

David W. Griffis, CFA

Principal &amp; Portfolio Manager



## An Introduction to Cryptocurrency & Bitcoin

### WHAT IS CRYPTOCURRENCY?

The IRS defines virtual currency as a digital representation of value that serves as a medium of exchange, unit of account, and/or a store of value. Cryptocurrency is a form of virtual currency that uses cryptography to authenticate and secure transactions that are digitally recorded on a distributed ledger, such as blockchain.<sup>1</sup> Blockchain is not a cryptocurrency, rather it is the underlying technology that enables cryptocurrency. IBM describes blockchain as a shared, unchangeable ledger that facilitates the process of recording transactions and tracking assets in a network.<sup>2</sup>

The most popular cryptocurrency is Bitcoin, but several others exist. According to CoinMarketCap, over 4,000 different cryptocurrencies were in existence as of February 11, 2021.<sup>3</sup> Other popular cryptocurrencies include Ethereum, Litecoin, and XRP, known as Ripple. This paper will focus primarily on Bitcoin.

### BITCOIN BASICS

Bitcoin and other major cryptocurrencies operate utilizing three important pieces of information: the address, which is associated with a balance and used for sending and receiving funds, and the address's corresponding public and private keys. The creation of a bitcoin address begins with the creation of a private key. At that point, its corresponding public key can be derived using an algorithm. The address, which

can then be used in transactions, is a shorter, representative form of the public key.

The private key is what gives a cryptocurrency user possession of the funds on a given address. When currency is sent, the software signs the transaction with the user's private key (without revealing it), which signals to the entire network that the user has the authority to transfer the funds on the address from which the user is sending.

It is important to note that it is not possible to derive the private key by using the address or public key, i.e., it is a one-way street. This feature makes Bitcoin very secure. It also means that private keys that are lost cannot be recovered, in which case the user will not be able to access the Bitcoins in his or her account. In a letter dated July 22, 2020, the Office of the Comptroller of the Currency stated that any national bank can hold the unique cryptographic keys for cryptocurrency wallets.<sup>4</sup> This provides a measure of safety for users who are concerned about being locked out of their accounts.

Crypto custodians typically charge custody fees ranging from 4 to 10 basis points per month, but it varies by institution.<sup>5</sup>

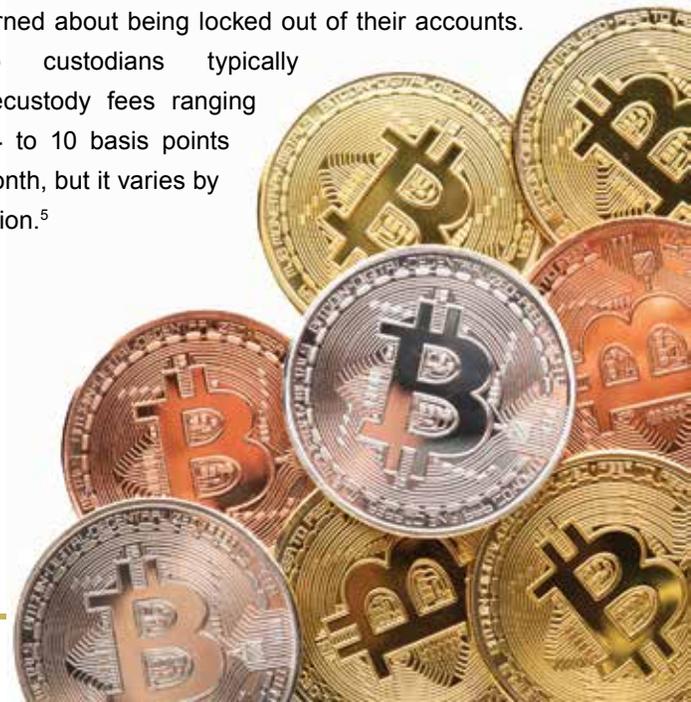
1 <https://www.irs.gov/businesses/small-businesses-self-employed/virtual-currencies>

