

May 10, 2022

## CRYPTOCURRENCY PRIMER

### *Crypto Fundamentals and Investment Opportunities*

- **Introduction to Cryptocurrencies.** Handing physical cash to another party in a transaction is quick, easy, and fee-less. Sending money over long distances or digitally, however, may take up to several days, often requires a fee, and has traditionally required trusting a financial intermediary like a bank or payment processor. Cryptocurrency transactions, on the other hand, are a digital equivalent to instantly handing over cash (even internationally) with minimal fees and no need for an intermediary. We introduce the technologies associated with the cryptic crypto world – blockchain, proof-of-work, altcoins, etc.
- **Investing in Cryptocurrencies.** In the second part of this primer, we cover the different pathways to cryptocurrency exposure. The main way to invest is to buy and hold cryptocurrencies from centralized exchanges. Shorting Bitcoin is made possible through margin trading on cryptocurrency exchanges. Furthermore, crypto-based derivatives have grown in popularity, especially since the October 2021 launch of the ProShares Bitcoin Strategy ETF (BITO) investing in Bitcoin futures. Derivatives can be used to speculate or hedge risk from unintended Bitcoin exposure in traditional portfolios.
- **Traditional Pathways to Investing.** A range of ETFs have become available offering traditional investors opportunities to invest in cryptocurrencies through more familiar channels. Futures-based ETFs are available in the US, while spot ETFs can be found in a few countries such as Canada and Switzerland. ETFs investing in Bitcoin mining and blockchain application companies also offer cryptocurrency exposure.
- **Regulatory Landscape.** Destabilizing financial systems, supporting terrorist money-laundering, and directly harming environmental goals are only a few reasons cited for flat-out crypto bans in nine countries. On the other hand, El Salvador became the first country to adopt Bitcoin as legal tender in June 2021. For the rest of the world seeking to regulate cryptocurrencies, a few trends persist.
- **Crypto and Blockchain Data Sources.** As an entirely new asset type, cryptocurrency research sidelines traditional valuation metrics. A range of new data sources and indicators have sprung up to sate institutional investors' data cravings. Facing a range of on-chain data metrics, coin price and supply stats, and exchange data providers, we denote a few starting points for quantitative cryptocurrency research.



Source: Pixabay.com

**Yin Luo, CFA, CPA**

[YLuo@wolferesearch.com](mailto:YLuo@wolferesearch.com)

**Kai Wu**

[KWu@wolferesearch.com](mailto:KWu@wolferesearch.com)

**Sheng Wang**

[SWang@wolferesearch.com](mailto:SWang@wolferesearch.com)

**Gaurav Rohal, CFA**

[GRohal@wolferesearch.com](mailto:GRohal@wolferesearch.com)

**David Elledge**

[DElledge@wolferesearch.com](mailto:DElledge@wolferesearch.com)

**QES Desk: 1.646.582.9230**

[Luo.QES@wolferesearch.com](mailto:Luo.QES@wolferesearch.com)

**Javed Jussa**

[JJussa@wolferesearch.com](mailto:JJussa@wolferesearch.com)

**Shu Liu**

[SLiu@wolferesearch.com](mailto:SLiu@wolferesearch.com)

**Hallie Martin**

[HMartin@wolferesearch.com](mailto:HMartin@wolferesearch.com)

**Victor Li**

[XLi@wolferesearch.com](mailto:XLi@wolferesearch.com)

**Larry Chen**

[LChen@wolferesearch.com](mailto:LChen@wolferesearch.com)

This report is limited solely for the use of clients of Wolfe Research. Please refer to the DISCLOSURE SECTION located at the end of this report for Analyst Certifications and Other Disclosures. For important disclosures, please go to [www.WolfeResearch.com/Disclosures](http://www.WolfeResearch.com/Disclosures) or write to us at Wolfe Research, Wolfe Research, 757 Third Avenue, Sixth Floor, New York, NY 10017.

## Table of Contents

<b>Introduction to Cryptocurrencies .....</b>	<b>3</b>
Bitcoin.....	5
Blockchain .....	7
Proof-of-Work .....	9
Shortcomings of Bitcoin .....	16
<b>Altcoins.....</b>	<b>19</b>
Ethereum .....	19
Dogecoin .....	21
Tokens.....	24
Stablecoins .....	26
<b>Cryptocurrency Investing.....</b>	<b>27</b>
Wallets and Custody .....	27
Purchasing Cryptocurrencies .....	28
Crypto Exchanges .....	31
Crypto Equity-Linked Products .....	34
<b>Applications of Blockchain .....</b>	<b>39</b>
DeFi .....	39
NFTs .....	40
Web3 .....	42
ESG Concerns and Crypto Regulations.....	43
<b>Crypto Data Sources .....</b>	<b>46</b>
Exchanges .....	46
Navigating the Blockchain with Blockchain Explorers.....	46
Alternative Vendors .....	49
QES Resources .....	50
<b>Bibliography .....</b>	<b>53</b>
<b>Disclosure Section.....</b>	<b>54</b>

## INTRODUCTION TO CRYPTOCURRENCIES

A cryptocurrency is a decentralized digital currency designed as a medium of exchange secured by cryptography, a secure communication technique between two parties. Money, as a medium of exchange, can be defined as anything accepted for a valuable good or service. Handing physical cash to another party in a transaction is quick, easy, and fee-less. Sending money digitally, however, may take up to several days, often requires a fee, and has traditionally required a financial intermediary such as a bank or payment processor. Cryptocurrency transactions, on the other hand, can be equated to instantly and digitally giving cash to the recipient with minimal fees and no intermediary.

Unlike fiat currencies, cryptocurrencies are not issued by governments, rendering their supply impervious to intervention. A distributed ledger technology called blockchain, records transactions in a chronological, timestamped manner and facilitates the verification of transactions by a decentralized network of computers rather than a central bank. Users directly hold their assets in the digital wallet rather than the custody of a bank account where balances can be effortlessly tracked. Although the complication of purchasing cryptos can be a barrier, the advent of mobile applications for wallets and cryptocurrency exchanges lessens this burden. On a macro scale, this potentially opens access to financial services and internet commerce for billions of people outside of the traditional banking infrastructure.

While originally intended to replace physical currencies with digital files and bytes, cryptocurrencies are widely speculated and viewed as a unique asset class. The total market capitalization of the crypto industry hit a record \$3 trillion in November 2021. Moreover, seven out of every 10 cryptocurrency holders invested for the first time in 2021, according to a study by crypto exchange Huobi<sup>1</sup>. A range of crypto-based derivatives also became widely available last year as crypto is blending into traditional exchanges in the form of both spot and futures-based ETFs. While a background in traditional finance is indispensable for investing, a grasp of relevant fields like cryptography and computer science is probably even more valuable to understand cryptocurrencies. The crypto industry is now too large to ignore (and fail). This report serves as a cryptocurrency primer for institutional investors.

**We would like to express our gratitude to Justin Ullman, a new member of the QES team. Justin's tireless work effort made this research possible.**

### *Cryptography*

Unlike physical gold or cash, the greatest threat to digital currency is the potential impersonation of owners and false duplication of digital assets. Despite popular belief, Bitcoin is not the first digital currency. Instead, there were previous attempts. However, Bitcoin addressed issues of digital currency counterfeiting using modern cryptographic hash algorithms, a technology associated with digital signatures and password encryption. Understanding the technology is essential to trusting the security of cryptocurrencies.

Cryptographic hash algorithms are mathematical functions, which take an arbitrary-length input of text, perform complex mathematical operations, and output a fixed-length string of numbers and letters called a hash value. Every unique input produces a different hash value. However, entering the same input should always yield the same output. More importantly, changing even one letter of input

<sup>1</sup> See <https://www.scmp.com/presented/tech/tech-trends/topics/cryptocurrency-investor-outlook/article/3163204/huobi-reveals> for more detail.

completely alters the resultant hash value. In Bitcoin's case, the encryption algorithm is called SHA-256 – a standard algorithm used in password storage and digital signatures<sup>2</sup>.

Cryptographic hash algorithms are both collision resistant and one-way. Collision resistant means every input produces a unique output (see Figure 1). One-way means that a hash value cannot be reverse engineered to find the original input. As an analogy, every person (input) has a unique fingerprint (hash value). When given a random fingerprint (hash value) alone, one cannot guess the owner. When given a name and a fingerprint, however, one can check if they match easily. Similarly, hash algorithms can be checked by hashing the input and verifying the output matches what is expected. These qualities are useful for securing digital currency transactions, because original copies of transaction data can be publicly broadcasted with a matching hash value. Changing data also varies its hash value, therefore hashing the transaction data easily verifies its unaltered state if the result matches the original hash value.

**Figure 1 Altering Input Data Affects the Hash Value**

<i>Message</i>	Yin sent 5.50 bitcoins to Javed on 1/31/22 at 10:54AM Hallie sent 12.00 bitcoins to Shu on 1/31/22 at 10:56AM Victor sent 6.75 bitcoins to David on 1/31/22 at 10:58AM
<i>Hash</i>	4fc503371be1f1db800defa446963b6679fa1b1a28364237a7a8a54c7c552411
↓	
<i>Message</i>	Yin sent 5.51 bitcoins to Javed on 1/31/22 at 10:54AM Hallie sent 12.00 bitcoins to Shu on 1/31/22 at 10:56AM Victor sent 6.75 bitcoins to David on 1/31/22 at 10:58AM
<i>Hash</i>	ea0ebbd3ac518f67cd3cf1bddf668216de2add7572703e2c65b9891c017127a1

Source: SHA-256 hash algorithm demo at [moveable-type.com](https://moveable-type.com)

Public-key cryptography, the technology associated with digital signatures and password encryption, is used extensively in cryptocurrencies. Public-key cryptography uses a pair of private and public keys created with hash functions to digitally sign documents. Private and public key pairs are cryptographically matching strings of text used to create and verify digital signatures, respectively<sup>3</sup>. Private keys, as their name implies, are kept private by their owners and act like passwords for sending cryptocurrency – akin to debit card PINs. Public keys are hash values derived from the private key and are equivalent to a bank account number for receiving funds. The signature serves as evidence that the private key owner sees the document. Due to the one-way quality of cryptographic hash functions, a private key cannot be reverse engineered and re-created from a user's public key. We will cover the use case of public-key cryptography in a later section.

