



# Cryptocurrency Primer

Fall 2018

**OBERON  
SECURITIES**

Disclaimer: Oberon Securities, LLC is a registered broker-dealer and member of FINRA and SIPC. The information provided in this report is for informational purposes only and is not intended to be, nor should it be considered to be, an advertisement or an offer or a solicitation of an offer to buy or sell any securities. The information herein, or upon which opinions have been based, has been obtained from sources believed to be reliable, but no representations, expressed or implied, or guarantees, can be made as to their accuracy, timeliness or completeness. All opinions and information set forth herein are subject to change without notice.

---

## Table of Contents

Do You Really Understand Cryptocurrencies: The Basics!.....	1
Cryptocurrency Overview .....	1
Digital Currency in a Secure Wrapper, Comes with Its Own Tracking System .....	2
Blockchain Summarized .....	3
Breaking Down Cryptocurrency Protocol .....	3
What is a Blockchain? .....	3
What is a Consensus Mechanism? .....	4
Smart Contracts: Addition to Blockchain Technology .....	5
Smart Contracts Applied: Decentralized Applications (DApps).....	5
Case Study: The DAO.....	5
History.....	7
Satoshi Nakamoto, the Legend .....	7
The Deluge: A Myriad of Cryptocurrencies Hit the Market .....	7
Cryptocurrencies Differentiated .....	8
Making the System Work: Mining and Nodes .....	8
Cryptography: the Essential Ingredient for Securing Coins and Tokens .....	10
Private Keys and Public Keys.....	10
Security .....	10
Wallets and Storing Cryptocurrencies .....	11
Major Players.....	12
Major Cryptocurrencies .....	12
Cryptocurrency Exchanges.....	15
Differentiating Factors in the Industry .....	17
What are the Pros and Cons of Each of These Companies/Coins? .....	17
Liquidity and Volatility in the Market.....	21
Liquidity.....	21
Volatility.....	21
Understanding Cryptocurrency Volatility .....	21
Approaching Valuation .....	24
Absolute Valuation .....	24
Relative Valuation.....	24
Cryptocurrency-to-Commodity Modeling.....	25

## Cryptocurrencies Primer

---

Fiat Modeling, ForEx Valuation .....	25
Marginal Cost Valuation .....	26
Cryptocurrency Performance Valuation.....	26
Token Valuation.....	27
Valuation Conclusion .....	27
Financing.....	28
Venture Capital Funds and Major Institutional Investors .....	28
ICOs and STOs an Alternative Sources of Financing.....	30
Regulatory Environment .....	31
Governmental Regulation.....	31
Current Regulatory Landscape .....	31
SEC Taking Cryptocurrency Seriously .....	32
Future Action.....	32
Appendix A: Cryptocurrency Exchanges.....	34
Appendix B: Top Cryptocurrencies by Market Cap .....	35
Appendix C: Top Coins by Market Cap .....	39
Appendix D: Top Tokens by Market Cap .....	43

# Do You Really Understand Cryptocurrencies: The Basics!

## Cryptocurrency Overview

Cryptocurrencies refer to a class of virtual/digital currencies that use coins or tokens (think “virtual money”) to facilitate the exchange of value for goods and services. As cryptocurrencies have evolved, taxonomy and nomenclature has evolved with it. Originally, cryptocurrencies referred solely to digital currency, like Bitcoin. Today, blockchain and tokenization-related technologies, which serve as the underpinnings of asset-backed or service-backed “tokens,” are also included within this definition. “Cryptocurrency” is an umbrella term for all “coins” and “tokens” regardless of their applications.

There are 3 different classifications: coins, utility tokens, and tokenized securities (some cryptocurrency experts use different classification systems):

### *I) Coins*

Coins are designed to be used as a medium of exchange (of value); popular examples include Bitcoin or Litecoin. Similar to fiat currency, these coins are not backed by commodities like gold; unlike fiat currency, they are not generally backed by government. Coins are essentially digital cash that can be exchanged peer-to-peer (P2P), with a unique set of properties enabling secure transactions (allegedly preventing fraud and counterfeiting) and making the exchange irreversible.

### *II) Utility Tokens*

Utility tokens refer to cryptocurrencies, sold in “initial coin offerings” (ICOs), which are created and accepted as payment for specific services. Essentially, consumers seeking to use an application’s service would buy the issued tokens to gain access to the service. FileCoin, a utility token, is a primary example; it enables individuals who purchase them to have a right to use cloud storage space offered by the entity. Intuitively, the token’s value is attached to the company’s service(s) offering. The more in demand the application’s service, the higher prices customers would be willing to pay for the token.

### *III) Tokenized Securities*






Tokenized securities refer to cryptocurrencies sold in a “standardized token offering” (STO) that act as equity in a company. They streamline equity offerings by eliminating

middlemen in the process. This system implements traditional cryptocurrency features that provide traceable certification for transactions. In addition, automation for certain corporate governance practices like voting or dividend payout policies may be introduced. Although tokenized securities are not as popular as their siblings due to regulatory concerns, organizations are pushing to popularize these tokenized securities.

### Digital Currency in a Secure Wrapper, Comes with Its Own Tracking System

Cryptography is one of the key technological drivers paving the way for the potential widespread adoption of cryptocurrencies. Cryptography, a branch of mathematics focused upon the protection of digital information, is used to make the currency secure. Blockchain, also enveloped by encryption, is a record-keeping system that tracks cryptocurrency transactions and is specifically designed to try to eliminate counterfeiting and fraud, although cryptocurrencies still have certain security weaknesses detailed later.

Exhibit 1: Cryptocurrency Taxonomy

Coins	Utility Tokens	Securitized Tokens
Cryptocurrencies designed to be used as a medium of exchange	Cryptocurrencies designed to be used for a service	Cryptocurrencies designed to represent an asset or future cash flows
<p>Examples</p>  Bitcoin  Cardano  Litecoin  Ripple	<p>Examples</p>  OmiseGO  Siacoin  Steem  Tron	<p>Examples</p>  Science Blockchain  Blockchain Capital

Source: Oberon Securities

# Blockchain Summarized

## Breaking Down Cryptocurrency Protocol

Cryptocurrencies rely on an underlying technology called “blockchain” to operate. Blockchain can be broken down into two parts: the blockchain itself and the consensus mechanism.

## What is a Blockchain?

A “blockchain” is a decentralized list of transaction records, referred to as “blocks.” A blockchain is essentially a digital ledger or database of information in which people share access and the responsibility of maintaining and auditing the ledger. The data in the ledger is audited using a “consensus mechanism,” a type of auditing technique. The consensus mechanism uses “hash functions,” a series of mathematical transformations, to ensure the existing records and incoming transactions are correct.

Blockchain is revolutionary because of how it records and maintains information. The ledger does not exist in a single computer; rather, it is “mirrored” or recorded across a network of computers. This decentralization of records has important security and economic implications.

Since there is no single authority that controls cryptocurrency, there is no need for central banking involvement of any kind. This means the supply of currency cannot be altered on a discretionary basis, which would otherwise result in unexpected inflation or interest rate changes. Since the ledger is distributed across a wide network, like the World Wide Web, it would be very difficult to corrupt or destroy. Modifying previous records on the blockchain is almost impossible because of the computational power and speed needed to complete the task, particularly because information in the blockchain is processed using a set of calculations that generate a unique identification number. If an individual were to make a small change to the previous records in the blockchain, the resulting signature would be different, and users responsible for maintaining the blockchain would identify and reject the modified blockchain.

Given that the transactions on the blockchain are public and decentralized, consumers and users do not need to “trust” a central authority. Unlike a traditional payment system, cryptocurrency users do not need to rely on a bank or payment system to verify

their transactions. As a result, users do not need to register with a financial institution or give their personal information to use cryptocurrencies (although this changes if a user wants to register for a cryptocurrency exchange).

### **What is a Consensus Mechanism?**

A consensus mechanism is a validation protocol, responsible for validating new information added to the blockchain and ensuring that the distributed blockchain ledgers match.

In a blockchain, the consensus mechanism is the most important factor that determines security and economic incentives. There are different consensus mechanisms that are used to verify information in a blockchain in different ways, and as a result have very different purposes.

Two examples of consensus mechanisms are proof-of-work and proof-of-stake.

#### ***Proof-of-work (POW) method***

Proof-of-work involves using computing resources like a computer or mining rig (a highly specialized hardware setup designed to mine cryptocurrencies) to try to solve a computationally intense problem to add a transaction to the blockchain. Individuals with more computational power are more likely to solve the problem first, verify the transaction, and collect a reward in cryptocurrency. The system will automatically trust the block with the most computational work in it.

#### ***Proof-of-stake (POS) method***

The proof-of-stake algorithm is a new consensus algorithm proposed for Ethereum in response to how computationally and energy intensive the proof-of-work algorithm is. Rather than using computational resources to compete for the right to verify transactions, proof-of-stake proposes a lottery system based off the user's cryptocurrency. Users send their cryptocurrency into a pool, or their "stake," where their stake is proportional to their chances of validating the next block and earning the reward. If a user validates a fault block, the user is punished by losing a proportion of the cryptocurrencies they put as a "stake." Although this method has not been implemented yet, the POS method provides a less power-hungry alternative to POW. It is important to note that this consensus algorithm is still developing, and has not been fully proven to work yet.