2 <https://www.ibm.com/blockchain/what-is-blockchain>

3 <https://coinmarketcap.com/>

4 <https://www.coindesk.com/banks-in-us-can-now-offer-crypto-custody-services-regulator-says>

5 <https://www.coindesk.com/prime-trust-now-charges-no-fee-for-crypto-custody>



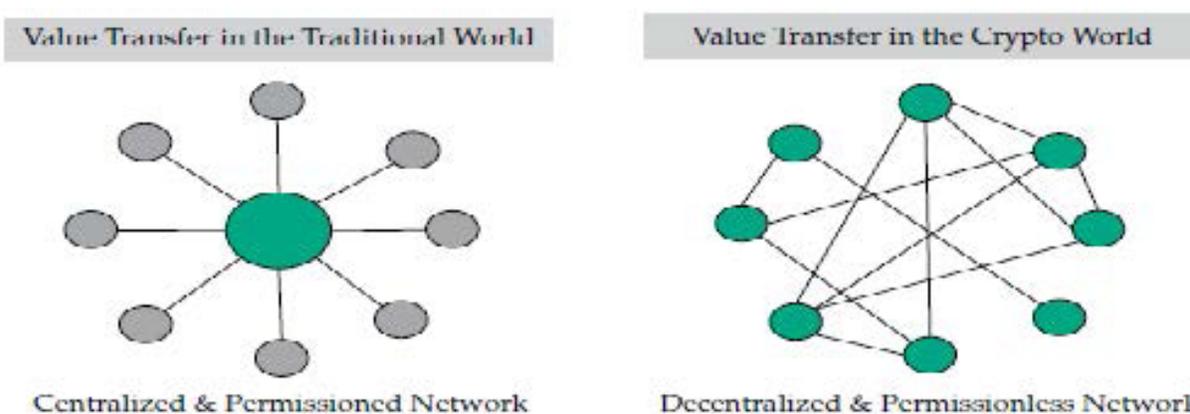
To purchase Bitcoin, the first step is to download a Bitcoin wallet, which is where the Bitcoins will be stored. This can be in the form of a mobile wallet, desktop wallet, or a hardware wallet, which looks like a USB flash drive. There are free and paid versions of the mobile and desktop wallets which offer different features but serve the same core function of storing Bitcoins.<sup>6</sup> The Bitcoin wallet is linked to a debit or credit card, Apple Pay, or bank account and allows the user to deposit and withdraw money from the Bitcoin wallet. Bitcoin can be bought and sold using the Bitcoin website, a Bitcoin wallet app, the Bitcoin peer-to-peer trading platform, or on a cryptocurrency exchange. Regardless of the method chosen, it just takes a few clicks, and the Bitcoin is deposited into (withdrawn from) the Bitcoin wallet and the corresponding cash is removed from (deposited into) the Bitcoin wallet.

When sending and receiving Bitcoin, the receiver's wallet provides them with an address or QR code to be shared with the sender. The sender enters the address or scans the QR code of the receiver, enters the amount to be sent, and confirms the payment to be made to the receiver. The transaction is then processed, and the wallets of both parties are updated.<sup>7</sup>

One of the appeals of Bitcoin is the ability to transfer large sums of money relatively quickly. According to CryptoVantage.com, sending Bitcoin can take anywhere from seconds to over an hour, but usually it takes 10 to 20 minutes.<sup>8</sup> The reason for this lies in Bitcoin's decentralized and permissionless network, which is illustrated in Figure 1.<sup>9</sup> A decentralized network can be thought of as a network that is built and maintained by a group of computers that are owned by many different parties. This means that users can transact with each other directly in the same way that payments applications, like Venmo, operate. This allows transactions to be processed quickly, 24 hours a day. As an example: on April 12, 2020, an individual transferred 161,500 Bitcoin – with a value of \$1.1 billion at the time – in just one transaction. The transaction settled in 10 minutes.<sup>10</sup>



