terms, blockchain is a distributed ledger. Data on a blockchain is stored and verified by a connected network of computers, rather than through a single entity.

Where, historically, trusted institutions have served as the owners and verifiers of data—for instance, a bank owns information about your finances and verifies transactions on your behalf—no such institution exists on the blockchain. Instead, data is dispersed throughout a network and protected behind layers of encryption.

Complex mathematical computation is required to verify transactions, and each computer on the network plays a role. Each time a new identity is created or transaction is requested, computation is needed. Storage is needed. Processing power is needed. The blockchain borrows space and power from connected computers to run the necessary computations. In exchange for this computing power, members receive rewards from the network. For most current use cases, rewards are "tokens" of cryptocurrency.

Thus, the blockchain is a connected network of computers that all lend a portion of their processing power to running its complex computations.

WHY COMPUTATIONS ARE SO COMPLEX

Encryption is the core promise of blockchain, offering layers of protection that a centralized storage entity currently cannot.

A bank, for example, maintains a database of personally identifiable information (PII) that has the potential to be hacked. If someone gains access to the database, they gain access to thousands of individuals' PII.

On the blockchain, no such central repository exists. A member's PII is used to generate an encrypted key, which is a long string of random numbers and letters. This private key is used to verify that the user is who they say they are without revealing the user's PII. Unlike current identification methods, the key cannot be reverse engineered to reveal PII.

Take the example of Social Security numbers (SSN). If someone gains access to your SSN, they can get more information about your identity fairly easily. In many cases, the SSN, coupled with easily secured PII, is the only key needed to complete transactions on your behalf. This is a breeding ground for identity theft.

On the blockchain, a private key serves as a user's identity but reveals no information about them, as it's been run through several layers of encryption. Consequently, the original PII cannot be accessed through simply having the private key.

Because encryption requires complex mathematical equations, the need for computing power is enormous to handle the encrypting demands of each new identity, as well as for every transaction on the network. This is why the blockchain uses and rewards access to the processing power of its connected computers.

INCENTIVES TO PARTICIPATE

Some people have gone so far as to dedicate entire warehouses of servers to running computations on the blockchain. They do this because the more computing power you lend the network, the more value you receive in return. Their shared processing power is used to create identities, verify transactions, and run the computations required to generate new tokens of cryptocurrency in a process called mining.

Another way to earn rewards is simply through adoption. The earliest members of a blockchain are rewarded for their participation, generating incentive for the network to grow.

As more people join, incentives gradually decrease, so the first to sign on reap the highest rewards. This may account for the high volume of initial coin offerings (ICO) in 2017 as people look to get in on the ground floor. It may also shed light on Jim Yong Kim's "Ponzi scheme" comment—in the cryptocurrency world, rewards skew in favor of early arrivers.

HOW CRYPTOCURRENCIES OPERATE ON BLOCKCHAIN

Cryptocurrencies, unlike fiat currencies, are unregulated, and their value is determined largely by public perception.

