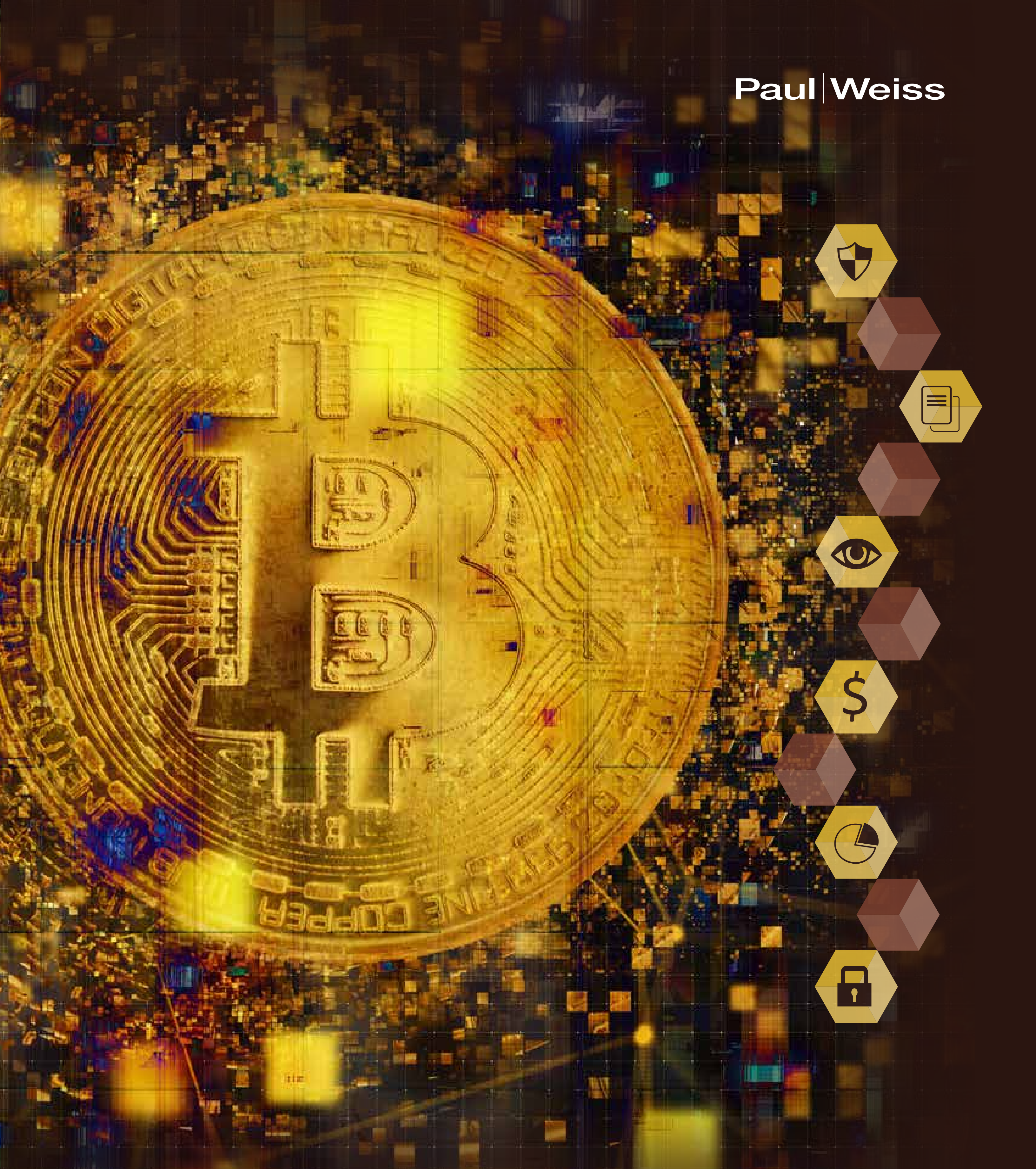
Paul | Weiss



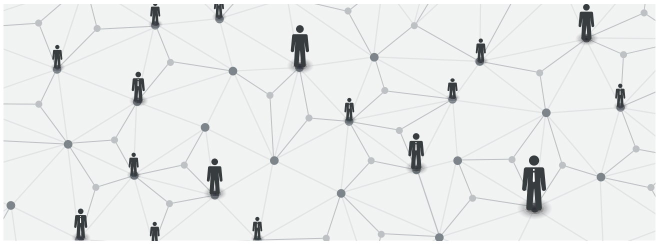
Cryptocurrency

The development and growth of cryptocurrencies and blockchain technology has implications for many industries, including finance, media, and healthcare. In a series of papers, we will discuss the variety of ways in which cryptocurrencies and blockchains are being used in different fields. This paper, the first in our series of three papers, discusses cryptocurrencies, including how they operate in conjunction with the blockchain and how Bitcoin, the first major cryptocurrency, compares to traditional, fiat currencies.