**Figure 1**



6 <https://bitcoin.org/en/choose-your-wallet?step=1&platform=windows&user=experienced>

7 <https://www.youtube.com/watch?v=7maNVTM8B1E>

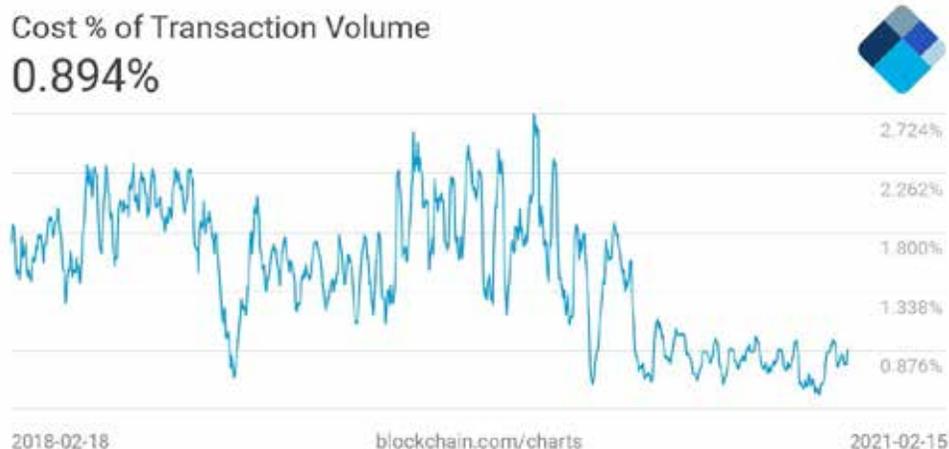
8 <https://www.cryptovantage.com/news/ask-cryptovantage-how-long-does-it-take-to-send-bitcoin/#:~:text=In%20general%20sending%20Bitcoin%20can,what%20occurs%20when%20sending%20bitcoin.>

9 Hougan, M; Lawant, D. (2021). Cryptoassets: The Guide to Bitcoin, Blockchain and Cryptocurrency for Investment Professionals.

10 Turner Wright, "Bitfinex Made a \$1.1 Billion BTC Transaction for Only \$0.68," Cointelegraph (13 April 2020). <https://cointelegraph.com/news/bitfinex-made-a-11-billion-btc-transaction-for-only-068>.

The cost of sending and receiving Bitcoin varies based on the size of the transaction and network supply and demand. Larger transactions require more work and therefore, require a higher fee. At times, congestion occurs on the network, which also results in higher fees. According to Blockchain.com, there is essentially a pool of transactions waiting to be settled at any given time. The miners – who settle the transactions – choose which transactions to settle, giving precedence to those willing to pay higher fees.<sup>11</sup> This can result in users bidding up the fee to have their transactions processed more quickly. The cost as a percentage of transaction volume is shown in Figure 2.<sup>12</sup>

The cost of purchasing Bitcoin varies depending on the platform that is used. PayPal's fee starts at \$0.50 for purchases under \$25.00 and increases for larger purchase. Coinbase has a similar structure with its fee starting at \$0.99 for purchases under \$10.00 and increasing for larger purchases. Robinhood offers free cryptocurrency trades.<sup>13</sup>



## HOW CAN VERO BEACH GLOBAL ADVISORS GAIN EXPOSURE TO BITCOIN?

Currently, neither Charles Schwab nor Fidelity Investments can hold cryptocurrency. The best way for Vero Beach Global Advisors to gain exposure to Bitcoin is via Grayscale Bitcoin Trust (symbol: GBTC), which is a closed-end fund. According to its website, GBTC is invested solely and passively in Bitcoin. As of February 12, 2021, the fund has AUM of \$30.2 billion and charges an annual fee of 2.0%.<sup>14</sup> Additionally, the fund trades at an 8.88% premium to its net asset value (NAV) and has traded at a 17.85% premium to its NAV over the last 52 weeks.<sup>15</sup> The fund does not pay a dividend as Bitcoin does not produce cash flows.