<sup>2</sup> See <https://academy.binance.com/en/articles/what-is-hashing> for more detail about cryptographic hash functions and SHA-256.

<sup>3</sup> See <https://www.ibm.com/docs/en/ztpf/1.1.0.14?topic=concepts-public-key-cryptography> for more about public-key cryptography.

## BITCOIN

Bitcoin is the first real-world application of blockchain – a distributed ledger technology – set forth in a 2008 white paper under the pseudonym Satoshi Nakamoto (see Nakamoto, [2008], available [here](#)). Its continued popularity for payments owes to its relative simplicity and strong cryptographic security. Its legacy is largely a result of its innovative use of the digital distributed ledger technology, which has also created new realms of possibility in finance and other industries like health care and global shipping. While originally designed to record transaction data in Bitcoin, blockchains can record any type of data. Blockchain's potential to disrupt entire industries has been compared to the creation of the internet.

At a high level, Bitcoin is a digital medium of exchange whose transactions are cleared in a decentralized manner. Bitcoin transactions are recorded on a public, anonymous ledger and shared among a peer-to-peer (P2P) network of computers running Bitcoin software. The P2P structure ensures that no single entity has central authority to edit transactions or alter the supply of Bitcoins. Instead of the traditional data structure of tables, Bitcoin's ledger is structured into timestamped groups of transaction data called blocks, which are linked in a single, continuing chronological chain. Participants in the network are incentivized to complete difficult computational challenges based on modern cryptography – a process called Bitcoin mining – to create blocks in exchange for a reward. The artificial difficulty of verifying blocks renders the blockchain virtually immutable and irreversible, providing the trust of a bank ledger without needing a financial intermediary.

As an asset, Bitcoin has been touted as digital gold for its store of value function, its limited supply, and seeming lack of correlation with traditional financial products. Bitcoin's rapid rise used to be mainly driven by retail investors. However, its supposed lack of correlation has also made it an appealing addition to traditional institutional portfolios. Recent institutional buy-in drove the price of Bitcoin to its all-time high in November 2021 of over \$68,000. Bitcoin's market share in the cryptocurrency market, however, fell from 70% to 40% in 2021, as new cryptocurrencies emerged<sup>4</sup>. As Bitcoin is the skeleton for thousands of other spin-offs "altcoins," understanding the basic technological foundation is crucial to evaluating what other cryptocurrencies offer.

### P2P Networks

A P2P network is a decentralized model for communication among a distributed network of computers<sup>5</sup>. Computers in the network directly exchange messages and data to form a virtual web of flowing information, which all network participants can download like a database. An example of a P2P network is torrent software, in which peers upload files for all to view and download – commonly used for illegally sharing copyrighted duplications of music and movies. Any computer which downloads a P2P network's software can participate in the network's communication.

The Bitcoin P2P network is a global network of hundreds of thousands of computers communicating to share broadcasts of Bitcoin transactions. Its peers, also called nodes, are computers running Bitcoin software and connected to the Internet. Anyone can download Bitcoin software and set up their own node. Instead of uploading illegal movies, peers in the Bitcoin network relay updates of new Bitcoin transactions for the network to view and download. Downloading and storing the flowing information inherently leads to a decentralized database of Bitcoin transactions.

<sup>4</sup> View the Bitcoin market cap dominance chart at [https://www.coingecko.com/en/global\\_charts](https://www.coingecko.com/en/global_charts)

<sup>5</sup> See <https://academy.binance.com/en/articles/peer-to-peer-networks-explained> for more detail on P2P networks

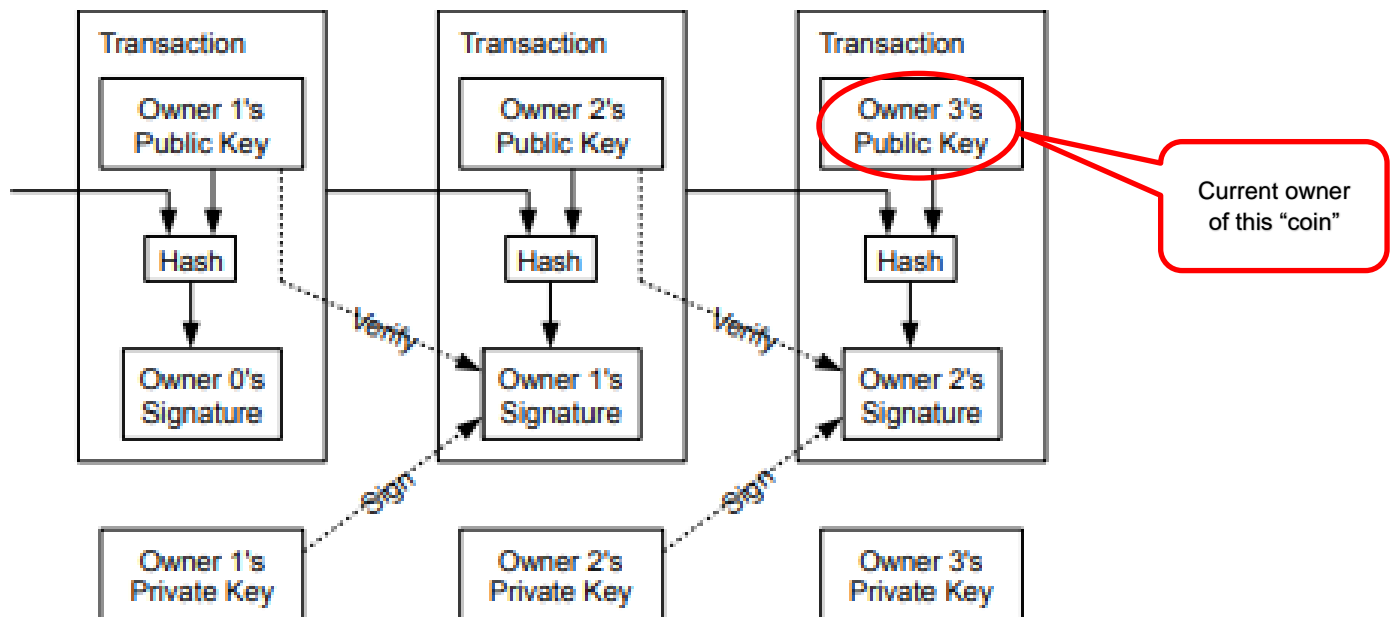


As a decentralized database, copies of Bitcoin's database are shared among all nodes in the network, who store a copy in their hard drives rather than a single master copy stored in a central server hub. The database when downloaded currently requires about 380 gigabytes of storage space<sup>6</sup>, and increases in size as transactions are added. Since a copy exists on every node's hard drive, no single entity can unilaterally alter the Bitcoin database – governments cannot demand to freeze funds or control the Bitcoin supply. Contrarily, all nodes are free to edit their own individual copies to add transactions. Any node can broadcast transaction messages to others, but none can ultimately force others to change their copies.

### Bitcoin Transactions

On a technical level, an electronic coin is an encrypted chain of digitally signed transactions (See Nakamoto, [2008], available [here](#)). Sending and receiving Bitcoin boils down to broadcasting a message to the network that a new transaction is being added to its chain. Peers can broadcast any message to the network. They can also broadcast fraudulent transactions sending Bitcoins they do not own. Broadcasts, therefore, must contain three key pieces of information (see Figure 2 Model of an Electronic “Coin”) to ensure they are spent only by their rightful owners – the public key of the new recipient, a digital signature created with the sender's private key, and a cryptographic hash of the previous transaction. The chain of transactions shows how the Bitcoin transferred ownership.

Figure 2 Model of an Electronic “Coin”



Source: Satoshi Nakamoto, “Bitcoin: A Peer-to-peer Electronic Cash System” (2008)

As shown in Figure 2 Model of an Electronic “Coin”, Owner 1 was the original owner/holder. Owner 1 sent the Bitcoin to Owner 2. In turn, Owner 2 sent the Bitcoin to Owner 3, who is the last recipient in the transaction and thus the rightful owner of the Bitcoin. As discussed in the cryptography section, a public key is like a public bank account number given out to receive funds. To prevent impersonation,

<sup>6</sup> See <https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/> for Bitcoin blockchain size.

every user has a unique pair of matching private and public keys to identify themselves. A transaction message needs a recipient's public key to denote the Bitcoin's new destination. "Owning" a Bitcoin is the equivalent of one's public key being the last recipient in its chain of transactions. A Bitcoin's history of ownership is traced through the public keys listed in its transaction history, with the last key being the current owner.

The digital signature ensures that the sender of the message owns the Bitcoin being transferred. A sender creates the digital signature by hashing their private key in combination with the transaction text and broadcasting the result. The signature cannot be simply copied and re-used since it changes based on the transaction text, producing a unique signature every time. Recipients verify the signature by decrypting it with another function using the previous recipient's public key. Since the Bitcoin's current owner should be the previous recipient, the sender's private key should match the last recipient's public key. The verification function confirms or denies if the sender's private key matches the previous recipient's public key – without revealing the private key. If they don't match, nodes who receive the transaction broadcast immediately reject it, otherwise the transaction is sent to a temporary waiting room for pending transactions called the mempool.