What is a cryptocurrency?

A cryptocurrency is a digital asset that can function as a medium of exchange. As the name suggests, cryptocurrencies use cryptography to secure and verify transactions and control the production of new units of the cryptocurrency. These transactions, in turn, are stored on a “blockchain” ledger. Bitcoin, the first cryptocurrency, was introduced in 2008 but did not gain widespread public attention until early 2017. Today, there are over 2,200 different cryptocurrencies, some of the most notable of which are Bitcoin, Ether, Ripple, Litecoin, Monero, and Facebook’s proposed cryptocurrency Libra.

What is Bitcoin?



Bitcoin, the most well-known cryptocurrency, is a decentralized digital currency network that employs blockchain technology to facilitate digital transfers of value, without the need for a centralized or trusted middleman. Bitcoin, together with the underlying blockchain technology, was developed by one or more developers, who used the pseudonym Satoshi Nakamoto and published a white paper and accompanying open source code on October 31, 2008. The Bitcoin network is open to the public (*i.e.*, anyone can purchase or transfer bitcoin) and allows for permissionless, trustworthy and secure transactions across the world.

Quick Figures

(as of August 14, 2019)[1]

Cryptocurrency:

Number of Cryptocurrencies: Over 2,400
Number of Exchanges: Over 200
(regulated and unregulated)
Total Market Cap: Over $265 billion

Bitcoin:

Number of Bitcoins in Circulation:
Over 17 million (out of a total 21 million)
Total Market Cap: Over $180 billion
24-Hour Trade Volume: Over $19 billion

Purchasing/Using Bitcoin

In the years since its creation, purchasing Bitcoins has become relatively simple.

- Users can store their private keys in a "wallet" and can choose from several different types available from multiple providers, including mobile wallets, web wallets and hardware wallets.
- Users can create an online account on a cryptocurrency exchange, where the user can provide credit card or bank account information and purchase Bitcoin (or other cryptocurrencies) for value.
- Once a user purchases cryptocurrency, he or she is assigned a "private key" – a unique numeric ID like a password consisting of a string of letters/numbers. Each private key is personal to and only known by the user to which it is assigned.
- The private key is used to access the purchased Bitcoins and to execute transactions.

Comparison to Fiat Currency

This section explains certain key attributes of Bitcoin and other cryptocurrencies by comparison with traditional cash or fiat currency. The following quick reference table provides a roadmap:

	Cash	**Bitcoin**
Security	Anti-counterfeiting security	Crypto security
No Double Spending	Tangible exclusivity	Ledger that records unique transactions
Regulatory Scheme	Institutionally backed (*e.g.*, Central bank)	Decentralized peer-to-peer
Accepted as Money	Traditional payment method; global reciprocity	Gaining acceptance by merchants and consumers
Scarcity	Central bank regulated supply	Finite supply and computational limits
Stability of Value	Generally stable, subject to economic and policy factors	Very volatile, to date

Anti-counterfeiting

Cash

Paper cash contains many security features to prevent counterfeiting. These can include: randomly disbursed security fibers, watermarks, color-shifting ink that changes from copper to green as the note is tilted 45 degrees, a vertical security thread woven into the note's fabric, and unique serial numbers.

Bitcoin

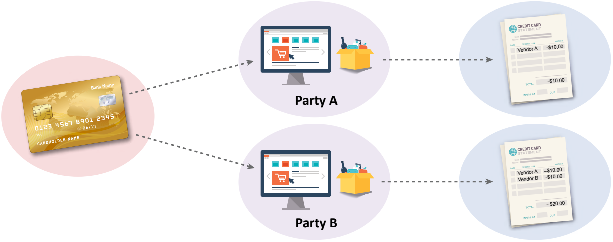
Security features of Bitcoin are twofold: Bitcoin's security relies on: (i) cryptography and (ii) the blockchain (*i.e.*, the distributed public ledger).