## Smart Contracts: Addition to Blockchain Technology

In 2015, the Ethereum platform was released adding scripting functionality to blockchain technology. Although it is most commonly associated with its cryptocurrency (Ether), Ethereum is essentially a computing platform that allows additional scripting functionality in the form of “smart contracts.”

Smart contracts are actually bits of code that allow users to execute commands automatically on the Ethereum network. Furthermore, smart contracts are recorded on the blockchain, making smart contract tampering virtually impossible, meaning that they can run automatically (there can still be user error in creating smart contracts). If cryptocurrencies were like the stock market, Ethereum allows one to create financial derivatives of the underlying cryptocurrency.

The concept of a vending machine shares similar properties to smart contracts on blockchain, in that it has hard-coded rules that define what will happen when certain conditions are met and then executes those actions when the conditions are fulfilled. There is no alternative. If Larry puts a dollar in the vending machine, he will receive his soda. Now imagine a vending machine that not only takes money and returns a snack, but also uses that money to reorder the products that need to be replenished automatically. It also can order cleaning services and pay its rent. There is no manager; all of these processes were already coded.

## Smart Contracts Applied: Decentralized Applications (DApps)

A “Decentralized Application” (or DApp) is an application that runs on a decentralized peer-to-peer network like Ethereum or EOS. Traditional applications consist of a front end, consumer interface, and a back end that is responsible for running the software hosted on a server. The DApp is unique because it hosts its back end on a blockchain.

Like any blockchain related product, DApps require computing resources from its users to operate. DApps provide an incentive for users to be a volunteer by generating tokens. These tokens are used to grant access to a DApp, and these DApps are partially responsible for the explosion of tokens. Eth-Tweet, twitter for Ethereum, is an example of a DApp.

## Case Study: The DAO

The DAO was a digital decentralized autonomous organization and a form of investor-directed venture capital fund, founded in May 2016 by members of the Ethereum community. Decentralized autonomous organizations (DAOs) are entities that operate

exclusively through smart contracts. The DAO was intended to operate like a VC fund for the crypto and decentralized space. It hoped to provide a new decentralized business model for organizing commercial and non-profit enterprises. This lack of a centralized authority would, in theory, reduce costs and provide more control and access to investors. Essentially, anyone with a project idea would be able to pitch the idea to the community and potentially receive funding from the DAO.

Represented on the Bitcoin-inspired platform of Ethereum, the DAO did not have a typical management structure or board of directors. As it pertains to the area in which the DAO served, it was stateless. This quickly became an issue as government regulators were not sure of how they would control and monitor a stateless fund. Further, the DAO was crowdfunded, meaning that it was founded by raising small amounts of money from a large number of people, via a token sale in the spring of 2016. In fact, it turned out to be the biggest crowdfund ever.

The DAO had a creation period where anyone was allowed to send Ether, the currency of Ethereum, to a special wallet addressed in exchange for DAO tokens. The DAO raised an equivalent of \$150 million at the time. The DAO was built as a complex smart contract on the Ethereum blockchain. The smart contract was programmed with several rules and features that allowed companies to make proposals for funding. Once a proposal was whitelisted by a curator, the DAO investors would then need to vote on the proposal. If the proposal got a 20% consensus, the requested funds would be released into the contractor's wallet address.

Unfortunately, in June 2016, users took advantage of a major vulnerability in the DAO code that allowed them to drain funds from the DAO. In the first few hours alone, 2.6 million Ethereum were stolen, the equivalent of \$70 million dollars. The attacker was able to "ask" the smart contract to give Ether back numerous times before the smart contract updated its balance. It should not be a surprise that this attack led to the beginning of the end for the DAO. This security vulnerability was actually discovered a month in advance, but a solution was not found and implemented in time. Eventually, it was delisted from trading on major exchanges such as Poloniex and Kraken, and the DAO closed in the latter part of 2016.

Despite the revolutionary potential of these new technologies, it is important to realize that they are still being tested and could have flaws.

# History

## Satoshi Nakamoto, the Legend

In 2008, Satoshi Nakamoto, a pseudonym for an anonymous technologist, introduced a white paper describing Bitcoin: “a purely peer-to-peer electronic cash system.” Nakamoto outlines his idea for the creation of a new electronic payment system designed to replace traditional (analog) currency and fix specific faults with the current financial system. According to Nakamoto, third-party financial institutions left users (specifically vendors) very vulnerable to fraud in the established electronic systems. Essentially, his innovation purported to wipe out the need for some of the commercial money centers, banks and credit card services.

Nakamoto’s proposed technology innovation would use cryptography and economic incentives to eliminate the need for a trusted central authority, essentially creating an open, peer-to-peer exchange of digital money. In this environment, users could trust the system because the transactions were guaranteed, and once created, irreversible. The blockchain system would keep redundant virtual records regarding all transactions, thereby eliminating the need for interference or mediation.

The first Bitcoin block (the “genesis block”) was mined on January 3, 2009, and the first Bitcoin transaction took place on January 12. The following year would be a proof-of-concept phase for the pioneering cryptocurrency. With more people learning about blockchain technology and the potential of cryptocurrencies, Bitcoin surged in popularity.

## The Deluge: A Myriad of Cryptocurrencies Hit the Market

Beginning in 2011, other cryptocurrencies rushed into the market. These alternative coins (“altcoins”) were proposed as improvements to Bitcoin. Litecoin, one of the first alternative coins issued to compete with Bitcoin, uses nearly identical protocols to Bitcoin but alleges faster processing times for transactions. Zcash, another entrant, offered “better” user security. Aside from this deluge of new coins, cryptocurrency companies launched a plethora of tokens using the blockchain infrastructure. Tokens are backed by services or assets. Tokens like Filecoin and Ripple were designed to function like vouchers which could be exchanged for specific services. Currently, there are more than a thousand cryptocurrencies with the number growing yearly.

# Cryptocurrencies Differentiated

Cryptocurrencies have three features that differentiate them from traditional monetary currencies: they are trustless, decentralized, and immutable (although there are many cryptocurrencies that make changes to these features). Operating in a P2P environment, cryptocurrencies do not rely on financial institutions to verify the identity of the individuals or the particulars of a transaction, unlike the traditional banking system. Transactions are completed through the network supporting the cryptocurrency, rather than a central organization.

## ***I) Trustless***

Data posted on a blockchain—a digital, public ledger—is visible to everyone and must be approved by the network via a protocol established among users. Therefore, there is no need for a bank or trusted third party to mediate transactions; the technology platform (“network”) is designed to do it. This theoretically prevents issues such as double spending from occurring because the users would not approve transactions involving cryptocurrencies a user could not spend. Further, with smart contracts a cryptocurrency is set up in such a way where neither party involved in a transaction needs to trust one another in order to execute payments for goods.

## ***II) Decentralized***

Cryptocurrencies, as opposed to fiat currencies, are not controlled by any single authority and are thus decentralized. Traditional currencies, such as the U.S. Dollar, are backed by the governments that issue them and exert influence over the supply and value of the currency through mints and interest rates. Since cryptocurrencies are not currently issued or overseen by governments, decisions made about the currency must be formulated by a direct consensus made by all holders of the currency on the network.

## ***III) Immutable***

When a transaction is consummated, it is automatically recorded in the digital (virtual) ledger and allegedly can never be changed once it is verified. Each transaction on a blockchain is posted to the public ledger.

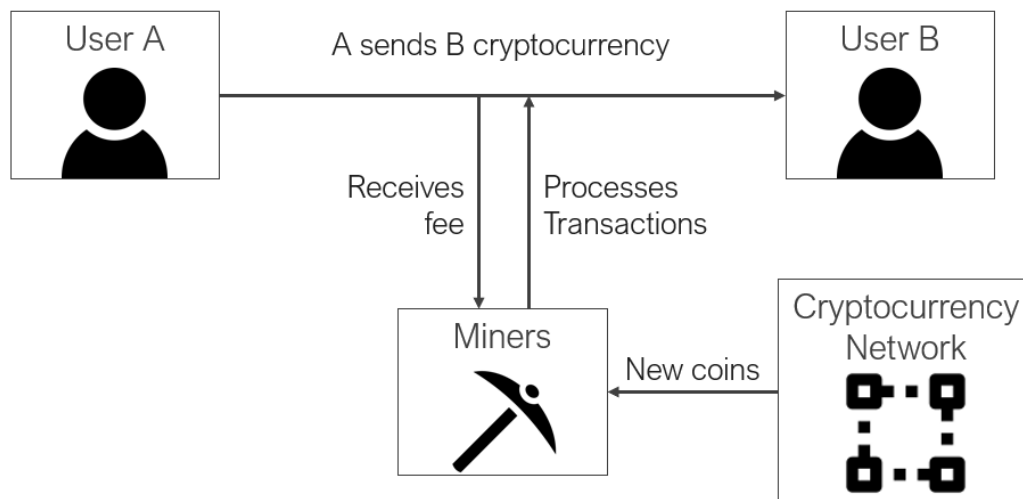
## **Making the System Work: Mining and Nodes**

Most cryptocurrency ecosystems (including Bitcoin) are supported by “Miners” and “Nodes.” Miners are individuals who maintain the network, verifying and processing

new transactions by contributing computer processing power. Nodes are units that record transaction history. Cryptocurrencies require immense amounts of computer processing power and energy. Consequently, there are people and entities that are dedicated to making sure that every transaction meets a certain standard and that the network is operating properly. When a transaction is signaled, it will be confirmed by multiple nodes and miners and then added to the public ledger, essentially verifying the validity of transactions before consummation.