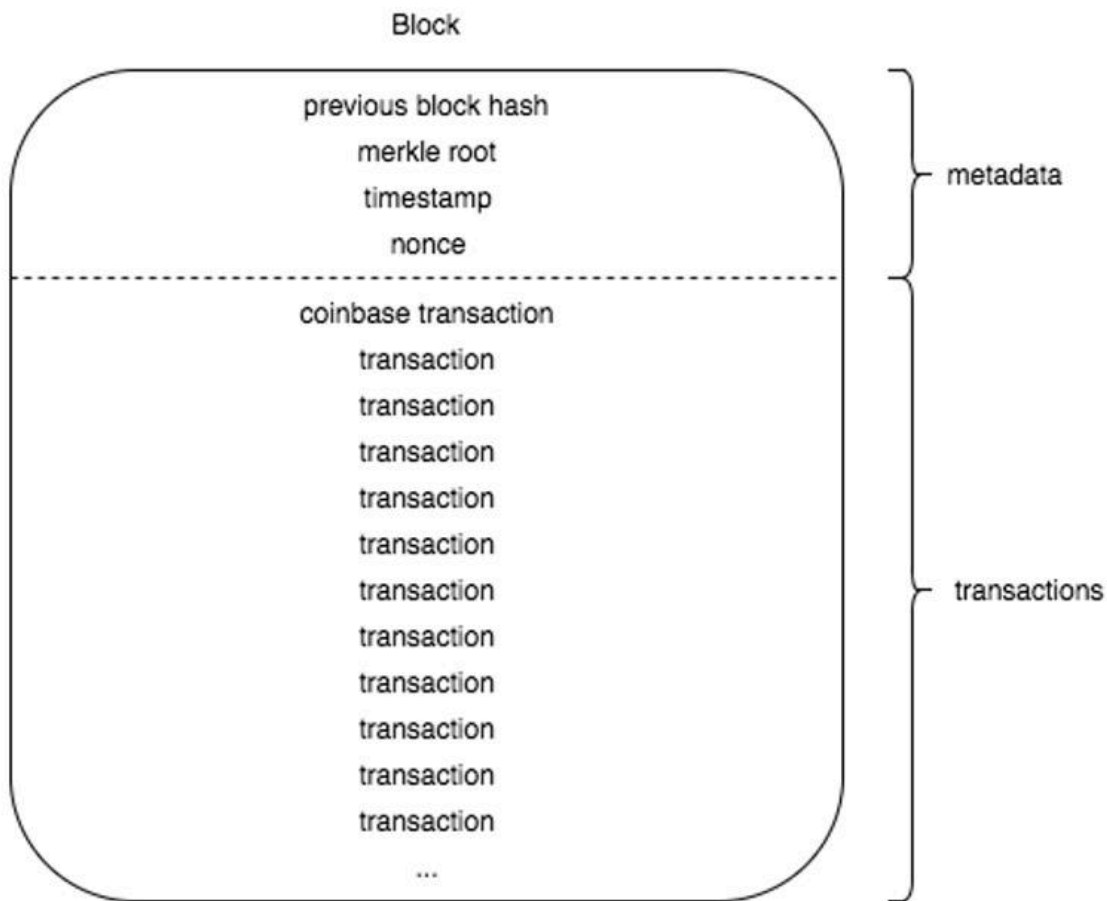
When the text of a transaction is run through a cryptographic hash algorithm, the resulting hash value is the transaction hash – an identifier for the specific transaction. The new transaction must include the Bitcoin's previous transaction hash to link them in a digital chain. The Bitcoin's history of ownership is reflected in the chain of transaction hash values. A Bitcoin's history cannot be changed because altering the text would change a transaction hash, along with those in the chain thereafter.

## BLOCKCHAIN

Since any node can broadcast to others, nodes can also broadcast multiple transactions, spending the same Bitcoin unit at one time. A P2P database therefore could only function if the network's participants can agree on the order of transactions to determine who gets the Bitcoin. Bitcoin's solution to this is to organize transaction data into a public, immutable, and irreversible chain of timestamped groups called blocks instead of the traditional table structure of data (See Babich, et al, [2021], available [here](#)). The order of transactions is determined by which transaction is gathered from the mempool, added into a timestamped block, and validated first. The data structure, known as blockchain, proves the existence of certain data at a point in time. Its purpose is to replicate a bank ledger in which information is recorded and distributed, but not freely edited thereafter.

At a high level, individual blocks have two parts: a header containing metadata and a body listing thousands of Bitcoin transactions (see Figure 3 Illustration of a Block for an illustration). Blocks are like a binder storing accounting entries in which the first page contains information summarizing the contents and the rest records transactions. Each block, or binder, has a set storage space or number of pages. Once the storage capacity is filled with transactions, the block is closed off to changes and added to the end of the blockchain, like a binder is filed in chronological order on a shelf. Then, another block or binder is opened, and the process is repeated.

Figure 3 Illustration of a Block

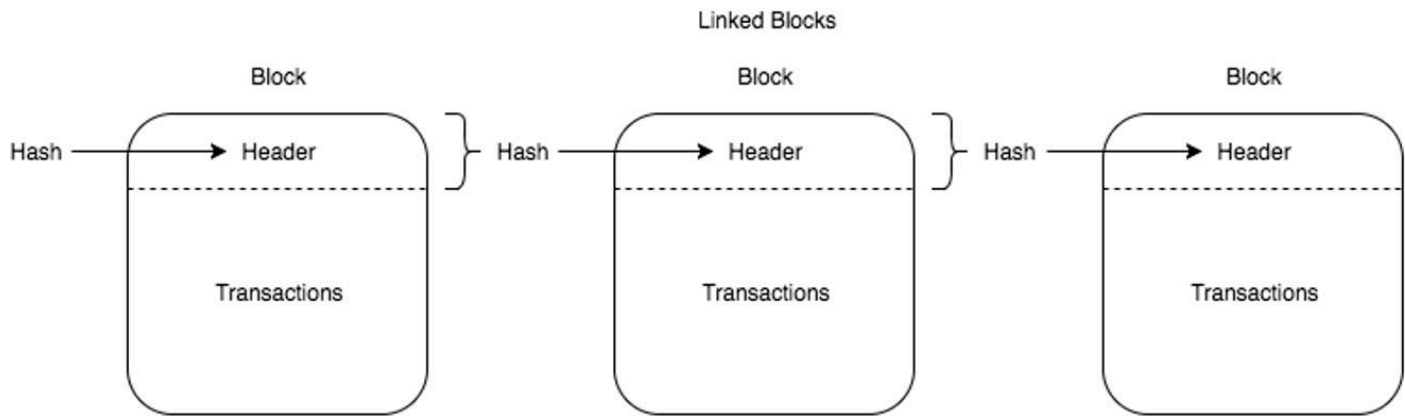


Source: PluralSight "Blockchain Architecture"

The metadata includes the block's key identifying information and summaries of the block's transaction data. This includes an index number also known as the block "height," denoting the block's position in the blockchain – a larger number indicates a more recent block. The number of transactions within the block, its aggregate transaction volume in bitcoins, and a hash value of aggregated transaction data known as a Merkle root are included. A timestamp denotes when the block was validated, proving that certain transactions existed at the time of the block's creation. Every block also contains a unique number only used once, called nonce, which represents a proof-of-work – a concept we will explain in the next section. Lastly, when all a block's data is run through a cryptographic hash function, a block hash value is created. Each block's header contains the hash for the previous block in the blockchain, linking them together (see Figure 4 A chain of blocks linked with hash values).



**Figure 4 A chain of blocks linked with hash values**



Source: PluralSight "Blockchain Architecture"

The block hash is the identifier for the block, but more importantly, renders the block immutable. Given the properties of hash functions, altering even one character in a block's data – whether tampering with a transaction amount or the block's index number – completely changes its hash value. The hash values of every block in the chain thereafter also changes as each block contains the previous hash. Incorrect copies of the blockchain are caught easily since different hash values can be pinpointed and rejected by the network of nodes constantly cross-referencing each other. The immutability of this blockchain establishes a publicly accepted order of events.

The content of any block and the order of blocks can be found in a public blockchain explorer. Individual blocks contain thousands of transactions and exchange tens of thousands of Bitcoins each – often worth well over \$1 billion in total volume. At the time of writing this report, the Bitcoin blockchain contains over 723,000 completed blocks with over 230 million verified transactions.<sup>7</sup>

## PROOF-OF-WORK

Now, after we outlined how a blockchain is structured, in this section, we discuss one key security feature inherent in the blockchain. Since nodes do not know one another's identities or motivations, agreeing on a single copy of the blockchain based on trust alone is impossible. Although a block cannot be changed after it is created, how could others trust that broadcasted blocks are not fraudulent at inception? Since anyone can broadcast blocks, dishonest nodes could attack the network by flooding it with fake blocks. The solution to such an attack is a consensus mechanism, which facilitates agreement by rendering the creation of fraudulent blocks too costly to undertake. Bitcoin's consensus mechanism is called proof-of-work.

In a proof-of-work model, broadcasting a new block requires attaching a cryptographic proof that electricity-expensive computational work was completed. Altering the blockchain thus requires a lot of computational "work," deterring most would-be hackers from the tremendous effort of attacking the network by creating fraudulent blocks. Although a hacker could create a proof-of-work and share the fraudulent block, it is unlikely that they would be willing to do this at scale. Proof-of-work consensus relies on cryptographic hash functions, block hash values, and nonces.

<sup>7</sup> See <https://www.blockchain.com/explorer> for blockchain statistics and charts.

The actual proof-of-work which must be attached to a block is the mentioned nonce (a number only used once) included in the block headers. The number added must be one which, when hashed in combination with the rest of the block, produces a hash value starting with several starting zeroes (see Figure 5 Incrementing the Nonce to Search for a Working Hash Value). This system is implemented by requiring criteria for block hash values; every valid block hash must start with an adjustable number of zeroes, increasing the difficulty of finding a working nonce exponentially as more zeroes are required. Since hash functions create completely random strings of text, finding a nonce with qualities can only be done through running cryptographic hash calculations through trial-and-error until a valid block hash is found. In practice, this mathematically entails testing billions of numbers on average – the working nonce therefore is proof of the required computational work being completed.