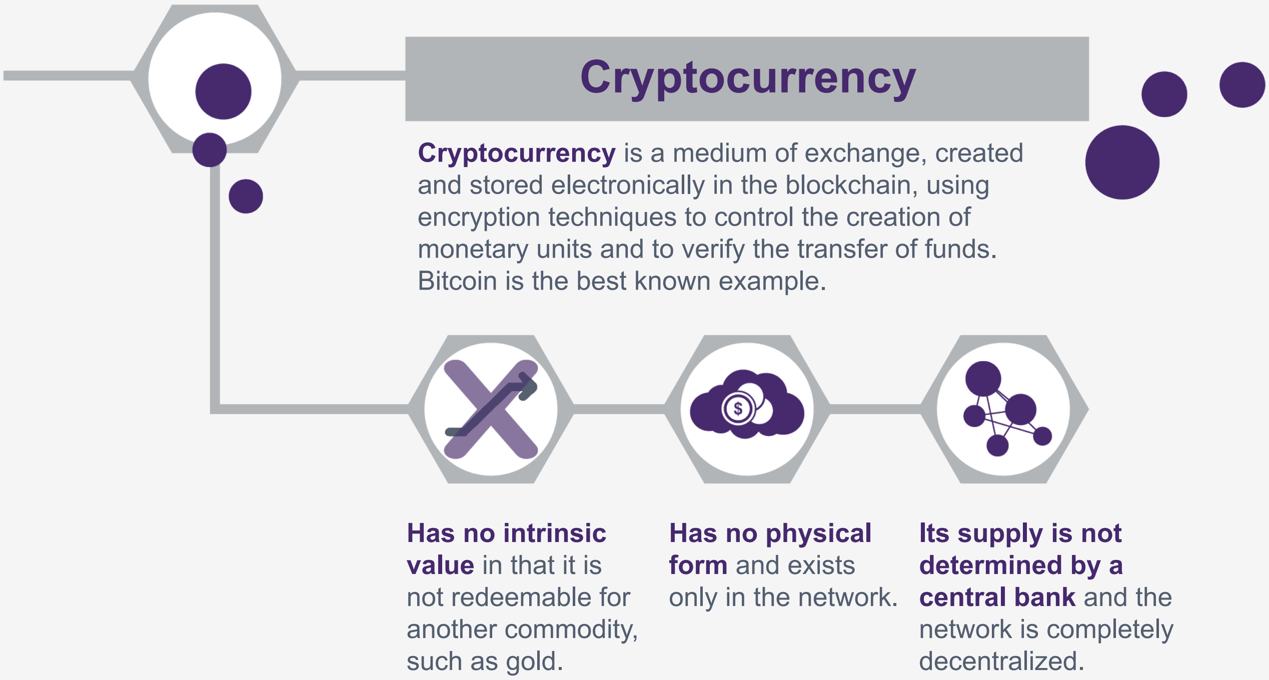
Without a tangible commodity to back the coin's value, its success depends on its ability to attract interest. To generate interest and bring a new coin to market, its creators, sometimes referred to as inventors, founders, or developers, will create a plan for growth and present it during an initial coin offering (ICO). At that time, investors commit capital to the project and receive a portion of tokens, based on the valuation of the cryptocurrency, with the hope that valuation will grow, and their tokens can be sold for profit down the line.

At a glance, this process is not dissimilar from an initial public offering (IPO), and its name evokes that parallel. However, instead of a regulated process in which investors receive shares in a company and its relatively tangible assets, investors in an ICO are purchasing the probability of inflation, with no regulating bodies to ensure the legitimacy of their investment.

An ICO also differs from an IPO in that it begins with a declared capital-raising goal, and if the goal is not met, the ICO fails. Early backers are thus incentivized to recruit others if they believe in the project. In this way, ICOs are more like crowdfunding projects, such as Kickstarter and GoFundMe, and are sometimes referred to as crowdsales.

Valuation of each coin is dependent on a variety of factors, including the complexity of its blockchain and the price of Bitcoin. Although digital payments are ostensibly a goal of cryptocurrencies, these coins are rarely accepted as tender, and in most cases, investors are purchasing not utility but the hope that their coin will gain popularity.

Each cryptocurrency comes with its own selling point. For example, Litecoin operates in much the same way as Bitcoin, but it's faster. Ethereum, with tokens called Ethers, uses its blockchain to reimagine social contracts through the distributed ledger. As of early February 2018, it is the second-highest valued cryptocurrency, trailing Bitcoin. The Ethereum blockchain also hosts applications beyond Ethers, including the popular game CryptoKitties, which bears similarities to baseball cards in that players purchase unique and collectible cat avatars, but which differs from baseball cards in the cats' ability to reproduce.



Cryptocurrency

Cryptocurrency is a medium of exchange, created and stored electronically in the blockchain, using encryption techniques to control the creation of monetary units and to verify the transfer of funds. Bitcoin is the best known example.

Has no intrinsic value in that it is not redeemable for another commodity, such as gold.

Has no physical form and exists only in the network.

Its supply is not determined by a central bank and the network is completely decentralized.