In exchange for maintaining the network, these individuals are compensated in two ways: new Bitcoin (BTC) (hence “mining” cryptocurrencies) or transaction fees. These rewards are meant to attract and incentivize miners to verify transactions for the network. It is important to note that transaction fees are optional and are meant to incentivize productivity. Bitcoin, by design, has a finite amount of coins that can be mined: 21 million coins. The creator felt that limiting supply was essential to Bitcoin’s value. As of this writing, approximately 17 million BTC have been mined.

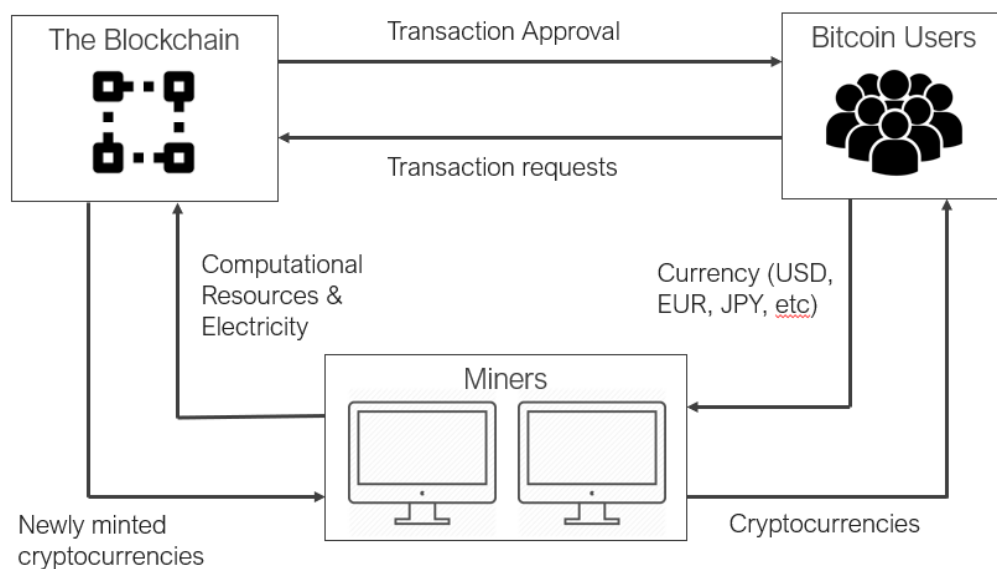
**Exhibit 2: A Diagram of Mining Activity**



*Source: Oberon Securities*

When the mining cap for BTC is reached, miners will be incentivized to maintain the network by exclusively taking a transaction fee instead of receiving newly minted coins. It is important to know that each type of cryptocurrency works differently, but many cryptocurrencies use similar mechanisms to incentivize individuals to maintain the network.

Exhibit 3: Cryptocurrency Ecosystems



Source: Oberon Securities

## Cryptography: the Essential Ingredient for Securing Coins and Tokens

Cryptocurrencies exist because cryptography has become sophisticated enough to support and protect it.

### Private Keys and Public Keys

Cryptocurrency transactions are powered by public-key cryptography—essentially a pair of numbers representing a “private key” and a “public key.” A private key (a “virtual key” issued only to an account holder for a specific amount) is essentially a unique password for an account. The key is a number between 1 and 78 digits long and it is the only way to access cryptocurrencies held in the account. If an individual loses his or her private key, there is no way to regain access to the holdings in their account. A public key is similar to a routing number; it is available for everyone to see so that they can send money to the address. However, a public key does not permit access to withdraw money from an account, it only allows for deposits.

### Security

Transactions made via traditional methods (e.g. visa payments) are increasingly susceptible to fraud, especially identity theft. Using someone else’s credentials or credit card information, people can make fraudulent charges to the account and steal their money. Cryptocurrencies reduce this problem by relying on public and private key architecture to make and verify transactions from the associated parties. Private keys

should not be revealed to the public under any circumstances. Restricting access to private keys prevents security breaches.

Furthermore, the network of nodes (or copies of transaction histories) provides a layer of security to the blockchain network through redundancy. A hacker targeting a traditional banking system can gain access to the entire system by hacking the bank – all parts of the banking process are funneled through this central authority. However, with Bitcoin or any blockchain-based system, information and control are separated across the network of nodes. Therefore, it is exceedingly challenging for an attacker to hack the system and commit a fraudulent transaction unless they control more than 50% of all the nodes, which is virtually impossible because the energy and computing resources needed to complete an attack is prohibitively expensive.

Cryptocurrencies have far better security against hackers, but it is not foolproof. If an individual were to obtain someone else's private key – essentially accessing their password – this individual would have access to all of the user's cryptocurrency. This can be accomplished by phishing, where a scammer tricks an individual into disclosing their private key information. In this case, cryptocurrencies' immutability also makes them dangerous. Since transactions are immutable, if the scammer is successful and transfers money out of the account, there is no possibility for retrieval. Hence, aspects of this technology and security are still a work in progress.

## **Wallets and Storing Cryptocurrencies**

Cryptocurrencies are stored in a "wallet." Cryptocurrency wallets do not actually store money. Rather, they protect the private and public keys of the user. There are two types of wallets: hot and cold.

### ***Hot Wallet***

Hot wallets are connected to the internet. As a result, it is more convenient if an individual trades frequently. On the other hand, the internet connection presents some security risks. By being connected to the internet, these wallets are vulnerable to being hacked or infiltrated by malicious parties.

### ***Cold Wallet***

Cold wallets are not connected to the internet. These wallets can be cumbersome to use frequently, but are safer because they are difficult to attack. A cold wallet can come in many forms: a USB stick, specialized hardware, or a piece of paper. This is as simple as it seems; the person just needs to record their key pair.

## Major Players

### Major Cryptocurrencies

As of August 2018, the total cryptocurrency market capitalization is over \$268 billion. Coin Market Capitalization refers to the total market value of a specific cryptocurrency. Similar to market cap for public equities, the calculation is price times the units of currency circulating. Although there are similarities between cryptocurrencies and regular currencies, a cryptocurrency will often have specific goals in addition to being a widely accepted medium of exchange and a store of value. The top 5 cryptocurrencies by Market Capitalization can be found below.

#### ***Bitcoin (BTC)***

##### **Coin Market Cap: \$111 Billion**

Bitcoin was originally launched in 2009. Although Bitcoin was not the first attempt at creating digital currency (there have been previous attempts like Digicash, E-Gold, and early PayPal), it was the one that brought virtual currencies into the public eye and completely changed the way people think about digital money.

The popularity of Bitcoin has helped its adoption among companies and users. Several merchants and businesses have adopted Bitcoin as a form of payment including numerous well-known companies such as: Overstock.com, eGifter, Khan Academy, Microsoft, Dish Network, and more. At the government level, countries such as the United States, Canada, and Japan have all declared Bitcoin legal, while Iceland, Vietnam, and Russia are still working through regulatory issues. Bitcoin introduced the idea of a public ledger to properly document every transaction. In essence, value is transferred between Bitcoin wallets, which are concurrently in the blockchain. Bitcoin wallets keep the secret private key or seed, which is used to sign transactions, providing proof of origins and ownership. The signature also prevents the transaction from being altered by anybody once it has been issued.

At the time of writing, Bitcoin is by far the most widely accepted cryptocurrency in the market. Aside from online merchants and retailers, several service providers have accepted Bitcoin as a fiat currency. Fiat currency is currency that the government declared to be legal tender despite not being backed by a physical commodity. Today Bitcoin can be used to purchase a plethora of products and services including, but not limited to electronics, software and gear (i.e. Microsoft, Newegg, and Dell), flights, and



travel amenities (Expedia). Lastly, in 2016, a Bitcoin.com online casino launched. The site is completely anonymous and lets users gamble with Bitcoin.

There are several pitfalls to Bitcoin. Most people have heard of Bitcoin and related concepts such as “blockchain” or “ledger” but they do not really understand how Bitcoin works, making it ripe for fraud. Second, there is volatility associated with Bitcoin in particular and cryptocurrency in general. Volatility is driven by the limited amount of coins in existence. It is expected that volatility will decrease as time goes on. Lastly, it is important to keep in mind that Bitcoin is still in its infancy and needs to go through the same development and stumbling blocks that any new technology or industry undergoes in its evolution.

### ***Ethereum (ETH)***

#### **Coin Market Cap: \$30 Billion**

Ethereum is the second largest cryptocurrency, created by Vitalik Buterin, a Russian-Canadian programmer who was dissatisfied with the functionality of Bitcoin. Bitcoin was initially created with the sole purpose of creating value, and no one foresaw it evolving into its current state. As the industry faces continuous growth, more and more demand is placed on existing codebases until they can no longer handle the demand. Buterin felt it was easier to start from scratch. Ethereum is an entire ecosystem that can adapt to ever-changing needs.