**Figure 5 Incrementing the Nonce to Search for a Working Hash Value**

The figure illustrates the process of finding a valid hash for a block by incrementing the nonce. It shows two examples of block data and their corresponding hashes.

**Example 1 (Top):**

- Block:** # 1
- Nonce:** 1
- Data:**
  - Yin sent 5 bitcoins to Javed on 2/10/22
  - Kai sent 7 bitcoins to Hallie on 2/11/22
  - Mack sent 8 bitcoins to Ed on 2/11/22
- Hash:** 28cec017f451924c5023c725c48cab2732c35654707e376af8eaba04fbbcbdd

**Example 2 (Bottom):**

- Block:** # 1
- Nonce:** 22928
- Data:**
  - Yin sent 5 bitcoins to Javed on 2/10/22
  - Kai sent 7 bitcoins to Hallie on 2/11/22
  - Mack sent 8 bitcoins to Ed on 2/11/22
- Hash:** 000091a628b67d77cdf465fb7386c4237cc2de635bd70d0ee5616effa4229f68

**Callout Box:** This nonce must be incrementally adjusted until a hash value starting with four zeroes is found.

Source: Andersbrownworth.com

Changing a block's data will change its hash along with every block in the chain thereafter. To be accepted by the network, a changed block would need a new proof-of-work. The consensus mechanism facilitates trust and security in the blockchain, with the caveat that peers will only accept the longest copy (more blocks added) of a blockchain as the true copy. Changing any block thus requires the miner

to catch up to the newest block and outpace the rest of the network, maintaining the longest blockchain copy. An effective attack like this would require more than half of the network's power, so the security of the blockchain increases as more miners join the network and as the chain gets longer. While other consensus mechanisms exist, the proof-of-work model is considered by far the most secure.

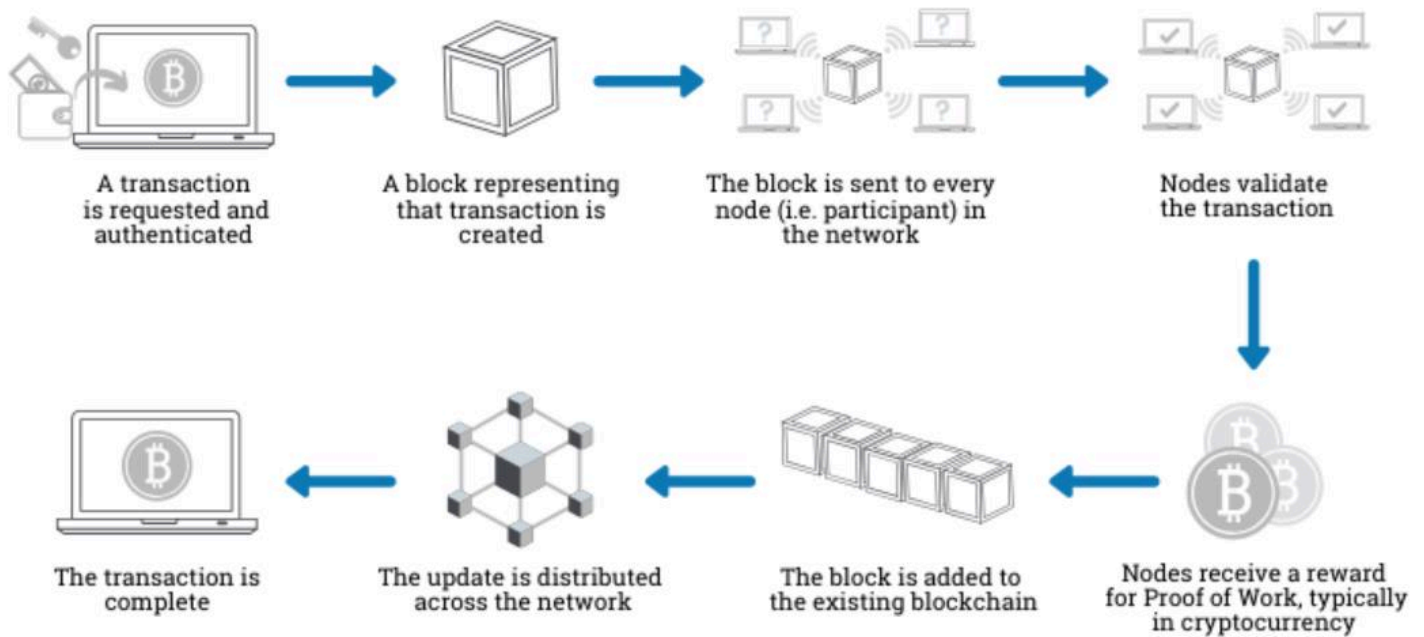
### **Bitcoin Mining**

Mining is the process during which all transactions broadcasted to the network are confirmed, a process usually taking 10-20 minutes. According to the structures of Bitcoin detailed above, a transaction must go through several steps after broadcasting to be confirmed. Immediately after a transaction is broadcasted, it is added to the mempool. Thereafter, it must be packaged into a block and added to the blockchain. The packaging process is called mining and follows a set of strict cryptographic rules to prevent fraudulent blocks. These rules restrict previous blocks from being easily modified – changing the amount of a previous transaction for example – protecting the blockchain's chronological history. These rules incentivize users to secure the network as honest actors.

Since the Bitcoin network is decentralized, the task of packaging transactions into a block candidate, finding a proof-of-work, and broadcasting new blocks is also decentralized. Nodes who take up this task of forming blocks in exchange for a reward are called miners. To encourage participation, miners are incentivized with newly minted Bitcoins as a reward for completing these energy-intensive functions. The process is called Bitcoin "mining" because it has been compared to gold miners spending energy to find gold into circulation. New blocks are added to the blockchain at a target frequency of about once every 10 minutes, meaning new Bitcoins are added into the monetary base regularly.

At a high level, the mining process requires scraping transactions from the mempool, organizing their data in block format, and finding an accompanying proof-of-work, or cryptographic proof that computationally intensive calculations are performed. The proof-of-work requirement pits miners against each other in a race to find a nonce, an arbitrary number used only once in cryptographic communication. Once a valid block is formed, the winning miner broadcasts it to peers, who then validate transactions and check the block's hash value for enough starting zeroes. Verifying that a block's hash value meets the requirements simply entails running the block's full contents through the SHA-256 hash function and cross-referencing it with the results. If the block is valid, nodes add it to their copy of the blockchain and broadcast it to pass along the new data to other peers until the full network received it (see Figure 6 Construction and Approval Process of a Block).

**Figure 6 Construction and Approval Process of a Block**



Source: Euromoney.com

The fastest miner to broadcast a valid block to the network is issued a reward from two sources. Every transaction contains a flat amount of Bitcoin transaction fees allocated for the miner who validates it. Payers may also include a premium on top of the flat amount to encourage miners to validate their transactions first. When scraping transactions from the mempool, miners generally choose those which rewards the most in fees. Base transaction fees for a given transaction range from \$1 to \$50 value in Bitcoin. Historically, the fees were typically below \$5. Fees make up a relatively small portion of miners' rewards, as they range between 0.10 bitcoins and 0.3 Bitcoins per block. It is critical to note that slower miners who fail to broadcast a valid block first receive no reward. As a result, the electricity spent by these failed miners is wasted. We will come back to this topic later.

Albeit counterintuitive, most of the mining reward is issued to the winning miners by themselves rather than by the payers. Every block must contain a special transaction called the "coinbase" which denotes adding a generation of new Bitcoins to the block miner's public key address (also known as a Bitcoin wallet). The coinbase differs from typical transactions because there is no sender of a coinbase. Importantly, the amount which can be rewarded decreases over time based on rules of the Bitcoin protocol. While some contend there is no underlying value behind Bitcoin, the electricity expended by the full network to mine a block can be viewed as the intrinsic cost of Bitcoin. As more miners compete for the same reward, the aggregate number of hashes calculated by the network increases. This reduces mining profitability since more electricity and better hardware are required to outpace other miners (see Figure 7 Relative Profitability of Mining Over Time).

**Figure 7 Relative Profitability of Mining Over Time**


Source: Blockchain.com, Wolfe Research Luo's QES

The entire process described above happens automatically at lightning speed, calculated by hundreds of thousands of computers in the Bitcoin network. A Bitcoin mining node can be setup seamlessly by simply running Bitcoin mining software on a computer at home – albeit electricity costs alone are likely to outweigh the gains. Initially, mining was done using basic computer processors. However, GPUs used for computer gaming have proven to be significantly faster (see [Deep Learning Statistical Arbitrage Strategies](#) for details on GPU computing). More recently, specialized computers called Application-Specific Integrated Circuit (ASIC) machines have been developed for the sole purpose of mining. Mining operations in practice are often large facilities running thousands of specialized computers. Their main costs post-setup include rental for the facility, electricity, and staffing for infrastructure maintenance.