GENERATING TOKENS

Where fiat currencies print new money, tokens of most cryptocurrencies are “mined” through the solving of mathematical equations. With enough computational power, garnered from connected computers on the blockchain, a new token is introduced to the network. In the case of Bitcoin, there is a cap at 21 million tokens, which has caused contention among the community, many of whom believe the cap better serves those who view Bitcoin as an investment than those who believe in its power as a currency.

As of early February 2017, the estimated annual electricity consumption of Bitcoin is 47.83 terawatt hours, approximately as much as the country of Singapore or 4.4 million U.S. households.[2]

One notable exception to the mining process is Tether, which purports to be backed by U.S. dollars deposited into a Taiwanese bank account, though that claim is under investigation.[3] (See page 8 for more on the Tether controversy.) In Tether’s case, new tokens are “printed” when new deposits are made.

Mining of cryptocurrencies—particularly Bitcoin—has grown to such a frenzy that some have begun worrying about its environmental impact.

TRADING AND TRANSACTIONS

To buy, sell, and trade cryptocurrency, one has several options, ranging from lower-cost, higher-tech platforms to investing in funds of professionally managed crypto assets.

For many, trading happens on an exchange platform, such as the widely used Coinbase.

Coinbase and platforms like it offer users the ability to trade cryptocurrencies or buy and sell for fiat currency. These exchanges each come with their own version of a “digital wallet,” which is where a user’s identity and transaction history are stored, in the form of a public and private key.

Third-party vendors and cryptocurrencies themselves also offer their own versions of digital wallets, and users may opt to use whichever best fits their needs. Often, the benefit of an exchange’s wallet is convenience and the ability to hold multiple cryptocurrencies in one place.

[2] *https://digiconomist.net/bitcoin-energy-consumption*

[3] *http://www.tetherreport.com/*

When a transaction is requested, computers on the blockchain perform encryption computations to verify the requester's identity and confirm that sufficient funds are available in their digital wallet. When this verification is complete, the "blocks" of data having traveled through a "chain" of encryption, the transaction is recorded and reflected in the digital wallets of both the sender and receiver.

By comparison, many current transactions involve a payment processing company as an intermediary, which requests information from both the payer's and recipient's banks. The banks, in turn, update their clients' accounts, and the transaction is recorded with the payment processing company and each bank, individually. Their ledgers can be cross-referenced, but they are not a single shared entity as is the blockchain's distributed ledger.

WHY SO CONTROVERSIAL?

From an investment standpoint, cryptocurrency runs a high risk because its value is contingent on the whims and beliefs of the investing public.

In the vast majority of cases, no tangible commodity underpins the price of a coin, and many are involved in a somewhat circuitous—certainly tenuous—valuation relationship.

Many coins, for example, factor in the price of Bitcoin to determine their own value. Bitcoin, in turn, appears to share a relationship with Tether, the "stablecoin" claiming to be backed by U.S. dollars, currently under investigation by the U.S. Commodities and Futures Trading Commission (CFTC).[4] An analysis of Bitcoin's price rises indicates that 48.8% of its increases occurred during the two-hour periods following deposits of Tether into its network, Bitfinex.[5] If Tether's deposits were not, in fact, backed by deposits of USD, as claimed, Bitcoin's value was likely artificially inflated. Each coin basing its value on Bitcoin's would also be affected.

Furthermore, substantial division exists in the blockchain community over cryptocurrency's purpose and future. Those who maintain that cryptocurrency is a payment method intended for digital transactions argue that Bitcoin's arbitrary cap of 21 million tokens favors those who view cryptocurrency as an investment. If true to its stated purpose of being a currency, the token cap would limit inflation. As a result of this ideological division, a group split from Bitcoin in 2017 to form Bitcoin Cash.

[4] *https://www.bloomberg.com/news/articles/2018-01-30/crypto-exchange-bitfinex-tether-said-to-get-subpoenaed-by-cftc*

[5] *http://www.tetherreport.com/*

The question remains: If cryptocurrencies are not viable as currencies, wherein lies their inherent value? Unlike asset classes linked to production, commerce, or the success of companies in meeting particular objectives, cryptocurrencies as an asset class are valued solely on the arbitrary creation of supply and the interest that supply can generate.