Cryptography converts ordinary data into a unique series of numbers and letters that is unintelligible without decryption. The National Security Agency has developed various cryptographic algorithms, including Secure Hash Algorithm 256, which is a widely used cryptographic hashing standard employed by Bitcoin. Bitcoin's hash algorithm always returns a unique, but unintelligible, output result for any unique, unencrypted, input content. That is, no two different inputs will ever return the same output. Moreover, even a tiny difference in inputs produces a massively different output. Experts believe that hacking the algorithm to reproduce the original input is impossible with current computer technology.[2]

Second, Bitcoin transactions are subject to verification before they are cleared to be included in the blockchain. The blockchain ledger is itself cryptographically hashed, and it is also distributed in hashed form over multiple independent computer servers. This makes the blockchain impenetrable according to experts, earning it the nickname the "immutable ledger." As such, cryptocurrency transactions stored in a blockchain ledger are considered impervious to falsification or alteration.[3]

No double spending

Cash

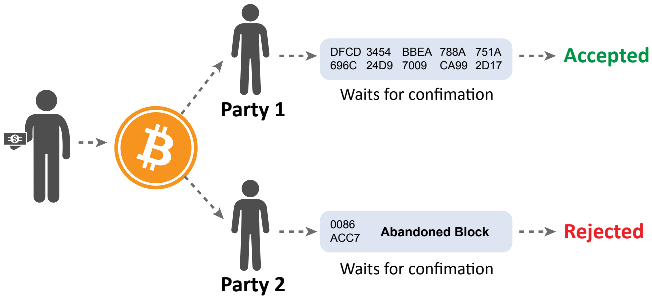


The value of money depends, in part, on the inability to spend the same unit of money (*e.g.*, the same $5 bill) multiple times. With cash, this concept is easy to understand. If you pay for your morning coffee with a $5 bill, for example, you can't use that same $5 bill to pay for anything else. Paying with a credit card, or even a mobile payment service operates to preserve the same principle. Each individual transaction is verified by a centralized intermediary like a bank or credit card company, and the amount spent is debited from the consumer's account instantaneously. When a person initiates a subsequent transaction, her or his account is debited again, and the balance is further reduced. This ensures that a person can never spend the same money twice.

Bitcoin

Unlike cash, digital currencies (like Bitcoin and other cryptocurrencies) could, in principle, be copied absent a mechanism that prevents double spending. In reality, a digital coin can be thought of as an encrypted computer file, and like any other file, it could be copied and transferred multiple times without some form of external protection.

Bitcoin and other cryptocurrencies address this problem by using the blockchain ledger to ensure that no one can spend the same coin twice. When someone tries to spend a Bitcoin, the transaction goes through a verification process to confirm who is the current owner of that Bitcoin – this is done by comparing records maintained in the blockchain. If ownership is verified, then the transaction will be authorized; but, if the ledger indicates that the Bitcoin has already been spent by its purported owner, the transaction will be declined.



Also, immediately upon its authorization, each new transaction is recorded in the blockchain ledger. Therefore, if the same person tried to spend the same Bitcoin twice, the transaction would be invalid because the blockchain would already reflect the change of ownership made in the first transaction. To reconcile near-simultaneous transactions, the blockchain uses exact time stamps and a reconciliation protocol to ensure that the priority of transactions is preserved.

Regulatory Scheme

Cash

In the United States, the Federal Reserve issues dollars and acts as a trusted third party to guarantee that currency. Fiat currencies of other nations are regulated in substantially similar ways.

Bitcoin

Bitcoin runs on a peer-to-peer network. Like the Internet, no one person or entity controls it, and there is no single regulatory or other central authority. However, certain design and coding decisions have historically been made by majority consensus amongst the Bitcoin community. Other key decisions, like the ultimate supply of Bitcoins available, are hard-coded into Bitcoin's underlying algorithms.

Accepted as money

Cash

Cash is a traditional payment method and is universally accepted as a form of payment. Even mobile payment services, like Venmo or Apple Pay, are traditionally linked to cash.

Bitcoin

Certain merchants and larger companies (particularly in the tech space) have begun to accept Bitcoin. Companies that currently accept payment via Bitcoin include Overstock.com, Microsoft, Subway, Expedia and others.[4] Many of the companies that offer Bitcoin as a payment option partner with a third party payment processor to convert Bitcoin to local currency.