Launched in 2015, Ethereum is a decentralized software platform enabling smart contracts and Distributed Applications (DApps) to be built and to run without any downtime, fraud, control, or interference from a third party. In addition, it is the basis for its own virtual currency, Ether. While the Bitcoin blockchain tracks the ownership of digital currency, the Ethereum blockchain focuses on running the programming code of any decentralized application. Put another way, Ethereum is a ledger technology that companies use to build new programs. Ethereum allows for the building of decentralized applications on top of it, making it great for innovation. Finally, instead of mining for coins like in Bitcoin, miners work to earn Ether, a crypto token that fuels the network.

### ***Ripple (XRP)***

#### **Coin Market Cap: \$12 Billion**

Launched in 2012, Ripple has established itself as one of the world’s most prominent cryptocurrencies. Ripple’s goal is to offer fast, reliable, and affordable cross-border payments. Ripple is a San Francisco-based technology company that is developing a

global settlement network for cryptocurrency transactions designed to ensure more efficient communication between financial institutions. It allows users to exchange money from one currency to another in seconds. Ultimately, this service could eliminate the need for money transfer systems like Western Union or SWIFT. Effectively, Ripple acts as a conduit between the two transferred currencies. Ripple does not require mining; instead there is an existing supply of 100 billion XRP which is held and distributed by the company. Several online sellers in the dining and grocery, health and beauty, and tobacco industries, among others, accept Ripple. These businesses include, but are not limited to, PexPeppers, HempUSA, and Azarius.

Ripple has several advantages over other cryptocurrencies. Transactions take less than 4 seconds and cost a fraction of a penny. Ripple has partnered with several of the world's largest banks and high profile institutions such as Google Ventures. The pitfalls are that it is more centralized than other cryptoassets. Ripple owns 60% of all XRP which gives them leverage to manipulate the market. Further, after a transaction is complete, an XRP is burned, reducing supply over time (hardly an issue now since there are 100 billion) unless it is somehow replenished. Lastly, since XRP was pre-mined, each co-founder awarded themselves 20 billion XRP each; many believe this to have been unfair.

### ***Bitcoin Cash (BCH)***

**Coin Market Cap: \$9 Billion**

Bitcoin Cash has quickly become one of the most valuable cryptocurrencies in the world. In August 2017, it split off from the Bitcoin network to improve transaction efficiencies. When Bitcoin initially took off, the network struggled to keep up with transaction volumes. Consequently, users would have to wait hours or days to see their transactions processed. Some Bitcoin miners wanted to increase the block size on the Bitcoin exchange, but they did not receive much support. So, they broke away (“hard-forked”) from the original blockchain infrastructure and created Bitcoin Cash as a new currency. Many cryptocurrency exchanges have already integrated Bitcoin Cash. It is not accepted by vendors who do not accept Bitcoin.

### ***EOS (EOS)***

**Coin Market Cap: \$4 Billion**

EOS is a second generation blockchain for the development of industrial-scale decentralized applications (DApps). The two main features of this new technology are the removal of transaction fees, and scalability (ability to conduct millions of transactions per second). Essentially, DApps are digital applications that exist and run

on a blockchain or P2P network and they are outside the purview and control of a single authority. For cryptocurrencies, the DApps exist and run on a blockchain network in a public, open-sourced, and decentralized environment free from control by any single party or authority.

EOS is being built to create the world's most robust infrastructure for DApps. The EOS system is comprised of two key elements: EOS.IO and EOS tokens. EOS.IO is similar to the operating system of a computer; it manages and controls the EOS blockchain network. The EOS tokens are the cryptocurrency of the EOS network. A developer that simply holds EOS tokens will have access to the system and may build and run DApps. A voting system enables EOS token holders to determine if an application is accepted or not.

## **Cryptocurrency Exchanges**

Cryptocurrency exchanges play a crucial role by giving consumers easy-to-access points to trade cryptocurrencies. Cryptocurrency exchanges are similar to stock exchanges; exchanges provide a marketplace for trading cryptocurrencies, and they profit by charging additional fees on transactions that take place on their platforms.

There are numerous exchanges, and they each define themselves differently. For example, geography is a factor. Due to regulation, exchanges like Coincheck and Korbit are exclusive to Asia. Furthermore, exchanges also carve out niches by trading specific cryptocurrencies that are not traded on mainstream exchanges like Binance, Coinbase, or Kraken. Exchanges employ different rates, fee structures, professional integration, trading, and short-selling. Below are some of the largest cryptocurrency exchanges internationally.

### ***Coinbase***

Coinbase is one of the largest cryptocurrency exchanges in the world, serving 33 countries. Founded by Brian Armstrong and Fred Ehrsam in 2012, it was first launched as a digital wallet for users to store Bitcoin. Eventually Coinbase expanded its services, launching a brokerage service and the first licensed Bitcoin exchange: GDAX. Currently, Coinbase offers a platform for Bitcoin, Ethereum, Litecoin, and Bitcoin Cash.

In addition to being an exchange, Coinbase provides a mobile wallet and web wallet application. By having a wallet designed to work with a specialized exchange, Coinbase users can conveniently transfer Bitcoins between platforms at no additional cost to the

user. Coinbase is an exchange, but often operates as both broker and wallet manager, and caters to retail and non-technical clients who want to work with cryptocurrency.

### ***Gemini***

Gemini was launched by the Winklevoss brothers in 2014. Gemini currently operates in the United States, Canada, United Kingdom, Hong Kong, South Korea, and Singapore. The exchange was the first licensed Ethereum and Zcash exchange in the U.S. and exclusively trades those cryptocurrencies. In addition to traditional features, Gemini offers “block trading.” Block trading is an order book facility that allows large trades of digital currencies outside of Gemini’s traditional order books, providing users with additional liquidity opportunities.



### ***Kraken***




Founded in 2011, Kraken was an earlier competitor to Coinbase. However, the platform supports seventeen different cryptocurrencies, including Bitcoin, Litecoin, Ethereum and more. Kraken is well entrenched in the crypto finance community, offering Bitcoin pricing on Bloomberg.




## Differentiating Factors in the Industry



Cryptocurrencies have several dimensions for differentiation due to their complex nature. It would be almost impossible to directly compare cryptocurrencies because they can vary drastically.

### What are the Pros and Cons of Each of These Companies/Coins?

Coin	Pros	Cons
<b>Bitcoin</b> 	<ul style="list-style-type: none"> <li>• Bitcoin is the most popular and accepted cryptocurrency making it very liquid</li> <li>• Low transaction fees, usually less than 1% of the transaction</li> <li>• Bitcoin allows users to separate accounts from public personas allowing for privacy and security not seen with credit cards, PayPal, etc.</li> <li>• Bitcoin is decentralized, which means it is not affected by political influence of its creators unlike other cryptocurrencies</li> </ul>	<ul style="list-style-type: none"> <li>• Due to its history of price fluctuation, Bitcoin attracts speculators that make it susceptible to high price volatility</li> <li>• Because of the large mass of inexperienced users, it is more prone to scams, fraud and attacks more than other currencies</li> <li>• Bitcoin's volatility makes it a risky long term investment and difficult to use in normal transactions</li> <li>• Bitcoin mining is highly energy-inefficient compared to other transaction systems</li> </ul>
<b>Ethereum</b> 	<ul style="list-style-type: none"> <li>• Ethereum has more far more functionality than Bitcoin due to smart contracts</li> <li>• Smart contracts allow endless possibilities for automated and conditional transactions - increasing the value of Ethereum</li> <li>• Large interest and support from the community</li> <li>• Ethereum is a platform and an ecosystem and can have value-added applications on top of the currency</li> <li>• Many projects and existing tokens use Ethereum, and thus it is widely used and may be around for a while</li> </ul>	<ul style="list-style-type: none"> <li>• Development issues have led to a slow and congested network</li> <li>• Ethereum is designed to be flexible and is seen as less efficient than other blockchains</li> <li>• Ethereum must support the applications built on the platform, which slows down the network</li> <li>• A recent hack caused the Ethereum community to vote to break its immutability rule and reverse the hack</li> </ul>

Coin	Pros	Cons
<p>XRP</p> 	<ul style="list-style-type: none"> <li>• Ripple (XRP) was specifically designed for financial institutions</li> <li>• XRP has extremely fast transaction settlement times and runs efficiently</li> <li>• Unlike Ethereum, XRP does not face scalability issues, meaning global adoption is up to users</li> <li>• XRP can process 1500 transactions per second compared to the 2-4 of Bitcoin and 15-25 of Ethereum</li> <li>• XRP has a considerable number of partnerships with other companies</li> <li>• XRP is very affordable compared to other currencies</li> </ul>	<ul style="list-style-type: none"> <li>• XRP is not mined and the company that developed XRP controls approximately 60% of existing XRP coins</li> <li>• Many mainstream banks have not adopted XRP</li> <li>• XRP competes with cryptocurrencies with similar features but high-profile partnerships (Stellar)</li> <li>• Regulatory concerns could hamper partnerships and investors</li> </ul>
<p>Bitcoin Cash</p> 	<ul style="list-style-type: none"> <li>• Being a slightly modified copy of Bitcoin, Bitcoin Cash shares the same features as Bitcoin</li> <li>• Bitcoin Cash has modified its transaction capabilities to be able to handle 60 transactions per second</li> <li>• Even lower transaction fees compared to Bitcoin</li> </ul>	<ul style="list-style-type: none"> <li>• Being one of several Bitcoin copies, Bitcoin Cash suffers from lack of acceptance</li> <li>• Even though Bitcoin Cash can handle transaction traffic well, due to a lack of popularity it only faces 0.11 transactions per second</li> </ul>
<p>EOS</p> 	<ul style="list-style-type: none"> <li>• EOS is an experimental cryptocurrency that can handle millions of transactions per second</li> <li>• It offers smart contract features like Ethereum</li> <li>• EOS leverages parallel computation used in image rendering and artificial intelligence to accelerate transaction processing</li> </ul>	<ul style="list-style-type: none"> <li>• EOS is still under development making the future of EOS unclear</li> </ul>