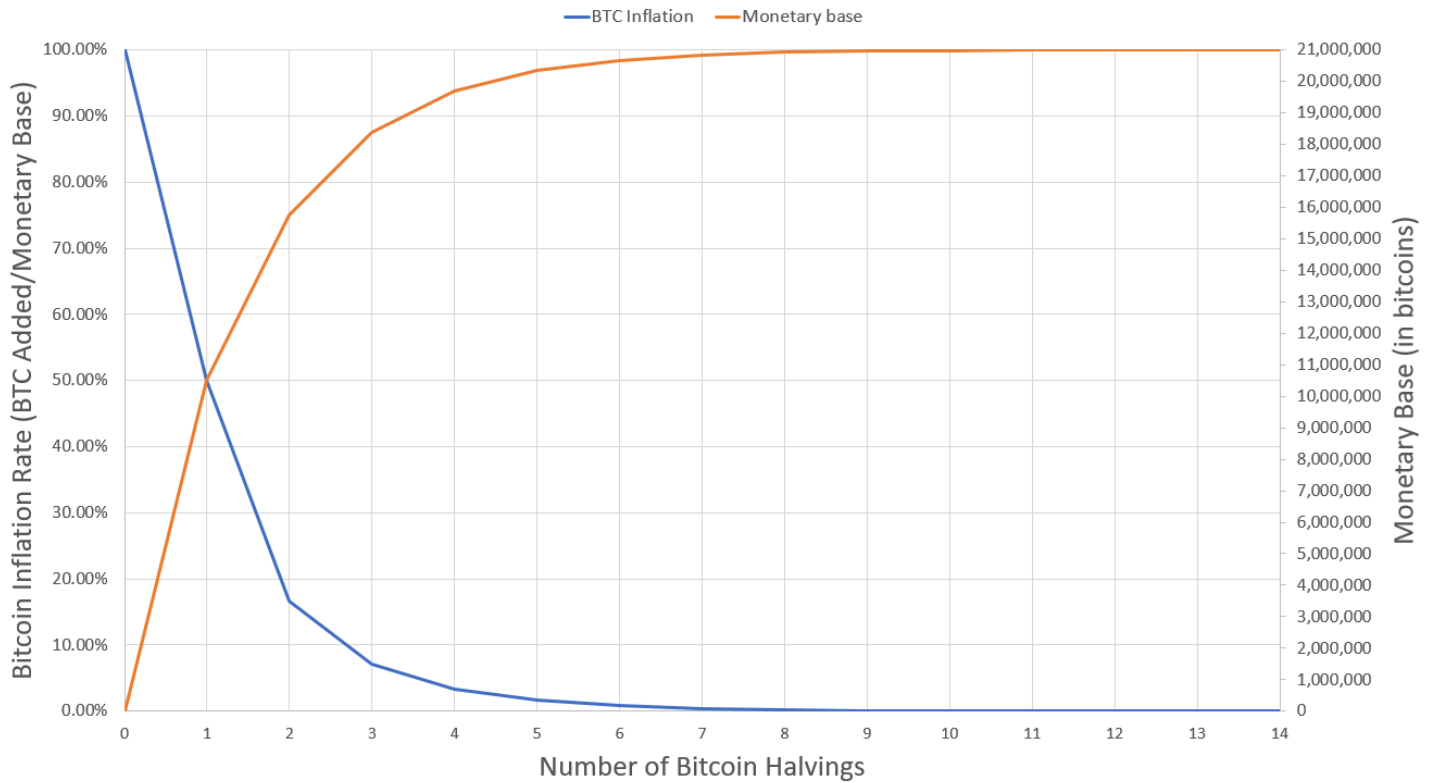
### Supply and Difficulty

A cryptocurrency's supply is determined by its developers at inception. Its inflationary or deflationary effect on price can make or break a project. From inception, Bitcoin's maximum supply was limited to 21 million Bitcoins, of which around 18.9 million have already been mined. After every 210,000 blocks formed, the coinbase reward reduces by a half. The original reward for mining one block was 50 Bitcoins. This number halves after every 210,000 blocks mined (or roughly four years). As 722,000 blocks (representative of 18.9 million Bitcoins) have been mined, the current reward stands at 6.25 Bitcoins. Historically, Bitcoin halving events were preceded by bear markets as rewards diminish and mining becomes more difficult. However, these bear markets were followed by crypto bull runs. Bitcoin's "digital gold" analogy relates to the diminishing returns to mining over time, increasing rarity and upward pressure on its price. As shown in Figure 8 Bitcoin Inflation Rate and Size of Monetary Base over



Progression of Bitcoin , the diminishing block reward affects Bitcoin's inflation rate and growth of its monetary base over time.

**Figure 8 Bitcoin Inflation Rate and Size of Monetary Base over Progression of Bitcoin Halvings**



Source: Wolfe Research Luo's QES

Bitcoin's creators also kept in mind the effects of upgrading hardware and a larger number of participating miners on its future supply. The difficulty of mining adjusts every two weeks to prevent Bitcoin supply from drying up too quickly, affecting its price. Difficulty is represented by a relative number analogous to the average number of hash attempts needed to find a nonce. Mining difficulty automatically adjusts by changing the required number of starting zeroes in a block's hash, with a target block validation rate of one block every 10 minutes. Requiring one more zero exponentially increases the number of hashes required to mine a block. Higher difficulty favors the miners with the fastest equipment and largest operations. In order to compete, many smaller miners form mining pools, or nodes by combining resources to increase the likelihood of winning blocks. The difficulty tends to change during periods of high Bitcoin interest as more miners join the network or new resources are allocated to mining, but can also decrease when regulatory events cause mining operations to close or reduce.

Once a nonce is found by a miner (or mining pool), it broadcasts a completed block to the network. A node that receives this message will run the block through a hash function to check the starting zeroes thereby validating the nonce. The validation is then relayed into the network. Once most of the network agrees on the block by checking the starting zeros, the block is finalized and added to a nodes blockchain rendering it immutable.

This report is intended for Shipin Xie. Unauthorized redistribution of this report is prohibited.

## SHORTCOMINGS OF BITCOIN

Despite its popularity, Bitcoin also suffers from a number of problems.

### ***Scalability***

The data storage capacity of a block is limited to 1MB, meaning only a set number of transactions can be included in a block. Combined with the limited block generation rate, this implies the Bitcoin network can only process seven transactions per second (TPS). The slow processing speed is a common criticism of Bitcoin's potential scalability as a currency, as network congestion could lead to significantly higher fees and longer wait times for pending transactions. Furthermore, higher trading activity in the network leads to higher fees for processing pending transactions. As a comparison, Visa processes around 24,000 TPS. The fastest alternative cryptocurrency networks – Polygon and Solana – rival payment processors' speed at 65,000 and 50,000 TPS, respectively, making them better suited for everyday commercial transactions.

### ***Energy Consumption***

Proof-of-work mining is intended to require computational effort – naturally causing mining operations to consume large quantities of electricity. Most modernized mining operations run on renewable energy like hydropower or nuclear energy. Although individuals can mimic the setup on a smaller scale at home for lower profits, economies of scale are heavily favored in the process. The vast consumption of energy has led to an outcry from climate activists. Bitcoin's total estimated yearly energy consumption is 121-terawatt hours of electricity per year – roughly 0.55% of total global electricity production – rivaling that of smaller countries. Tesla CEO Elon Musk cited Bitcoin's detriment to environmental goals when he reversed a policy of accepting Bitcoin payments for cars. Each Bitcoin transaction consumes a staggering 1,173 Kilowatt Hours (kWh) of electricity, or enough to power an average US household for six weeks<sup>8</sup>. As shown in Figure 9 Comparison of Bitcoin's Electricity Consumption and Cost Per Transaction to Other Cryptocurrencies, other cryptocurrencies consume materially less electricity.

<sup>8</sup> See <https://www.moneysupermarket.com/gas-and-electricity/features/crypto-energy-consumption/> for more detail.

**Figure 9 Comparison of Bitcoin's Electricity Consumption and Cost Per Transaction to Other Cryptocurrencies**



Source: Moneysupermarket.com

It is worth highlighting that Bitcoin's carbon footprint cannot be accurately estimated, because consumption is split between clean and dirty energy sources. Carbon footprint played a major role in China's outright ban of crypto mining, as 57% of China's electricity production comes from coal-fired power plants<sup>9</sup>. On the other hand, the carbon footprint of hydro-powered mining operations is different from those powered by fossil fuels. Regardless, Bitcoin undeniably consumes unnecessary, excessive, and wasteful electricity. Other types of consensus mechanisms, such as the newer and more popular proof-of-stake, do not require the entire network to calculate hashes at once. Instead, only a single node assembles a block without the need for a nonce. The single node or minder is selected using a bidding process requiring a fraction of proof-of-work's electricity consumption.

### ***Store of Value Property***

A store of value is any commodity, currency, or asset which maintains its value over a long period of time (or even appreciates) and can reliably be exchanged. Gold, owing to its defensive nature in economic crises, is seen as the ultimate store of value asset. Cash, although losing value during

<sup>9</sup> ibid

inflationary periods, is also considered a store of value. While Bitcoin is increasingly viewed as a store of value, a major issue is its price volatility. Bitcoin's price often spikes and collapses by more than 50% in short periods of time. Most recently, Bitcoin's price fell by 50% within two months from its November 2021 peak.

Despite the volatility, runaway inflation has prompted a loss of faith in numerous fiat currencies. Turkey, for example, has seen a surge in Bitcoin and cryptocurrency interest as its financial issues nearly halved the value of the lira in 2021. To the chagrin of its government, Turkish crypto transactions volume multiplied 15-fold in 2021 compared to the prior year<sup>10</sup>. Wealthy Ukrainians also flocked to cryptocurrency exchanges leading up to Russia's invasion in February to exchange their hryvnia. Ukraine is the fourth most crypto-savvy country in the world according to the Global Crypto Adoption Index. While seen as a less than ideal store of value by most investors, cryptocurrency is the only option available for some investors.

This report is intended for Shilin Xie. Unauthorized redistribution of this report is prohibited.

---

<sup>10</sup> See <https://go.chainalysis.com/2021-geography-of-crypto.html> for details in Chainalysis's report.