Blockchain enthusiasts believe the power in this technology is its dual ability to verify identity without revealing it, offering a new and safer way to complete many tasks that currently rely on third parties for verification. Conversely, protections are limited, and regulators have yet to tackle the difficult problems posed by cryptocurrencies, which largely operate outside the bounds of current financial oversight.

Not all regulating bodies wish to legitimize cryptocurrency with oversight. For example, India's government is actively working to curb the crypto craze, with its finance minister, Arun Jaitley, declaring, "The government does not recognise cryptocurrencies as legal tender or coin and will take all measures to eliminate the use of these crypto-assets in financing illegitimate activities or as part of the payments system," on February 1, 2018.[6]

[6] *https://qz.com/1195316/budget-2018-busts-bitcoin-arun-jaitley-has-just-killed-indias-cryptocurrency-party/*

Who likes Blockchain?

Cryptocurrency Idealists

Some people believe cryptocurrency has the potential to upend the financial system in a positive way. One such group of enthusiasts has moved to Puerto Rico, many of them with millions, some with billions of dollars accrued during the cryptocurrency boom, where they intend to create an improved society with cryptocurrency as the core financial system. They call it Sol.

Cryptocurrency Opportunists

Where there is opportunity, there will always be opportunists. Certain players look to take advantage of cryptocurrency's momentum to secure a tidy profit for themselves, whether through exchanges or involvement in an ICO.

Blockchain Expansionists

Certain supporters of blockchain technology believe its most powerful future uses are in non-currency transactions. They want to develop its potential and offer alternatives to central brokers of all kinds of information not limited to finance, such as a person's social network.

Activists

Although a seemingly niche use case, several political and social uses for blockchain are already emerging. The United Nations' children's agency, UNICEF, has recruited gamers to mine Ethereum for the benefit of Syrian children,[7] and anarchist Amir Taaki is training hackers in what he hopes will be a complete overthrow of the state system.[8] (More in Projects of Note on page 14.)

Hackers

Due to its encryption demands, blockchain technology represents significant employment opportunities for hackers.

Who has reason to be wary of Blockchain?

Financial Institutions and Traditional Brokers of Information

Because blockchain aims to reduce reliance on trusted institutions, these institutions could be hurt by broader adoption of the technology.

Regulating Bodies

Blockchain and its attendant cryptocurrencies largely operate outside the bounds of current financial oversight, presenting risks for investor safety and a challenge for regulators.

Identity Protectionists

Although blockchain promises a new era of secure and consistent identity on the internet, some remain concerned about unanswered questions, such as what would happen if a bad actor were to purchase enough mining power to control 51% or more of the blockchain?[9] They could undermine the entire blockchain.

Environmentalists

The computing power required to run blockchain calculations is consuming a substantial amount of power. Bitcoin alone is responsible for the use of enough electricity to power millions of U.S. households. Additionally, upgrades in technology to handle ever-increasing computing demands are generating significant waste in the form of discarded digital equipment. Environmentalists are concerned about the unchecked impact of the current craze.

[7] *https://www.theguardian.com/global-development/2018/feb/06/unicef-recruits-gamers-mine-ethereum-aid-syrian-children*

[8] *https://qz.com/1192640/*

[9] *https://www.coindesk.com/blockchain-immutability-myth/*

MORE THAN A FAD, LESS THAN A GOLDEN TICKET

Bitcoin's dominance of late-2017 headlines piqued the interest of many investors looking to turn a quick and hopefully extraordinary profit. Seasoned professionals recognized the bubble as it was inflating, and many were unsurprised by the pop in early 2018. Still, the investing public remains undeterred, and cryptocurrency continues to capture attention.

With new projects and use cases continuing to emerge, clients are likely to ask about cryptocurrency and blockchain in the future. If you haven't already, now may be a good time to make a plan for addressing these topics when they arise. Consider both your own personal beliefs and your clients' best interests in whether you're willing to recommend cryptocurrency, and prepare to offer alternatives, as well.

For those looking to invest in new technology, look into blockchain projects and applications other than cryptocurrency. For those interested in the potential for cryptocurrency to upend the current credit landscape, you may explore other alternative payment options that operate in a more regulated space.