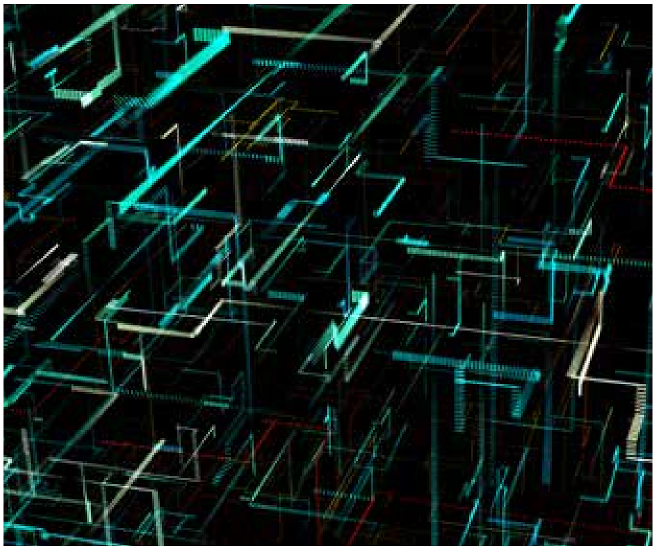
However, as discussed further under Stability of Value below, the high volatility of Bitcoin prices currently makes it difficult for consumers and merchants to rely on Bitcoin as an effective currency for transactions.

Scarcity

Cash

In most major economies, currency is issued by as an instrument of policy. There was approximately USD $1.70 trillion in circulation as of January 31, 2019, of which USD $1.66 trillion was in Federal Reserve notes.[5]

Bitcoin



In a cryptocurrency system, there is no central authority that regulates the monetary base. Instead, new units of the cryptocurrency are created by the "nodes" or servers that run the peer-to-peer network that stores and operates the underlying blockchain ledger. Bitcoin has a finite supply of 21 million Bitcoins, which is hard-coded into the algorithm that the Bitcoin "nodes" run. However, other cryptocurrencies have no maximum supply at all. For example Ethereum, which is the second largest cryptocurrency, has no supply cap.

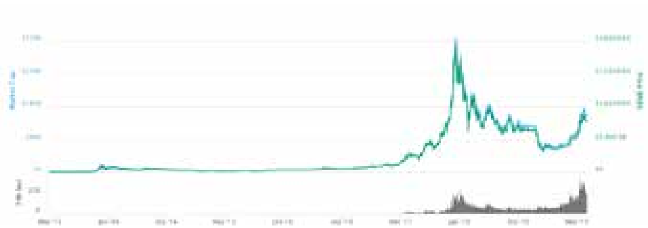
The process to create new Bitcoins is called "mining" and involves solving cryptocurrency problems to find new secure hashing sequences.[6] The computational power required to "mine" each new Bitcoin increases with the number of Bitcoins in circulation. This is because the calculations to find new secure hashing sequences become successively more difficult as the "easiest" possibilities are used up. The rate of new Bitcoin issuances is also programmed to decrease over time. While there are currently over 17 million Bitcoins in circulation with a current market cap of over $180 billion, it is estimated that we won't reach 21 million until 2140.[7]

Stability of Value

Cash

Though relatively stable, the value of cash fluctuates based on a number of economic and policy factors. The value of national currencies tend to be stable in most major economies. However, in developing economies, currency can fluctuate dramatically. For example, as of November, 2018, Venezuela's inflation rate hit 830,000%.[8] Zimbabwe's inflation rate reached 500 billion percent at its peak in 2009. By contrast, the United States, however, has maintained a rate of inflation of around two percent or less over the past decade.[9]

Bitcoin



Bitcoin (USD) Price, CoinMarketCap, <https://coinmarketcap.com/currencies/bitcoin> (last visited June 10, 2019).

Bitcoin's value is substantially more volatile and less predictable than most traditional currencies. It has fluctuated dramatically, and sometimes without warning or clear correlations with other asset classes. In 2017 alone, Bitcoin's price rose from $973 in January to $5,856 in October, and skyrocketed towards $20,000 by year end. By February 2018, however, Bitcoin had fallen below $7,600. Most recently, in June 2019, Bitcoin's price rose to approximately $10,000 and has stabilized slightly since then.[10] With its proposed cryptocurrency called Libra, Facebook and other founding members of the Libra Association aim to create a cryptocurrency that is backed by a reserve of real assets, which theoretically would be significantly less volatile than Bitcoin.

Conclusion

Many believe cryptocurrencies have potential to become widely accepted as a form of currency. However, extreme price volatility and other factors currently pose headwinds for widespread adoption of cryptocurrencies. Nonetheless, cryptographic security and the blockchain ledger offer unique qualities that arguably rival traditional currencies in certain respects.