Coin	Pros	Cons
<p><b>Litecoin</b></p> 	<ul style="list-style-type: none"> <li>• Litecoin is an alt-coin that has been around since 2011</li> <li>• Easy mining using new Scrypt algorithm</li> <li>• Fast confirmation times: 2.5 seconds to complete operation versus Bitcoin's 10 minutes</li> <li>• Its send-receive feature is one of the fastest compared to other cryptocurrencies (the block completion time is probably the fastest)</li> <li>• One of the earliest to use SegWit/anti-spam filter in order to limit the blockchain size</li> <li>• Very cheap, cheaper than Bitcoin, (has an almost 0% transaction fee)</li> <li>• Less volatile during market crash</li> <li>• Excellent leadership team (good future prospects)</li> <li>• Supported by all hardware wallets</li> </ul>	<ul style="list-style-type: none"> <li>• Decreased block time comes with increased security risks</li> <li>• More vulnerable to a 51% attack</li> <li>• If Bitcoin upgrades its transaction speed and scalability, Litecoin will lose its edge in the market</li> <li>• Not as well known as other cryptocurrencies specifically Bitcoin</li> <li>• Uses a memory-intensive function in its proof-of-work algorithm which makes Litecoin mining harder than Bitcoin</li> </ul>
<p><b>Stellar</b></p> 	<ul style="list-style-type: none"> <li>• Partnered with IBM</li> <li>• Faster transaction speed and lower fees than Bitcoin</li> <li>• Meant to be an enhanced version of Ripple</li> <li>• Quick transactions</li> <li>• The currency is seen in different exchanges such as Kraken and Binance</li> <li>• Trader and exchanges oriented</li> </ul>	<ul style="list-style-type: none"> <li>• Not entirely decentralized</li> <li>• It is a long-term hold, not something to day-trade or hold for a month</li> <li>• Not minable; supply depends on the parent company's predictions</li> <li>• Not as much value circulating in the market as Ripple</li> </ul>
<p><b>Cardano</b></p> 	<ul style="list-style-type: none"> <li>• Trying to remove the need for exchanges</li> </ul>	<ul style="list-style-type: none"> <li>• Not a lot of the planned features are currently in place</li> </ul>

Coin	Pros	Cons
<p><b>IOTA</b></p> 	<ul style="list-style-type: none"> <li>• Completely new technology (Tangle) which is different from other blockchains because it does not have blocks, fees, or scalability issues</li> </ul>	<ul style="list-style-type: none"> <li>• No smart contracts yet, which will be hard to implement due to the non-linear nature of the Tangle</li> <li>• New and innovative technology means it is still unproven</li> </ul>
<p><b>Tether</b></p> 	<ul style="list-style-type: none"> <li>• Low to no fees</li> <li>• The price of Tether is fixed against the USD, so it is a convenient “safe haven” to trade</li> </ul>	<ul style="list-style-type: none"> <li>• Audit results are not shared and details on how the liabilities are managed are not present</li> <li>• It is required to get verified, which takes a large number of steps</li> </ul>



# Liquidity and Volatility in the Market

## Liquidity

Liquidity, the ease of trading a security, is important for several reasons. Greater liquidity can lower trading costs and make market pricing more efficient and accurate. It also helps investors to easily exit positions to lock in gains or avoid significant losses in volatile economic cycles.

Although the more established cryptocurrencies like Bitcoin or Ethereum are expected to encounter greater liquidity as adoption increases, lesser known and/or newly issued cryptocurrencies generated by small ICOs or STOs may be highly illiquid, and share many similarities with holding securities in a private company. This may also be compounded by the fact that there may not be enough market makers or speculators to support all the new issuances.

## Volatility

At the beginning of August 2017, Bitcoin pricing was hovering at \$4,000 per coin and had a total market capitalization of \$67 billion. By December 2017, Bitcoin exceeded \$19,000 per coin, driving the coin market capitalization to more than \$319 billion. Today, Bitcoin is hovering around \$7,000 per coin with a \$111 billion market, a prime example of the volatility that is still being exhibited in the cryptocurrency market at this moment in time.

Currently there are conflicting opinions on the future of volatility in cryptocurrency trading. Due to an increasing number of trades across currencies and platforms, coupled with positive government regulation and wider adoption, analysts believe that this will help stabilize the pricing in the long term. It is still important to understand the potential factors that influence cryptocurrency volatility.

## Understanding Cryptocurrency Volatility

Like investing in other securities, risk is important for evaluating a cryptocurrency investment opportunity. Similar to traditional volatility, cryptocurrency volatility is defined as the variation in returns of a given security over a period of time, where more volatility means more risk. Below are some of the common facts that affect the short-term and long-term volatility of cryptocurrencies.

### ***Rate of adoption influenced by historical failures and success***

Early success, the crypto millionaires, and failures, including the bankruptcy of exchanges like Mt. Gox and the South Korean exchange Yopian Youbit, have triggered optimism in some and fear in others; however, many see indications of a market that will mature as governments start to create ground rules for the industry.

### ***Fluctuation of perceived value and store of value***

The prices of cryptocurrencies are sensitive to the fluctuations of other financial systems. Factors like the strength of traditional currencies, money flow in markets, and the responses from the government and banks heavily influence cryptocurrencies. Unlike fiat currencies, coins are not backed by the government and often have a limit on the number of coins available, similar to gold. Bitcoin, for example, has a programmed maximum of 21 million coins used in transactions. The store of value represents the ability of an asset to be stored and later retrieved while incurring a small amount of depreciation. Bitcoin's store of value fluctuates greatly with its price point. These two types of value drive the current spot price of cryptocurrencies.

### ***Limited exit opportunities***

Limited exit opportunities exist for investors with large cryptocurrency positions. For individuals with small positions, it would be possible to liquidate the assets without severely impacting market pricing. Thus, large holders of the currency, such as those with above \$10 million, are faced with limited option value. A large majority of the coins in the market are owned by a limited number of people. This allows the price of the coins to rise quickly as the masses flood exchanges with only a few coins to be had. This constriction on supply keeps price levels up as long as high demand is consistent. If large holders begin to liquidate in an aggressive fashion, there will clearly be intense pricing pressure.

### ***Fear of security breaches***

Bitcoin producers inform the public of security concerns in order to produce open source responses as security solutions. While these solutions can prove to be valuable, they also create uncertainty and volatility in the market. Although security breaches may result in greater scarcity of Bitcoins, the negative press resulting from the breach drives prices down.

### ***Recent changes in tax treatment***

The IRS has recently announced cryptocurrencies as an asset for tax purposes, resulting in price volatility. As a result, prices went up when a legitimate source recognized the concept as a currency. Prices have also been adversely affected; classifying Bitcoins as

property complicates the ability to use it due to the need to record the market value of the currency at every transaction point. Additionally, it has signaled that the IRS may potentially enforce stronger regulations on Bitcoin later, once again impacting the pricing.

## Approaching Valuation

Cryptocurrency valuation is very complex given that most cryptocurrencies are not asset-backed. There are several ways in which cryptocurrency valuation can be approached. This section covers different valuation methodologies, the advantages of each metric, and how they apply to cryptocurrencies.

### Absolute Valuation

Although cryptocurrencies are defined as assets, an asset-pricing model may prove challenging to use and apply. In general, an asset is valued by calculating the present value of the asset's cash flows—standard methodology would include preparing and reviewing a discounted cash flow analysis. This formula is fundamental for understanding how asset pricing works. However, traditional cryptocurrencies (excluding tokens) cannot be valued with this asset-pricing model because there are no dividends or cash payments. As a result, coins cannot be defined by a traditional asset-pricing model—intuitively this is true because cryptocurrencies were never intended to be treated as an asset or a store of value, but rather as a fiat currency.

### Relative Valuation

Similar to how a public company comparable valuation or a precedent transaction analysis gives a market valuation of a company, a relative valuation of cryptocurrencies can determine the “market” value of certain cryptocurrencies. Instead of choosing industry ratios like EV/EBITDA, EV/Revenue, etc., analysts could use cryptocurrency-specific ratios like  $(\text{Coin Market Capitalization})/(\text{Network Value to Transaction})$  or  $(\text{Coin Market Capitalization})/(\text{Transaction Speed})$  to determine the value of a cryptocurrency.