For those with high risk and volatility tolerance who remain interested in cryptocurrency, hopefully this paper will give you the baseline knowledge to offer guidance in engaging with cryptocurrency as part of a balanced portfolio.

GLOSSARY OF TERMS

Blockchain
A distributed ledger technology that decentralizes data and transactions, verifying information not through a central body but through a network of connected computers. Blocks of data travel through a chain of encryption, giving the technology its name.

Cryptocurrency
A digital currency comprised of tokens and operating on a distributed ledger. The “crypto” part of its name refers to the layers of encryption involved in creating tokens and verifying transactions. Examples include Bitcoin, Ethereum, Ripple, Bitcoin Cash, Cardano, and Litecoin. Sometimes referred to as coins.

Digital wallet
A place where a user’s identity information and transaction history are stored, in the form of a private and public key.

Exchange
A platform on which trades and sales of cryptocurrencies take place, similar to a stock market exchange. Examples include Coinbase and GDAX.

Initial coin offering (ICO)
A process through which creators of a new cryptocurrency present a plan and recruit backers for their project. If they meet their stated capital-raising goals, the ICO is successful, and the coin is created. If it fails, the ICO is unsuccessful, and the project does not move forward. Sometimes referred to as crowdsales.

Mining
A process in which new tokens of a cryptocurrency are brought to the blockchain network by connected computers performing complex calculations and lending computing power to the network.

Private key
A string of random characters and numbers that serves as a user’s identity on the blockchain. It is used to verify transactions and cannot be reverse engineered to reveal personally identifiable information (PII).

Public key
A string of random characters that serves as a record of transactions and token holdings on the blockchain.

Token
A unit of cryptocurrency. Tokens may be purchased with other cryptocurrency or fiat currency on an exchange, awarded as part of an initial coin offering (ICO), or mined. Where accepted, tokens may be used as currency in digital transactions.

10 MOST VALUABLE CRYPTOCURRENCIES

As of February 10, 2018

1. Bitcoin (BTC)

The first and gold standard, developed by unknown person or group of people using the name Satoshi Nakamoto, released in 2009

2. Ethereum (ETH)

Programmable contracts and money, developed by Vitalik Buterin, released in 2015

3. Ripple (XRP)

Enterprise payment settlement network, developed by Arthur Britto, David Schwartz, Ryan Fugger, released in 2012

4. Bitcoin Cash (BCH)

A hard fork from the Bitcoin cryptocurrency, proposed by Amaury “Deadal Nix” Séchet, launched 2017

5. Cardano (ADA)

Layered currency and contracts, developed by firm Input Output Hong Kong (IOHK) and led by Charles Hoskinson, released 2017

6. Litecoin (LTC)

Faster Bitcoin, developed by Charlie Lee, released 2011

7. NEO (NEO)

Chinese-market version of Ethereum, developed by Da Hongfei, launched in 2014

8. Stellar Lumens (XLM)

Digital IOUs, founded by Jed McCaleb and Joyce Kim, released in 2014

9. EOS (EOS)

Decentralized applications and decentralized autonomous corporations, developed by block.one, released 2018

10. IOTA (MIOTA)

Internet-of-things payments, founded by David Sønstebø, Sergey Ivancheglo, Dominik Schiener, and Serguei Popov, released in 2015

PEOPLE AND PROJECTS OF NOTE

Bitcoin's Creators

Bitcoin was created by an individual or group of people who choose to remain anonymous and use the moniker Satoshi Nakamoto. Despite speculation, the identity or identities of the creator(s) have not been confirmed.

Bitcoin's early backers and evangelists include Roger Ver, also known as "Bitcoin Jesus," and Brock Pierce, director of the Bitcoin Foundation and co-founder of Block.One, which developed its own cryptocurrency, EOS. Both Ver and Pierce are controversial figures with criminal activity in their pasts. Several Bitcoin Foundation board members resigned when Pierce was elected. He now leads the Puertopia/Sol movement in Puerto Rico.