We invite you to read the next paper in our series, which focuses on blockchain, the distributed ledger technology that enables cryptocurrencies. That paper also covers Ethereum, the most prominent platform for building blockchain-based applications.

[1] CoinMarketCap, <https://coinmarketcap.com> (last visited August 14, 2019).

[2] *See What is Cryptography?*, Techopedia, <https://www.techopedia.com/definition/1770/cryptography> (last visited Sept. 25, 2018); *see also* Roger A. Grimes, *All You Need to Know About the Move From SHA-1 to SHA-2 Encryption*, CSO Online, <https://www.csoonline.com/article/2879073/encryption/all-you-need-to-know-about-the-move-from-sha1-to-sha2-encryption.html> (last visited Sept. 24, 2018).

[3] *See* Don & Alex Tapscott, Blockchain Revolution: How the Technology behind Bitcoin is Changing Money, Business and the World 6-8, 17-18 (2016).

[4] *Who Accepts Bitcoins as Payment? List of Companies, Stores, Shops*, 99bitcoins.com, <https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins> (last visited October 26, 2018).

[5] *FAQs*, <https://www.federalreserve.gov/faqs/currency_12773.htm> (last visited, June 10, 2019).

[6] *See* Primavera De Filippi & Aaron Wright, Blockchain and the Rule of Law: The Rule of Code at 21 22, (Harvard University Press 2018).

[7] Controlled Supply, Bitcoin Wiki, <https://en.bitcoin.it/wiki/Controlled_supply> (last visited Sept. 24, 2018); JP Buntinx, *80% of All Bitcoins Will Have Been Mined In a Year From Now*, NullTX, <https://nulltx.com/80-of-all-bitcoins-will-have-been-mined-in-a-year-from-now> (last visited Sept. 24, 2018); *see also* CoinMarketCap, <https://coinmarketcap.com/> (last visited August 14, 2019).

[8] Will Martin, *Venezuela's Inflation Rate Just Hit 830,000% — and is likely to keep rising*, Business Insider, <https://www.businessinsider.com/venezuela-inflation-rate-hyperinflation-2018-11> (last visited January 17, 2019).

[9] Noah Smith, *Venezuela is Living a Hyperinflation Nightmare*, Bloomberg, <https://www.bloomberg.com/view/articles/2017-12-19/venezuela-is-living-a-hyperinflation-nightmare> (last visited Sept. 24, 2018).

[10] Hamza Shaban, *The Highs and Lows of the Wild Year of Bitcoin*, The Washington Post, <https://www.washingtonpost.com/news/the-switch/wp/2017/12/29/a-look-at-the-year-of-bitcoin/?utm_term=.c7b7ee822499> (last visited Sept. 24, 2018); David Meyer, *Cryptocurrency Traders Lose $115 Billion in 24 Hours as Bitcoin Bloodbath Continues*, Fortune, <http://fortune.com/2018/02/02/bitcoin-crash-8000-ethereum-ripple> (last visited Sept. 24, 2018); Bitcoin (USD) Price, CoinMarketCap, <https://coinmarketcap.com/currencies/bitcoin> (last visited June 10, 2019).

Our Team

Corporate

Mark S. Bergman
+44-20-7367-1601
mbergman@paulweiss.com

Manuel S. Frey
212-373-3127
mfrey@paulweiss.com

David S. Huntington
212-373-3124
dhuntington@paulweiss.com

Raphael M. Russo
212-373-3309
rrusso@paulweiss.com

Jonathan H. Ashtor
212-373-3823
jashtor@paulweiss.com

Litigation

Susanna M. Buergel
212-373-3553
sbuergel@paulweiss.com

Jessica S. Carey
212-373-3566
jcarey@paulweiss.com

Roberto Finzi
212-373-3311
rfinzi@paulweiss.com

Christopher D. Frey
+81-3-3597-6309
cfrey@paulweiss.com

Roberto J. Gonzalez
202-223-7316
rgonzalez@paulweiss.com

Jeannie S. Rhee
202-223-7466
jrhee@paulweiss.com

Richard C. Tarlowe
212-373-3035
rtarlowe@paulweiss.com

Karen R. King
212-373-3784
kking@paulweiss.com

Associates Jacobus J. Schutte, Anastasia V. Peterson, Marisa Seiss, Andrew J. Heffler, Deniz Gurbuz, Patrick R. Kessock and Apeksha S. Vora contributed to this white paper.

PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP

www.paulweiss.com