However, there is a challenge with the relative approach to valuing cryptocurrencies. Relative valuations rely on similar companies, but popular cryptocurrencies are built with differentiation in mind. This means that alternative coins are all built to offer very different features (like transaction processing, mining, etc.) that make them attractive to different audiences. For example, Ethereum offers an entire platform to execute automatic transactions or “smart contracts,” in addition to offering a platform to build applications on. Ripple is a cryptocurrency with features similar to Bitcoin, but with modified features targeted towards large financial institutions that help reduce the burden of high-volume, low-value international transactions. These seemingly small,

qualitative features make a significant impact on the value proposition and addressable markets for these cryptocurrency users. As a result, using relative valuation may not accurately capture value because of the variability in the currency.

### **Cryptocurrency-to-Commodity Modeling**

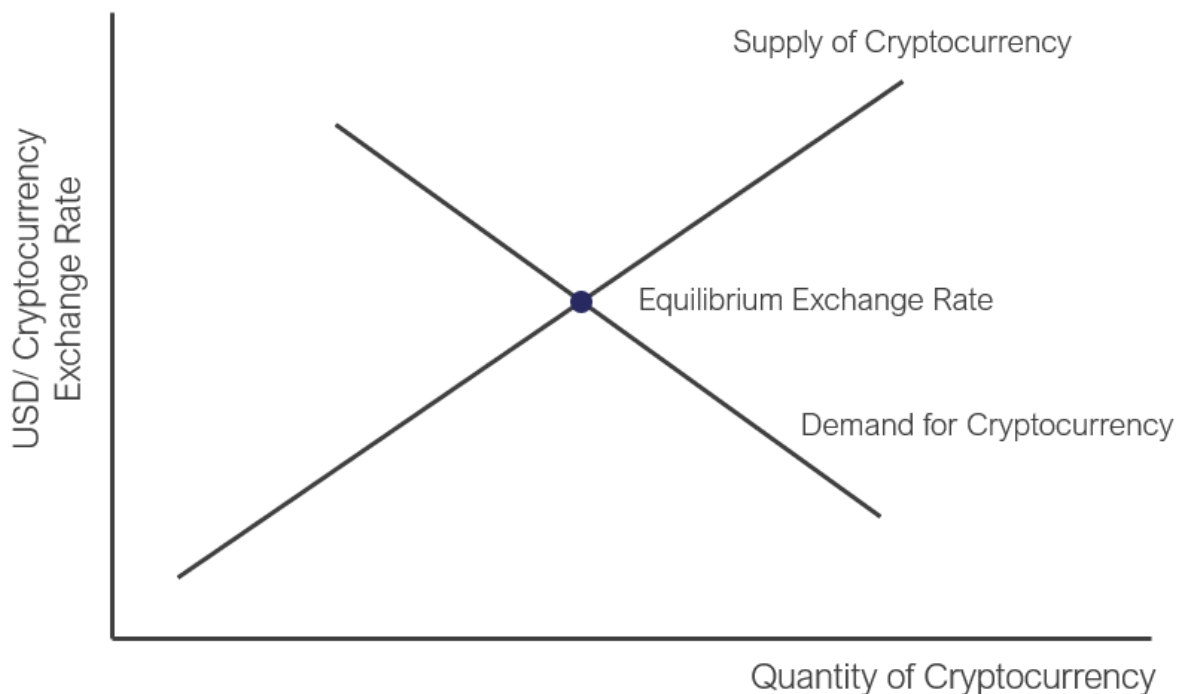
Much like commodities, cryptocurrencies possess intrinsic value. However, prices are still determined by supply and demand. It is the limited supply coupled with an asymptotic rate of growth and demand that gives cryptocurrency value. This is comparable to gold, with a somewhat stable supply. It should be noted that the cryptocurrency-to-commodity comparison can only be used for cryptocurrencies whose supply cannot be controlled.

A key assumption of this model is that fair market equilibrium is achieved. Other commodities like gold have matured over decades, and thus enjoy so-called equilibrium, but they still suffer from volatility from time to time. Cryptocurrencies have not reached that stasis. As a result, it may be a better prognosticator than a valuation tool. Additionally, large portions of the cryptocurrency market are controlled by “whales” preventing a stable market. Whales are large, anonymous investors that can influence prices due to how much they own.

### **Fiat Modeling, ForEx Valuation**

Instead of treating non-token cryptocurrencies as an asset worth “N” dollars, they can be treated like fiat currency with an exchange rate of N dollars for 1 Bitcoin or Ether. This is a very small difference in semantics, but the question shifts from “what is the value of the cryptocurrency” to “how much does cryptocurrency trade for.” The factors determining these exchange rates (i.e. the prices for cryptocurrencies) are now modeled by supply and demand rather than intrinsic value. In essence, the price of cryptocurrencies in USD is similar to Yen in dollars or Euros in dollars. However, this valuation argument cannot be applied to tokens due to the fact that they are asset-backed.

Exhibit 4: Pricing Cryptocurrency Using ForEx Valuation



### Marginal Cost Valuation

One other approach to cryptocurrency valuation is using the cost of mining cryptocurrencies as a proxy for value. People calculate the value of a cryptocurrency (like Bitcoin) by determining the amount of electricity (and consequently the price) needed to produce the cryptocurrency. This relies on the assumption that cryptocurrency miners would never sell cryptocurrencies below the cost of mining their cryptocurrencies, which is a sunk cost fallacy. If a miner spent \$10,000 worth of electricity to mine one XYZ-coin and the price is capped at \$8,000, classical economics dictates that he should sell the coin, despite making a \$2,000 loss. The sunk cost fallacy in this context might involve the miner holding the coin until the price is greater than \$10,000 (even though the price might just go lower). This approach cannot explain the current valuation, however; it only specifies a hypothetical minimum value.

### Cryptocurrency Performance Valuation

FundStrat, one of the leaders in Bitcoin price research, has suggested a new metric for determining Bitcoin pricing. This metric, Bitcoin Price to Mining Breakeven Cost (P/BE), is suggested to be a consistent indicator of performance. This valuation theory seems to match historical pricing well but also relies on questionable estimates for

breakeven costs. Furthermore, this valuation metric has received criticism for relying on the assumption that a miner would never sell coins for lower than their cost, which is a sunk cost fallacy.

## **Token Valuation**

Other cryptocurrencies are backed by goods or services. Similar to how the U.S. dollar was backed by gold (giving the USD some intrinsic value), specific cryptocurrencies launched in ICOs can have intrinsic value as well. Valuation approaches for token can be both absolute and relative, although specifics would vary from token to token.

Utility tokens or securitized tokens can be valued through an absolute approach by analyzing the underlying service or asset. A utility token can be valued by its services and a securitized token can be valued by its equity. For a utility token that allows users to access a demanding computing resource, the token can be valued by the subscription payments a user would pay to borrow the token from an initial investor. For a tokenized security of a company, the value of the token could be equal to the book value of that stake.

Similar to the absolute valuations, tokens can be valued relatively by their underlying service or asset. To continue the utility token example, a potential investor can benchmark the value of the token by comparing the computing performance of the service to other services like Amazon Web Services or Microsoft Azure. For a tokenized security of a company, valuation can be completed through a public comparable companies approach.

## **Valuation Conclusion**

In conclusion, valuation can be a tricky subject depending on the specific cryptocurrency at hand. Each coin is unique and the space is relatively new.

## Financing

### Venture Capital Funds and Major Institutional Investors

Over the past few years, institutional investors have noticed the uptick in cryptocurrencies' valuations and have begun to study and invest in these companies. ICOs raised over \$5.6 billion in 2017. Moreover, ICOs have exceeded that number by more than \$500 million so far in 2018.

Venture capitalists are taking an active role in the space for many reasons. VC firms are interested in the disruptive power of the underlying cryptocurrency and blockchain technology. Others are intrigued by the potential for returns by taking a position in an emerging industry that is projected to grow exponentially.

Eden Shochat, a Partner at Aleph VC, has an answer:

*One of the reasons that VCs were late was that much of the financing that came into the ICO world came in from the early wealth created by both Bitcoin and Ethereum. I think that is one angle where we had more than \$400 billion worth of wealth created in a very short while. For many of the people that came into the ICO world, they bought in- say for \$1,000- that is now worth \$10 million, so for them if you think of it as an investor, you're also thinking of it as leverage.*

---

Blockchain technology has penetrated several industries and fully crowdfunded projects now are present in the typically competitive fields of healthcare and real estate. As these mature and prove to be sustainable, VCs are going to want to hop on board. It is likely that they will be encouraged by actions from large entities such as Volkswagen and IBM, which have partnered with IOTA and Stellar, respectively.

A few notable venture capital firms are actively investing in the cryptocurrency market and/or already have investments in their portfolios, including:

#### ***FBG Capital***

FBG operates as an investment company providing real estate investments, investment management, and other services. Located in Beijing, China, it is a digital asset management firm in the blockchain-based capital market. FBG's portfolio of several



cryptocurrency and blockchain startups includes Eximchain (Blockchain, \$20M raise), Ultrain (Blockchain, \$20M raise), and Fragments (Cryptocurrency, \$3M raise).