Sol (Puertopia)

A group of newly wealthy cryptocurrency enthusiasts have moved to Puerto Rico with the aim of building a new utopian society with cryptocurrency as the financial system. They originally named the project Puertopia before learning the Spanish translation was, "eternal boy playground."[10] The project has since been renamed Sol.

Ethereum

Created by Vitalik Buterin, Ethereum is blockchain technology used to broker contracts on the digital ledger. Its technology is among the first and most prominent use cases of blockchain beyond cryptocurrency. Applications sit atop the Ethereum platform and use the blockchain to connect their users.

One example is the popular game CryptoKitties, in which players buy, sell, trade, and breed avatars of cats. The game is similar to baseball cards in that some traits are more desirable than others, and each CryptoKitty is unique. Unlike baseball cards, however, the cats can breed and create new generations of CryptoKitties.

UNICEF's Game Changers

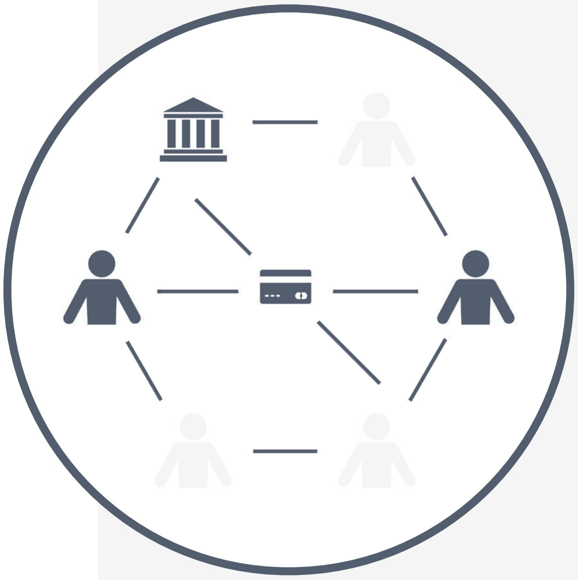
The United Nations' children's agency, UNICEF, began a program recruiting gamers to donate a portion of their computer's processing power to mining cryptocurrency for Syrian children. Although still in its infancy, the program is pioneering ways for blockchain technology and cryptocurrency to be used for humanitarian aid purposes.

Amir Taaki, Polytechnics, and Rojava

Anarchist and cryptocurrency influencer Amir Taaki is setting up an institute called Polytechnics with the aim of training a politically motivated cadre of hackers to overturn state systems. He spent time in Syria fighting ISIS on behalf of Rojava, a territory bordering Syria, Turkey, and Iran seeking to become its own autonomous state. If successful, his institute could give him and his students the ability to establish a viable alternative to current state systems of power.

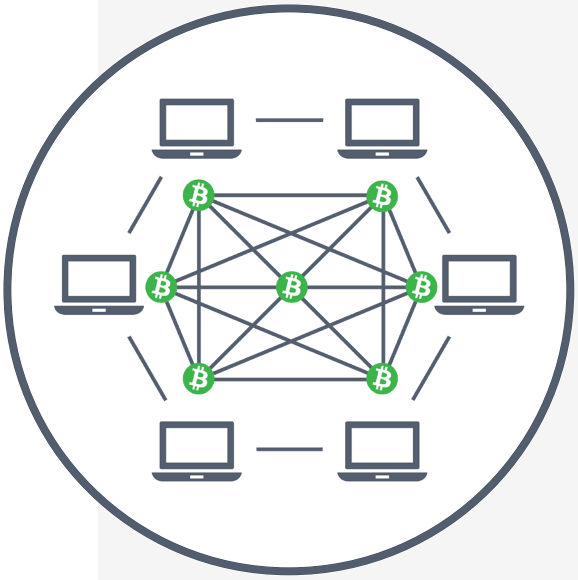
[10] *https://www.nytimes.com/2018/02/02/technology/cryptocurrency-puerto-rico.html*

PAYMENT PROCESS: CURRENT VERSUS BITCOIN



Current Transactions

Current payment systems require third-party intermediaries that often charge high processing fees...



Blockchain

...but machine-to-machine payment using the Bitcoin protocol could allow for direct payment between individuals, as well as support micropayments.

For use with financial professionals only.