## ALTCOINS

Given the massive supposed allure of Bitcoin, thousands of imitations – dubbed altcoins – have sprung up. All cryptocurrencies use blockchain. Altcoins attempt to address the shortcomings of Bitcoin in different ways. Litecoin's proof-of-work, for example, provides similar security with less electricity consumption than Bitcoin, by relying on computer memory rather than processing speed to mine. Polkadot alternatively allows developers to create separate blockchains piggybacking off of the Polkadot P2P network's security. Because there are far too many altcoins to name in this report, we will only cover Ethereum and Dogecoin, two coins with the highest name recognition (see [Multifactor Risk Models for Cryptocurrency](#) for details on other coins).

## ETHEREUM

After digital decentralization was borne out of Bitcoin, blockchain's value in other applications was quickly recognized. The Ethereum network, created in 2013 by Vitalik Buterin, is a distributed network of computers storing the Ethereum blockchain. Unlike Bitcoin, Ethereum was not developed solely as a currency, but rather as a versatile DIY platform for independent developers to create decentralized programs (see Buterin, [2014], available [here](#)). The Ethereum network has its own tradeable currency called Ether (ETH). By market capitalization, Ether is the second largest cryptocurrency and largest altcoin. Its price reached its all-time high in November 2021 at \$4,865.57. Ether's market cap grew nearly 650% from January 2021 to its November high of \$570 billion. Its current market cap is about \$400 billion.

In Bitcoin's case, the blockchain only holds transaction data. Each transaction's elements represent the simple transfer of ownership of Bitcoin. Therefore, each transaction contains: the signature of the sender, the address of the recipient, and a cryptographic hash or link to the previous transaction. Recall that a Bitcoin block is a 1MB package of transactions which contains a nonce. A blockchain is a linked chain of blocks.

Ethereum's blockchain similarly stores transaction data, but transactions have an optional field to store programmable code. As a result, Ether is programmable money, which can be sent conditionally. A large, decentralized supercomputer called the Ethereum Virtual Machine (EVM) utilizes computing resources from nodes in the network to provide processing power for the code to execute. Ether is mainly used to pay for transaction fees (called gas fees) to use the EVM's processing power but is also traded for speculation.

### Smart Contracts

Two types of public addresses exist in the Ethereum network. User accounts like Bitcoin addresses exist for individuals to buy and sell Ether. However, autonomous wallets which receive messages or transactions can redirect payments to others based on arbitrary code. Developers use this code to program anything from conditional smart loans to video games paying out cryptocurrency for achievements. These autonomous wallets are called smart contracts and are the baseline for Ethereum's possible applications to the real world. A defining feature is the ability to lock away funds temporarily until a condition is met.

Legal contracts rely on a series of written logical statements enforced by a court. On the other hand, smart contracts attempt to digitize enforcement by replicating logistics and enforcement within code. Smart contracts are not digital documents – they are essentially small computer programs stored in the

blockchain which execute when certain events are triggered. They are coded in Solidity, an Ethereum-specific, object-oriented language for implementing smart contracts. Anyone can program smart contracts but deploying them on the EVM requires gas, an Ether-based fee. Gas fees are proportionate to the amount of computational processing power required to run a Solidity program. The greater the computational processing, the higher the gas fees. Therefore, developers are incentivized to write computationally efficient code.

Like Bitcoin transactions data, contract code is open-source and publicly viewable in the Ethereum blockchain, increasing transparency and reducing errors. Smart contracts are self-executing, meaning their code controls when payment is disbursed. This enables trusted transactions and agreements to occur without a centralized authority or legal system. Smart contracts are also immutable; much like transaction data for Bitcoin. A contract's code cannot be altered once it is added to the blockchain. However, users may be subject to smart contract risk. Erroneous code has the potential to exploit user funds potentially rendering them unusable. A smart contract cannot be modified, even after an error is discovered. This is a significant drawback of smart contract structures. Overall, smart contracts serve as the backend of decentralized applications, or dapps.

### **Dapps**

Typical applications web and social media applications, like Facebook or YouTube, run mostly server-controlled code. This gives the owner full authority over the application and its usage. Twitter, for example, may ban a user from using its platform or delete existing posts to censor content. Ethereum was created to give developers tools which are free from control and interference by a single, central authority – even by its creators. Dapps is a general term for any application whose underlying code uses smart contracts on a blockchain network.

Ethereum is the second most popular cryptocurrency network and the first platform available for developing and hosting dapps. Most existing dapps today run on Ethereum's blockchain because application templates and development kits are readily available. In the context of Ethereum, dapps combine a back-end smart contract (i.e., blockchain) with a public, front-end user interface. The user interface, which may look like any standard application, can be integrated with smart contracts. The versatility of the user interface and underlying smart contract have opened countless possibilities for dapp developers – from decentralized gaming to finance and even social media applications.

### **Proof-of-Stake**

Ethereum's consensus mechanism for validating blocks is currently the same as Bitcoin's proof-of-work. With proof-of-work, gas fees increase as the network gets congested. The Ethereum network is currently undergoing a transition to a new consensus mechanism called proof-of-stake, slated to complete this year<sup>11</sup>. Proof-of-stake has become a standard for blockchain consensus mechanisms as it is far more environmentally friendly and processes transactions significantly faster. While the Ethereum network currently handles 15 TPS, it is expected to increase to 100,000 TPS once the transition is complete. This would allow for more dapps to run on the EVM.

Instead of relying on sheer computing power to mine blocks, proof-of-stake utilizes a random selection process for picking validators. Nodes have to stake a minimum amount of cryptocurrency (32 ETH required in Ethereum's case) in order to become eligible to validate blocks. Staking cryptocurrency means offering up an amount of crypto from one's wallet as collateral – locking it away in a smart

<sup>11</sup> See <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/> for more about Ethereum's transition to proof-of-stake.

contract for a certain period. The Ether is locked until a validator is randomly chosen from among the eligible nodes. The likelihood of being chosen depends on the size of one's stake. Like winning a lottery, the chance of being selected increases as you buy more tickets. One node is randomly chosen among all eligible candidates to validate the block and receive a reward. The node is incentivized to create the block honestly because approving a falsified transaction will cause the staker to lose all their staked money if the rest of the network finds an error when cross-referencing with their own copies.

Using Bitcoin's proof-of-work topology, anyone can attempt to create a block from the mempool. However, only one node will succeed, while other nodes may consume energy only to fail to find the nonce. The proof-of-stake topology rewards the privilege to form a block using a lottery-like selection process. If a node is granted this privilege, they can form the block or choose not to – losing their stake. If they choose to form a block, then they must gather transactions from the mempool, validate their digital signature, package the transactions into a block, and broadcast to the network.

The difference in energy consumption between proof-of-work and proof-of-stake stems from who performs the validation. In Bitcoin, all miners in the network compete to earn the right to validate, performing calculations at the same time – thus, the entire network is expending electricity at once. Proof-of-stake models require no hash calculations to validate, and only a single validator chosen gathers transactions from the mempool and assembles a block. It is more accurate to say proof-of-stake blocks are forged than mined, as no energy is expended to validate them. Since there is no wait time for a nonce, validators are chosen, and blocks are created in significantly less time than proof-of-work models. Peers check the validated block in the same manner as Bitcoin except block hash values have no set criteria.

The validator's stake serves as an incentive to correctly validate blocks – any node which validates transactions determined to be fraudulent by the network will both lose their stake and the right to stake in the future. Furthermore, part of the lost (known as slashed) stake is rewarded to the node which first detected such a fraudulent transaction, incentivizing honest checking of blocks by the network. While the minimum stake is 32 ETH or around \$100,000 at the time of writing, this cost can also be split among a large pool of nodes. Through smart contracts, staking pools have been developed which automatically aggregate and stake investors' money, dividing rewards among participants based on their share of the pool. Proof-of-stake is relatively more accessible than proof-of-work since the upfront investment of validating is liquid and substantially smaller. Unlike Bitcoins, Ethereum validators do not need to purchase computing devices for massive mining farms which cannot be easily re-sold. Stakers can also remove their locked Ether to stop staking at any point, giving up rights to validate blocks.

## DOGE COIN

Dogecoin is a cryptocurrency created in 2013 by software engineers Billy Markus and Jackson Palmer as a Bitcoin imitation based on a popular Shiba Inu-dog "meme". Accordingly, it was dubbed the first memecoin. Despite its name and logo coming from a meme, the underlying technology of Dogecoin closely mirrors Bitcoin with its own peer-to-peer network and proof-of-work consensus. All peers in the Dogecoin network carry a copy of its blockchain ledger and validate transactions through mining. Dogecoin transactions, however, are faster than Bitcoin – taking only one minute to validate new blocks on the Dogecoin blockchain compared to Bitcoin's 10 minutes. Furthermore, its supply has no lifetime cap (unlike Bitcoin's cap of 21 million coins), which encourages spending in transactions rather than long-term holding.

In its early years, Dogecoin was primarily used for ‘tipping’ users on social media platforms such as Reddit and Twitter for performing good deeds. However, it has since become one of the most widely known cryptocurrencies as a result of social media influencers<sup>12</sup>. Tesla CEO Elon Musk fueled its rocketing price by referencing the coin on Twitter (see Figure 10 Tesla CEO Elon Musk promoting Dogecoin on Twitter). Dogecoin also has the largest community following among all cryptocurrencies on Reddit, except for Bitcoin. In 2021, Dogecoin soared over 9,200% to an all-time high of \$0.7376 on May 8<sup>th</sup>, when Musk praised Dogecoin on an episode of Saturday Night Live.