### ***Fenbushi Capital***

Fenbushi is the first Chinese venture capital firm that exclusively invests in blockchain-focused companies. Its mission is to accelerate the inevitable future of the blockchain economy by supporting as many companies as possible. Fenbushi's portfolio includes Hashguard (Blockchain, \$10M raise), Tierion (Blockchain, \$26M raise), and Skuchain (Blockchain, Undisclosed).

### ***Blockchain Capital***

Blockchain Capital is a pioneering San Francisco-based venture capital firm investing in blockchain-enabled technology companies. Its initial fund was launched in the fall of 2013 and is the first VC Fund dedicated to the Bitcoin/blockchain ecosystem. Blockchain Capital's portfolio includes Coinbase (E-Commerce, \$217.2M raise), Gem (Blockchain, \$12M raise), and LedgerX (Bitcoin, \$12.9M raise).

### ***InBlockChain***

InBlockChain is the largest and most influential investment group in the Chinese blockchain space. It is among the largest global holders of Bitcoin and is an early investor in meaningful blockchain applications. Its internal products studio produced Yunbi, a leading global crypto-exchange, one of the highest-volume crowdfunding platforms, and other exciting infrastructure projects. Its portfolio also includes Eximchain (Blockchain, \$20M raise).

### ***Pantera Capital***

Pantera is a San Francisco-based investment firm focused exclusively on ventures, tokens, and projects related to blockchain tech, cryptocurrency, and cryptoassets. Pantera's portfolio includes Basis (Cryptocurrency, \$133M raise), NFC Direct (Bitcoin, \$17M raise), Xapo (Bitcoin, \$42M raise).

### ***Venrock***

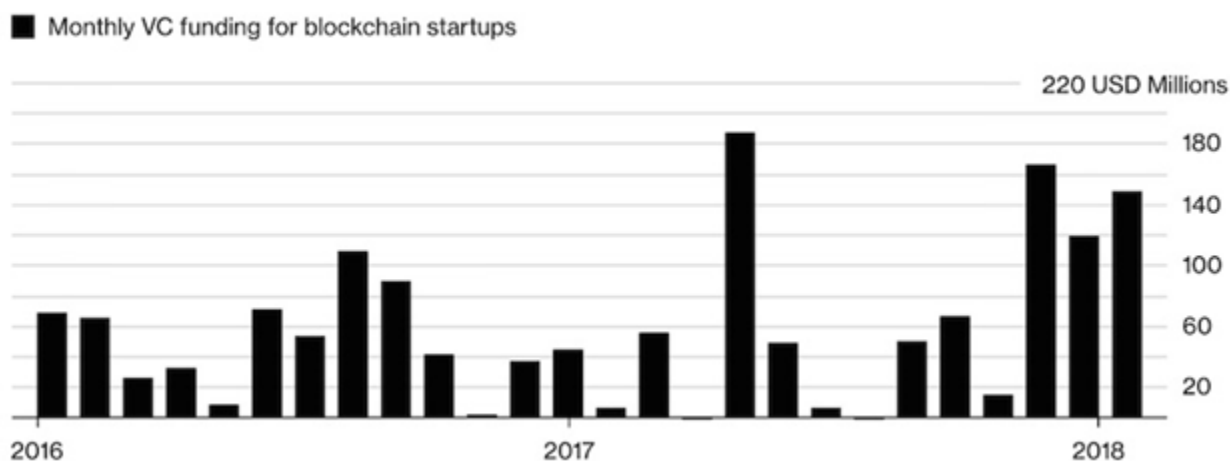
Venrock is a venture capital firm formed in 1969 to build upon the successful investing of the Rockefeller family in the 1930s. Venrock has invested more than \$2.5 billion in over 440 early stage companies, including Apple and Intel. Its latest partnership is with CoinFund, a blockchain technology research firm that provides consulting and research services to investors and companies interested in blockchain technology.

## ICOs and STOs an Alternative Sources of Financing

Initial Coin Offerings (ICOs) and Securitized Token Offerings (STOs) are recent funding trends and new forms of crowdfunding using cryptocurrency. Users “pre-mine” a token designed to provide some service or prove a stake in a company in exchange for money: ICOs for services and STOs for equity. Unlike shares of a public stock, these cryptocurrencies are fairly illiquid, meaning that these tokens cannot be easily bought or sold without affecting price.

Venture capitalists are showing more interest in ICOs. The main reason is the profit—cryptocurrency investors enjoy significant returns, with the liquidity of cryptocurrencies as a secondary driver. Tokens can easily be converted into Bitcoin or other cryptocurrencies as soon as the tokens are listed on an exchange. The investors can then convert them into cash via an online service such as Coinbase.

Exhibit 5: VC Funding for Blockchain Startups



Source: Coin Desk

# Regulatory Environment

## Governmental Regulation

Today, with the rising value of Bitcoin and its potential for global adoption, certain governmental authorities around the globe clearly intend to regulate the market. The purpose of these efforts is to safeguard investors when investing in this asset class. Likewise, the regulation will also be designed to reduce or eliminate illegal activities like money laundering.

Following a flurry of Initial Coin Offerings (ICOs), government agencies and regulators in the U.S., China, and elsewhere have started to focus on cryptocurrency activity. Now subject to increasing regulatory scrutiny, it has become evident that some of the ICOs floated were prone to potential anti-money laundering (AML) issues and challenges as well as fraudulent investment schemes. Thus, the SEC and other regulators are working to make cryptoassets and crypto securities more transparent. Ultimately, regulation may benefit the asset class.

## Current Regulatory Landscape

In the eyes of the SEC, there are two main types of cryptoassets: tokens and coins. Tokens are intended as a financial medium and are the main assets released during an ICO. Coins, specifically Bitcoin, Ethereum, etc., are tradable securities (intended to be a medium of exchange). In a House Appropriations Committee meeting on April 26, 2018, SEC Chairman Jay Clayton explained further:

*It's a complicated area. Because, as you said, there are different types of cryptoassets. Let me try and divide them into two areas. A pure medium of exchange, the one that's most often cited, is Bitcoin. As a replacement for currency, that has been determined by most people to not be a security.*

*Then there are tokens, which are used to finance projects. I've been on the record saying there are very few, there's none that I've seen, tokens that aren't securities. To the extent something is a security, we should regulate it as a security, and our securities regulations are disclosure-based, and people should follow those and provide the information that we require.\**

---

\* [appropriations.house.gov/calendar/eventsingle.aspx?EventID=395258](https://appropriations.house.gov/calendar/eventsingle.aspx?EventID=395258)

The SEC has already begun to police tokens. In December 2017, it filed its first complaint against an ICO, PlexCorps, for fraud relating to false marketing. The SEC cited PlexCorps for marketing and selling securities with false claims. In the following month, the SEC prevented AriseBank from starting a billion-dollar ICO for using aggressive and false marketing. Both offerings from PlexCorps and AriseBank were securitized tokens, and the regulatory action was in line with the SEC chairman's sentiment, setting the precedent for future regulatory action regarding tokens.

The regulatory environment of coins is starting to take shape as well. In July 2018, the SEC rejected an application from the Winklevoss twins for a Bitcoin-backed ETF, citing "lack of liquidity and custody." Based on this statement, it is widely expected that the SEC along with international regulators will administer changes to the sector so as to conform cryptocurrencies to security standards. The SEC ruling seems to indicate that while trading of cryptocurrencies is unregulated, any high-level investment activities will be subject to SEC regulations and may require portfolio managers to be registered broker-dealers. Further guidance is expected, as the SEC is currently reviewing two proposals, one by Bitwise Asset Management as well as a joint proposal by VanEck and SolidX.

### **SEC Taking Cryptocurrency Seriously**

On June 4, 2018, the SEC appointed Valerie A. Szczepanik as Senior Advisor for Digital Assets and Innovation. With previous experience in the cryptocurrency sector as Head of the SEC's Distributed Ledger Technology Working Group, Ms. Szczepanik spearheads the SEC's decision-making process regarding cryptocurrencies. Ms. Szczepanik is thought to have pivoted SEC's approach on cryptocurrencies, taking the position that it should be treated as a security.

### **Future Action**

While the regulatory landscape is taking shape, much of the sector is still the Wild West. One study from the University of Texas found that over half of the Bitcoin price increase from October 2017 to February 2018 was due to manipulative practices deemed illegal by the Dodd-Frank Act. Known as wash trading, these practices involved completing one's own sell order from another account. Bitfinex, one of the ten largest exchanges, acknowledged the practice and suspended the user, though according to an anonymous writer known as Bitfinex'ed, the practice continues.

Bringing a certain level of regulation may be good for the asset class. Regulation could help promote liquidity and transparency, while reducing or eliminating manipulation,

which should serve to secure more consumer protection and confidence in the asset class. With this new level of regulation, investors could be able to invest their capital more confidently, potentially growing the industry exponentially.