<sup>11</sup> <https://support.blockchain.com/hc/en-us/articles/360000939883-Explaining-bitcoin-transaction-fees>

<sup>12</sup> <https://www.blockchain.com/charts/cost-per-transaction-percent>

<sup>13</sup> <https://www.coindesk.com/bitcoin-trading-fees-on-paypal-robinhood-cash-app-and-coinbase-what-to-know>

<sup>14</sup> <https://grayscale.co/bitcoin-investment-trust/#overview>

<sup>15</sup> <https://www.bloomberg.com/quote/GBTC:US>

# CONCLUSION

The goal of this paper is to provide an introduction to cryptocurrency – more specifically Bitcoin – and its basic features. Tesla Inc. and MicroStrategy Inc. are two publicly traded companies that have recently made large investments in Bitcoin. MicroStrategy has gone as far as making Bitcoin its primary treasury reserve.<sup>16</sup> News headlines like this will continue to fuel the exuberance surrounding Bitcoin and other cryptocurrencies, but for the foreseeable future, there is not any evidence that cryptocurrencies will replace traditional currencies in any meaningful way.

## Below is a summary of a Forbes article provided the following Risk Factors Specific to Bitcoin and Other Cryptocurrencies

Successfully investing or trading bitcoin and other cryptocurrencies requires technical skill and at least a basic knowledge of how Blockchain works. Below are some of the most significant issues that investors should be aware of in this new and rapidly changing industry.

### 1. Loss or Destruction of the Private Key

Bitcoins (and this applies to other cryptocurrencies) are stored in a digital wallet and are controllable only by the possessor of both the public key and the private key relating to the digital wallet in which the bitcoins are held, both of which are unique. If the private key is lost, destroyed or otherwise compromised, an investor may be unable to access the bitcoins held in the related digital wallet which will essentially be lost. If the private key is acquired by a third party, then this third party may be able to gain access to the bitcoins.

*German-born programmer Stefan Thomas made headlines in 2020 after a lost password rendered his bitcoin stash worth \$220 million inaccessible. The secure hard drive, on which 7,002 bitcoins were stored, was an IronKey device. It gives owners 10 chances to guess their password before encrypting the contents. Thomas only had two attempts left to guess correctly before this situation occurred. The New York Times initially reported Thomas' plight and quoted him as saying: "I would just lay in bed and think about it: Then I would go to the computer with some new strategy, and it wouldn't work, and I would be desperate again." A potential loss of that magnitude makes "you sort of question your own self-worth," he added. On Saturday, the stash was worth about \$220 million, but as bitcoin prices surged this year, it had been valued above \$240 million.*

*When **cryptocurrency** billionaire Mathew Mellon died unexpectedly in April of 2020, access to his fortune in Ripple XRP was lost forever. The **crypto** billionaire held around half a billion US dollars of Ripple XRP. For security reason, only*

*himself had access to the funds, meaning the money may now be lost forever.*

### 2. Other Cyber-Security Risks Including Malicious Activity

Trading platforms and third-party service providers may be vulnerable to hacking or other malicious activities. For example, in August 2016, nearly 120,000 units representing US\$72 million-worth of bitcoins were stolen from the Bitfinex exchange in Hong Kong, which led to an immediate 23% drop in pricing. One year earlier, in September 2015, BitPay lost approximately \$1.8 million of bitcoins due to a phishing attack. Also, if one or more malicious actor(s) obtain control of sufficient consensus nodes on the Bitcoin Network or other means of alteration, then a Blockchain may be altered. While the Bitcoin Network is decentralized, there is increasing evidence of concentration by creating of "mining pools" and other techniques, which may increase the risk that one or several actors could control the Bitcoin Network or other similar Blockchain.