**Figure 10 Tesla CEO Elon Musk promoting Dogecoin on Twitter**













Source: Elon Musk's Twitter account @elonmusk

While the Dogecoin craze has largely died down, its legacy still shines from spreading intrigue in crypto like wildfire in 2021. Its meteoric rise embodies the volatility and flash opportunities in the crypto world, with countless coins having broken headlines and fallen back into obscurity overnight. Other memecoins have spawned to capture similar hype from retail investors, such as Shiba Inu (SHIB) coin or Dogelon Mars (ELON) – a mashup of Doge, Elon Musk, and going to Mars. In October 2021, Shiba Inu's market cap rose past Dogecoin's, and retail investors continue to monitor Reddit and Twitter daily for opportunities to catch the next Doge. Investors looking to gain crypto exposure may want to stay abreast of major influencers' social media pages. Figure 11 Altcoins to Know and Defining Features highlights a few other notable, high market cap altcoins.

<sup>12</sup> See <https://www.wsj.com/articles/what-is-dogecoin-how-to-say-it-and-why-its-no-longer-a-joke-thanks-elon-11612820776>

**Figure 11 Altcoins to Know and Defining Features**

	Cryptocurrency	Ticker	1M high price	Market Cap (billions USD)	Creation date	Note
	Bitcoin Cash	BCH	\$352.00	\$5.1B	Aug-17	"Hard fork" or direct spin-off of Bitcoin optimized for fast transactions with low fees. Block size is 32MB compared to Bitcoin's 1MB.
	Binance Coin	BNB	\$440.64	\$61.1B	Jun-17	Used to pay transaction and trading fees on crypto exchange Binance with a 25% discount. Can purchase tokenized stocks and ETFs on the Binance Chain platform.
	Ripple	XRP	\$0.80	\$28.7B	Jun-12	Currency for RippleNet payment platform, a real-time gross settlement system for global transactions.
	Solana	SOL	\$122.25	\$27.2B	Mar-20	Programmable blockchain like Ethereum offering greater scalability. Aims to provide low fee (< \$0.01) dapp and DeFi solutions.
	Avalanche	AVAX	\$90.25	\$15.0B	Sep-20	Dapp platform aiming to unseat Ethereum as host for smart contracts. Unique architecture with three blockchains for transactions, smart contracts, and block validation.
	Terra	LUNA	\$109.39	\$26.9B	Jan-18	Famous for Stablecoin TerraUSD (UST), created to facilitate mass adoption of price-stable cryptocurrencies.
	Cardano	ADA	\$1.10	\$26.1B	Sep-17	Open-source project requiring new technology to undergo peer-review research process. Reduces potential fraud and erroneous smart contract programming.
	Polkadot	DOT	\$20.62	\$13.9B	Oct-17	Designed to facilitate cross-blockchain transfers of data to support a decentralized version of the world wide web.
	Algorand	ALGO	\$0.81	\$4.3B	Jun-19	Designed to solve the blockchain trilemma of achieving speed, security, and decentralization all-in-one. This is the platform used to host the Central Bank Digital Currency (CBDC) of the Marshall Islands.
	Monero	XML	\$288.82	\$3.7B	Apr-14	Open-source, privacy-based cryptocurrency launched as a completely private alternative to Bitcoin. Notably delisted from many major exchanges and associated with criminal dark money.
	Fantom	FTM	\$1.38	\$2.3B	Jun-18	Platform for scalable, low transaction-time DeFi solutions. Transactions settled in 1-2 seconds with fees lower than a cent.

Source: CoinMarketCap



## TOKENS

Cryptocurrencies are categorized as either coins or tokens. Thus far, we have covered primarily coins. A token, on the other hand, is a digital representation of an asset, which is exchanged using an existing blockchain network. Tokens are also tradeable and fluctuate in price like coins. Coins are the native asset of a blockchain, while tokens do not have a standalone blockchain. Coins represent currencies – a store of value and medium of exchange, but tokens have many other applications. Although bought and sold like coins, tokens do not attempt to replace currencies in commercial use. All coins are tokens, but not all tokens are considered coins. At the basic level, the key difference between the two is merely based on their utility. If an investor wants to make a simple transaction, coins are best. On the other hand, if it is a service, utility tokens can be used.

Most tokens are associated with a dapp project (also known as dapp tokens) and exist for developers to grow their project by raising funds from sales (see Catalini and Gans, [2018], available [here](#)). CoinGecko, a coin data aggregator, lists over 11,000 cryptocurrencies available – most of which are tokens on Ethereum and other programmable blockchains like Avalanche or Solana which aim to raise funds for project teams. Basic Attention Token (BAT), for example, is a tradeable token rewarded to users for watching advertisements through a custom web browser called Brave. Investors should be aware that a substantial portion of tokens available are fraudulent projects.

Tokens come in three forms: security, governance, and utility.

- **Security tokens.** These tokens are akin to a digital share representation of equity. Purchasing security tokens is like owning a share in a company, as it finances the company in exchange for profit sharing.
- **Governance tokens.** These give buyers voting rights towards decision-making for a project. Voters' individual power is determined by their share of the governance tokens in circulation. Uniswap token, one of the largest tokens by market cap, gives buyers a right to vote on the future of the Uniswap DEX protocol as illustrated in Figure 12 Uniswap Governance Portal Where Token Holders Vote to Change the Protocol.
- **Utility tokens.** Utility tokens represent access to a product or service in a particular digital ecosystem. They can be redeemed with the issuer for a specific product or preferential treatment on a platform. Decentraland (MANA) is an example of a utility token on the Ethereum blockchain. MANA is used to purchase virtual real estate and goods in the Decentraland metaverse – a video game-like virtual world for socializing.

**Figure 12 Uniswap Governance Portal Where Token Holders Vote to Change the Protocol**

Hi UNICorns, welcome to the Uniswap Governance Forum!

Here is a quick outline of how the governance process works:

1. Submit a forum post ([Proposal Discussion section](#)).
2. Get in touch with [Uniswap Discord Admins](#) to discuss your proposal in a community call and on Twitter Space as well.
3. Create another forum post in the Temperature Check section and publish a [snapshot](#) (temperature check) vote with 2-5 days voting time. This action requires at least 1K UNI tokens [delegated or self-delegated](#). For the snapshot to be valid, at least 25k UNI should participate. **Please, provide TLDR process update on the top of your proposal so it is more easily accessible.**
4. Update the temperature check post with the community feedback.
5. Publish a [snapshot](#) (consensus check). This action requires at least 1K UNI tokens delegated or self-delegated. The snapshot would be deemed valid if at least 50K UNI participates.

[all categories ▾](#)

Latest Top Categories

Topic	Replies	Views	Activity
<p><b>Community Governance Process</b></p> <p>This document is a suggested process for developing and advancing Uniswap Governance Proposals. It is a living document intended to be owned, modified and enforced by the Uniswap community. Note: Autonomous proposals ar... <a href="#">read more</a></p>	21	15.0k	Dec '21
<p><b>Uniswap Governance Forum Rules</b></p> <p>This forum is dedicated to discussions on Uniswap governance. Relevant topics include: Governance Proposals Proposal Discussions Delegation Pitches Site Feedback This is not the place for: UNI price discussion Gener... <a href="#">read more</a></p>	2	4.3k	Sep '20

Source: [Uniswap governance portal found at gov.uniswap.org](https://gov.uniswap.org)

Crypto tokens are minted and sold with Initial Coin Offerings (ICOs) to fund a project, akin to an Initial Public Offering (IPO). They are mainly for private crypto startups hoping to receive funding and a pathway to capital from a wider range of investors. ICOs, also known as crowdsales, offer a potentially lucrative method of crypto asset investing, subject to extreme risk. Due to lack of ICO regulation and oversight, fraudulent projects, minting of more coins than promised, and “rug pulls” from developers taking the money and running are rampant scams seen in this segment of the crypto space.

In the ICO process, a startup company will release a white paper outlining the scope and roadmap for its project along with a funding goal. If the funding goal is not met through the crowdfunding, all funds are returned to the backers. If the goal is met, the company receives the money and will develop the project. Web browser company, Brave, raised its goal of \$35 million through an ICO by selling 1 billion Basic Attention Tokens (BAT). The Ethereum network is the most popular platform for tokens as most tokens are categorized as ERC-20 – a standard for programming Ethereum tokens.

## STABLECOINS

Cryptocurrencies are often being criticized for their speculative nature and extreme volatilities. As a result, a relatively new class of tokens called Stablecoins is introduced. Stablecoins can potentially provide the benefits of blockchain security and privacy with reduced price volatility. Large price swings are commonplace in the crypto world – and even fuel the get-rich-quick appeal for retail investors. Bitcoin, for instance, rose to its all-time high over \$68,000 in November 2021, then shed 50% of its value within weeks to \$35,000.

Unlike typical cryptocurrencies, Stablecoins are pegged against existing fiat currencies or commodities such as the US dollar or Euro and are typically fully collateralized with the underlying asset. Reserves for the companies behind Stablecoins may include a mix of paper dollars, cash deposits, Treasury bills, or precious metals. Backing companies retain 100% fiat collateralization to prevent arbitrage opportunities. They have mainly been used as a cash equivalent and liquidity in cryptocurrency portfolios. Although Stablecoins are backed by fiat currency, they are not necessarily directly redeemable for conventional currencies by their issuers. An issuer may or may not choose to offer convertibility to cash. Furthermore, liquidating Stablecoins at a cryptocurrency exchange still incurs fees.

The six most popular Stablecoins are Tether (USDT), USD Coin (USDC), Binance USD (BUSD), Dai (DAI), TerraUSD (UST), and TrueUSD (TUSD). All six are presented pegged 1:1 to the US Dollar – there is one unit of government reserve currency or an equivalent backing each coin. The popularity of Stablecoins has grown significantly since 2020. The combined market cap of all Stablecoins rose nearly thirty-fold from \$6 billion in January 2020 to over \$170 billion by January 2022.

This report is intended for Shubin Xie. Unauthorized redistribution of this report is prohibited.

## CRYPTOCURRENCY INVESTING

In this section, we briefly introduce the basic mechanisms of cryptocurrency trading, main products, exchanges, and related ETFs.