## Appendix A: Cryptocurrency Exchanges

Exchange	Base of Operations	Tradable Coins	Accept Fiat Currencies	Short Selling	Margin Trading	Fees
CoinBase	United States	5	Yes	No	No	Purchase Fees 1.49% - 3.99% with credit/debit cards
BitMEX*	Hong Kong	1	No	Yes	Yes	Maker Fee: 0.025%; taker fee: 0.075%
Binance	Malta	146	No	No	No	0.1% Trading fee However, if using, Binance Coin (BNB) there is a 25% deduction on trading fees
OKEx*	Hong Kong	185	Yes	Yes	Yes	Maker Fee: 0.15% - 0.02% (fees decrease with trading volume) Taker fees 0.2%-0.5% (fees decrease with trading volume)
Huobi*	Singapore	248	Yes	Yes	Yes	Maker/Take fees 0%-0.2%
BitFinex*	Hong Kong	79	Yes	Yes	Yes	Make/Taker fees 0-0.2%
Bithumb*	South Korea	37	Yes	No	No	Maker/Taker fee 0.15%
UPbit	South Korea	142	Yes	No	No	Make/Taker fee 0.05%
HitBTC	Hong Kong	22	No	Yes	Yes	0.01% make rebate, 0.01% take fee
ZB.com	Samoa	61	Yes	Yes	Yes	Make/Take fees 0.06%-0.2%
Bit-Z	Hong Kong, Beijing, Singapore	74	No	No	No	Make/take fee 0.1%
BitBox	China	62	No	Yes	Yes	Make/take fee 0.1%
Kraken	United States	17	Yes	Yes	Yes	Make/Taker fees 0% - 0.26%
Coinbase Pro (formerly Gdax)	United States	4	Yes	No	Yes	Make/Taker fees 0%-0.3%
Gemini	United States	3	Yes	No	No	Maker/taker fees 0%-1%

\*Currently not available to U.S. customers due to regulatory restrictions

Source: Oberon Securities

## Appendix B: Top Cryptocurrencies by Market Cap

As of August 20, 2018

Name	Symbol	Price (USD)	Market Cap (Millions, USD)
<b>Bitcoin</b> 	BTC	\$6,495.52	\$111,870
<b>Ethereum</b> 	ETH	\$282.14	\$28,629
<b>Ripple</b> 	XRP	\$0.335	\$13,205
<b>Bitcoin Cash</b> 	BCH	\$536.30	\$9,281
<b>EOS</b> 	EOS	\$4.93	\$4,464
<b>Stellar</b> 	XLM	\$0.224	\$4,200

Name	Symbol	Price (USD)	Market Cap (Millions, USD)
<b>Litecoin</b> 	LTC	\$56.65	\$3,283
<b>Tether</b> 	USDT	\$1.00	\$2,824
<b>Cardano</b> 	ADA	\$0.095	\$2,464
<b>Monero</b> 	XMR	\$94.80	\$1,549
<b>IOTA</b> 	MIOTA	\$0.519	\$1,444
<b>Tron</b> 	TRX	\$0.02	\$1,380
<b>Ethereum Classic</b> 	ETC	\$12.78	\$1,328
<b>Dash</b> 	DASH	\$141.72	\$1,172



Name	Symbol	Price (USD)	Market Cap (Millions, USD)
NEO 	NEO	\$17.78	\$1,156
Binance Coin 	BNB	\$9.71	\$927.4
NEM 	XEM	\$0.101	\$907.6
VeChain 	VET	\$0.0154	\$851.8
Tezos 	XTZ	\$1.36	\$827.5
Zcash 	ZEC	\$135.18	\$625.5
OmiseGO 	OMG	\$3.83	\$537.1
Lisk 	LSK	\$4.13	\$451.6

## Cryptocurrencies Primer

---

Name	Symbol	Price (USD)	Market Cap (Millions, USD)
<b>Qtum</b> 	QTUM	\$4.29	\$381.4
<b>0x</b> 	ZRX	\$0.708	\$380.9
<b>Ontology</b> 	ONT	\$2.25	\$340.7
<b>Bitcoin Gold</b> 	BTG	\$18.69	\$321.3
<b>Decred</b> 	DCR	\$37.90	\$315.7
<b>Bytecoin</b> 	BCN	\$0.0017	\$312.6
<b>Maker</b> 	MKR	\$430.0	\$287.3
<b>DigiByte</b> 	DGB	\$0.025	\$264.9

Source: [coinmarketcap.com](https://coinmarketcap.com)

## Appendix C: Top Coins by Market Cap

As of August 20, 2018

Name	Symbol	Price (USD)	Market Cap (Millions, USD)
<b>Bitcoin</b> 	BTC	\$6,495.52	\$111,870
<b>Ethereum</b> 	ETH	\$282.14	\$28,629
<b>Bitcoin Cash</b> 	BCH	\$536.30	\$9,281
<b>EOS</b> 	EOS	\$4.93	\$4,464
<b>Stellar</b> 	XLM	\$0.224	\$4,200
<b>Litecoin</b> 	LTC	\$56.65	\$3,283
<b>Cardano</b> 	ADA	\$0.095	\$2,464

Name	Symbol	Price (USD)	Market Cap (Millions, USD)
<b>Monero</b> 	XMR	\$94.80	\$1,549
<b>IOTA</b> 	MIOTA	\$0.519	\$1,444
<b>Ethereum Classic</b> 	ETC	\$12.78	\$1,328
<b>Dash</b> 	DASH	\$141.72	\$1,172
<b>NEO</b> 	NEO	\$17.78	\$1,156
<b>NEM</b> 	XEM	\$0.101	\$907.6
<b>VeChain</b> 	VET	\$0.0154	\$851.8
<b>Tezos</b> 	XTZ	\$1.36	\$827.5

Name	Symbol	Price (USD)	Market Cap (Millions, USD)
Zcash 	ZEC	\$135.18	\$625.5
Lisk 	LSK	\$4.13	\$451.6
Qtum 	QTUM	\$4.29	\$381.4
Bitcoin Gold 	BTG	\$18.69	\$321.3
Decred 	DCR	\$37.90	\$315.7
Maker 	MKR	\$430.0	\$287.3
Dogecoin 	DOGE	\$0.002	\$280.6
DigiByte 	DGB	\$0.025	\$264.9

## Cryptocurrencies Primer


Name	Symbol	Price (USD)	Market Cap (Millions, USD)
<b>ICON</b> 	ICX	\$0.64	\$248.1
<b>Nano</b> 	NANO	\$1.82	\$242.2
<b>Waves</b> 	WAVES	\$2.14	\$214.3
<b>MOAC</b> 	MOAC	\$3.22	\$200.9
<b>Verge</b> 	XVG	\$0.013	\$199.7
<b>Bitcoin Diamond</b> 	BCD	\$1.05	\$161.9

Source: [coinmarketcap.com](https://coinmarketcap.com)

## Appendix D: Top Tokens by Market Cap

As of August 20, 2018

Name	Symbol	Price (USD)	Market Cap (Millions, USD)
<b>Tether</b> 	USDT	\$1.00	\$2,824
<b>Binance Coin</b> 	BNB	\$9.71	\$927.4
<b>OmiseGO</b> 	OMG	\$3.83	\$537.1
<b>0x</b> 	ZRX	\$0.708	\$380.9
<b>Ontology</b> 	ONT	\$2.25	\$340.7
<b>Maker</b> 	MKR	\$430.0	\$287.3
<b>Zilliqa</b> 	ZIL	\$0.036	\$271.2








Name	Symbol	Price (USD)	Market Cap (Millions, USD)
Aeternity			
	AE	\$0.995	\$231.8
Basic Attention Token			
	BAT	\$0.210	\$209.6
Populous			
	PPT	\$5.00	\$185.1
Augur			
	REP	\$18.96	\$208.6
Pundi X			
	NPXS	\$0.0016	\$157.8
Bytom			
	BTM	\$0.167	\$167.1
Golem			
	GNT	\$0.15	\$144.1
Rchain			
	RHOC	\$0.439	\$159.0



Name	Symbol	Price (USD)	Market Cap (Millions, USD)
<b>Status</b>			
	SNT	\$0.039	\$136.2
<b>KuCoin Shares</b>			
	KCS	\$1.41	\$128.4
<b>Mithril</b>			
	MITH	\$0.328	\$123.6
<b>Dentacoin</b>			
	DCN	\$0.0004	\$116.2
<b>IOST</b>			
	IOST	\$0.013	\$112.0
<b>MaidSafeCoin</b>			
	MAID	\$0.241	\$109.0
<b>DigixDAO</b>			
	DGD	\$54.58	\$109.2
<b>Waltonchain</b>			
	WTC	\$2.92	\$117.2

## Cryptocurrencies Primer

---

Name	Symbol	Price (USD)	Market Cap (Millions, USD)
<b>Mixin</b> 	XIN	\$208.50	\$92.2
<b>Aelf</b> 	ELF	\$0.361	\$90.3
<b>Aion</b> 	AION	\$0.472	\$97.6
<b>Kin</b> 	KIN	\$0.00011	\$81.4
<b>ChainLink</b> 	LINK	\$0.315	\$110.3
<b>FunFair</b> 	FUN	\$0.018	\$89.4
<b>Bancor</b> 	BNT	\$1.60	\$84.0

Source: [coinmarketcap.com](https://coinmarketcap.com)

# Acknowledgments

*A special thanks to the summer staff that helped research and compose this report:*

---

Nathaniel Chevan

Paul Erlanger

Jack Finnegan

Ted Kim

Alexander Lawrence

Michael Noto

Stephanie Phen

Daniel Spear

**OBERON**  
**SECURITIES**

© 2018 Oberon Securities, LLC

Cover art by Computer Business Review