### 3. Risks Associated with Peer-to-Peer Transactions

Digital currencies can be traded on numerous online platforms, through third party service providers and as peer-to-peer transactions between parties. Many marketplaces simply bring together counterparties without providing any clearing or intermediary services and without being regulated. In such a case, all risks (such as double-selling) remain between the parties directly involved in the transaction.



<sup>16</sup> <https://www.zdnet.com/article/teslas-1-5-billion-bitcoin-purchase-points-to-cryptocurrency-as-tech-company-reserve-currency/>

#### 4. Other Risks Related to Trading Platforms and Exchanges

Digital currency trading platforms, largely unregulated and providing only limited transparency with respect to their operations, have come under increasing scrutiny due to cases of fraud, business failure or security breaches, where investors could not be compensated for losses suffered. Although one does not need a trading platform or an exchange to trade bitcoins or other cryptocurrencies, such platforms are often used to convert fiat currency into cryptocurrency, or to trade one cryptocurrency for another.

#### 5. Loss of Confidence in Digital Currencies

Cryptocurrencies are not backed by a central bank, a national or international organization, or assets of other credit, and their value is strictly determined by the value that market participants place on them through their transactions, which means that loss of confidence may bring about a collapse of trading activities and an abrupt drop in value.

#### 6. Regulations Preventing or Restricting Trading of Digital Currencies

There are significant inconsistencies among various regulators with respect to the legal status of digital currencies. Regulators are also concerned that bitcoin and other cryptocurrencies may be used by criminals and terrorist organizations. In the future, certain countries may restrict the right to acquire, own, hold, sell or use digital currencies.

#### 7. Taxation of Digital Currencies

It should be noted that there is substantial uncertainty with respect to the tax treatment of an investment in digital currencies. Bitcoins and other cryptocurrencies may be considered assets in certain jurisdictions and currency in others. Sales or value-added taxes may be imposed on purchases and sales of digital currencies.

#### 8. Slow-Down of Network

For bitcoins, mining is the process by which bitcoins are created and transactions verified. Through downloading a specific software, the user's computer becomes a "node" that validates blocks (i.e. details of some or all of the most recent transactions). Miners which are successful in adding a block to the Blockchain are automatically awarded bitcoins (plus transaction fees for transactions recorded). However, if the rewards for solving blocks and transaction fees are not sufficiently high, or if a high volume of transactions occur at the same time, the Blockchain may experience a slow-down. A slow-down is also possible for other cryptocurrencies, if the number of transactions on the blockchain is very high.

#### 9. Dilution Due to Competition or "Fork" in the Blockchain

Last but not least, cryptocurrencies are based in protocols which govern the peer-to-peer interactions between various users. Dissent between users as to protocols to be used may result in a "fork", opening two separate networks. For example, in 2016, Ethereum experienced a permanent fork in its Blockchain that resulted in two versions of its digital currency, Ethereum (ETH) and Ethereum Classic (ETC), which trade very differently. Very recently, Bitcoin also experienced its first fork, leading to the creation of Bitcoin Cash (BCC), a new cryptocurrency.



**VERO BEACH  
GLOBAL ADVISORS**

Registered Investment Advisor

verobeachglobaladvisors.com | (772) 213-8000  
4625 Florida A1A, Suite 9, Vero Beach, FL 32963

The views expressed in this material are the views of David W. Griffis through 2.16.21. The views are subject to change based on market and other conditions. This document contains certain statements that may be deemed forward-looking statements. Please note that any such statements are not guarantees of any future performance and actual results or developments may differ materially from those projected. This is not an offer or solicitation for the purchase or sale of any security and should not be construed as such. References to specific securities and issuers are for illustrative purposes only and are not intended to be, and should not be interpreted as, recommendations to purchase or sell such securities. Vero Beach Global, LLC is governed under the Securities and Exchange Commission as an Investment Advisor under the Investment Advisors Act of 1940. All investments contain risk and may lose value.