### WALLETS AND CUSTODY

The most popular method of investing in the crypto world is to simply trade in the spot market. To buy and hold any cryptocurrency, one needs a public key, or wallet for the respective network. A wallet is a colloquial term. It represents a piece of software which generates a pair of cryptographic private and public keys to send and receive crypto. Sending cryptocurrency generally only requires entering a passcode to the software, a transaction amount, and the recipient's address. Balances are calculated by cumulating the total coins in the blockchain transferred last to the wallet. This is generally done automatically and readily displayed on a wallet's user interface. The range of wallet software and services available is broad, so investors should consider two main aspects in choosing wallets: the storage type and the custody of its private key. As shown in Figure 13, the number of unique Bitcoin wallet addresses on the blockchain has been fluctuating around 600,000 to 700,000 in recent years.

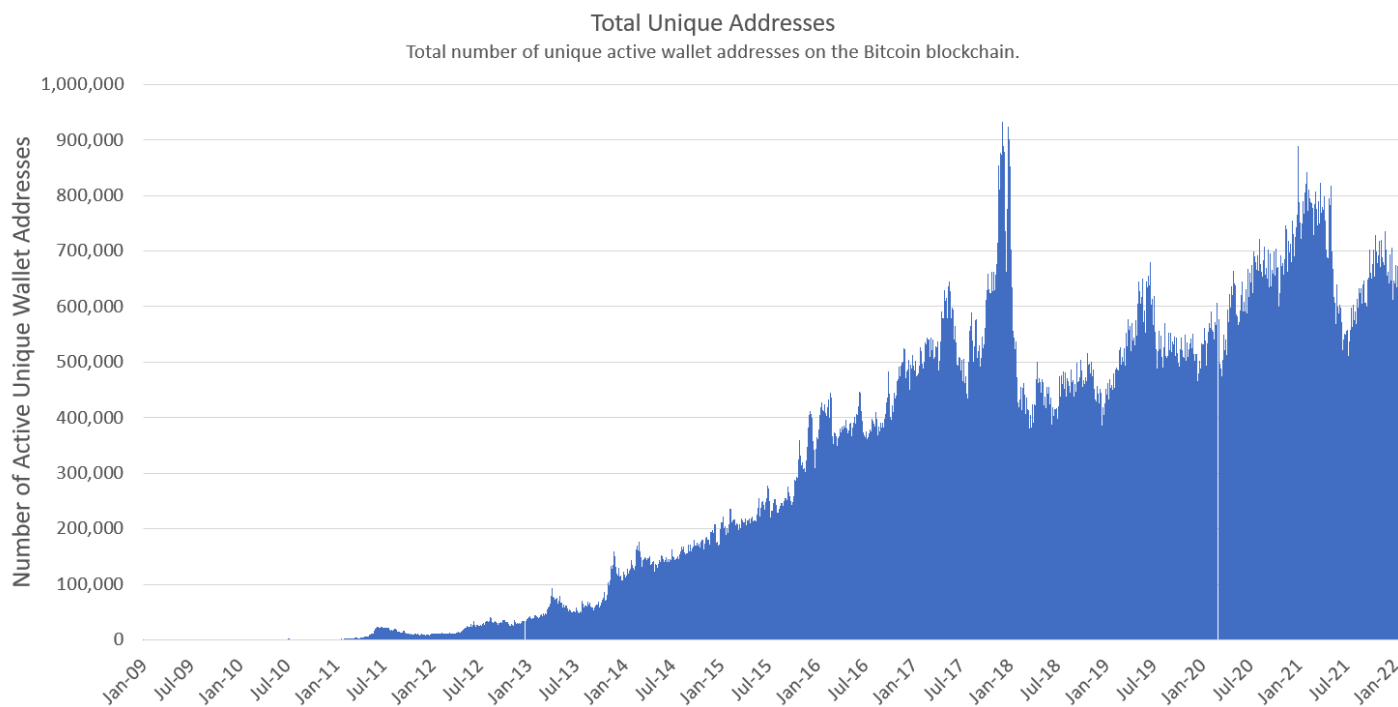
Wallets are either hot storage or cold storage, depending on whether the private key is stored online or offline<sup>13</sup>. Hot storage wallets are always connected to the internet, while cold storage ones are kept offline (they are briefly connected to the internet for unlocking coins). Wallet services found on the web or mobile apps are generally hot wallets – these are generally easier to set up and suited to everyday use but are more susceptible to cyber theft. On the other hand, cold wallets store keys in a USB stick or hard drive and are significantly more secure from cyber theft – they might be impractical for everyday use, and oriented to long term storage of crypto. Their usage can be compared to checkings and savings accounts, whereas a hot wallet should hold daily spending and a cold wallet store away the bulk of crypto assets.

Wallets are also considered either custodial or non-custodial<sup>14</sup>. The idiom “Not your keys, not your coins” circulates the crypto world as a forewarning against custodial wallets. Custodial means a third party controls your wallet's private keys. The benefit of custodial wallets lies in its convenient setup (typically requiring only an email address) and lower responsibility in securing keys, but the reputation of the custodian is paramount. Most custodial wallet services are still susceptible to cyber-attacks. Non-custodial wallets are those in which the investor holds the wallet's private key. Users with non-custodial wallets have full responsibility over private keys. Users have no means of recovering funds if the private key is lost or stolen.

<sup>13</sup> See <https://www.gemini.com/cryptopedia/crypto-wallets-hot-cold> for more on hot v. cold wallets.

<sup>14</sup> See <https://www.gemini.com/cryptopedia/crypto-wallets-custodial-vs-noncustodial#section-custodial-crypto-wallets-pro-and-cons> for more about wallet custody.

**Figure 13 Unique Bitcoin wallet addresses on the Blockchain**



Source: Blockchain.com

The most popular crypto wallet for Ethereum, MetaMask, is browser extension-based and allows users to directly exchange fiat currencies for cryptos. Experienced individual investors generally prefer non-custodial wallets. For institutions, there are custody service providers who securely hold assets in a combination of cold and hot storage, taking the trouble out of the process for hedge funds and asset managers<sup>15</sup>. Institutions with high AUM who value security will likely wish to opt for a custodial cold storage wallet service with loss insurance. Custodial services are provided by most major cryptocurrency exchanges such as Coinbase and Kraken. ETFs and trusts investing directly in crypto commonly entrust assets to a custodial cold storage provider.

## PURCHASING CRYPTOCURRENCIES

Bitcoin and Ethereum are only two out of thousands of cryptocurrencies offering highly lucrative investment opportunities. Centralized exchanges (CEXs) are the main platforms to directly exchange fiat currencies for popular cryptos and tokens. Depending on which exchange is used, there may be between a handful to hundreds of coin varieties available to purchase. Crypto-to-crypto, crypto-to-token, and token-to-token exchanges are all available. Exchanges are the starting points for investors who desire direct exposure to an underlying cryptocurrency.

Online brokers such as Robinhood, WeBull, and Interactive Brokers offer platforms for investing in cryptocurrencies. The convenience of a mobile application and simplified user interfaces make these brokers particularly attractive for retail investors. A key benefit of using brokers to trade cryptocurrencies

<sup>15</sup> See <https://www.investopedia.com/news/what-are-cryptocurrency-custody-solutions/> for more about crypto custodial solutions.



is lower fees. Broker commission fees are typically lower than exchange trading fees. However, most brokers do not allow users to directly hold cryptocurrencies – instead custodians are commonly used. In addition, the selection of coins available by online brokers is limited to popular coins like Bitcoin, Ethereum, and Dogecoin.

For individual investors purchasing crypto to hold directly, users usually create an account on an exchange website. This typically includes know-your-customer (KYC) identity verification and a phone number or email for Two-Factor Authentication. The exchange generates a new crypto wallet for the user or allows an existing wallet to be linked. Funds can be deposited by transferring fiat currency through bank wire, direct transfer, credit card, or money order. Users may buy, sell, and hold cryptocurrencies freely. Exchanges also allow users to place either market or limit orders. Most exchanges also offer an API for high frequency traders, enabling automated trading.

For institutions, most major exchanges have over-the-counter (OTC) desks for high volume crypto trading. Fees for OTC trades vary between 0.1% to 1% of transaction volume. In combination with custodial cold storage services, partnering with an exchange offering OTC trading takes most of the heavy lifting of managing cryptocurrency away from institutional investors, who can then focus on crypto investment ideas.

### *Shorting*

Margin accounts on crypto exchanges offer outlets for shorting cryptocurrencies. For margin trading, individuals must register a separate margin account on an exchange like Binance or Kraken. Opening a margin account typically incurs a fee. Similar to stock lending, shorting on margin trading is possible by borrowing crypto from other users.

An alternative, less common pathway to expressing a negative view on crypto is the use of leveraged tokens. Leveraged tokens allow investors to gain leveraged exposure. Unlike traditional products, these tokens do not maintain a fixed amount of leverage. Instead, they maintain a range of leverage typically between 2.0x to 4.0x. Their price movements are tied to an underlying cryptocurrency's perpetual swap contract price. Leveraged tokens come in two versions for each cryptocurrency – long and short tokens<sup>16</sup>. Short tokens are analogous to inverse ETFs. Purchasing the short token gives an investor leveraged exposure to the underlying cryptocurrency's swap contract on the short side.

### *Stocks and other Equity Products with Significant Crypto Exposures*

Some companies choose to either directly hold or have other direct exposures to cryptocurrency. Common stocks and other equity products (e.g., ETFs) are easy to hold, trade, and short. Therefore, investors can gain exposure to crypto via these stocks. We have a model called the Bella (Bitcoin Exposure Language Learning Analysis) and a data feed on these stocks (see [Measuring Stock-Level Exposure to Bitcoin](#) for details).

### *Cryptocurrency Derivatives*

While virtually all exchanges offer spot trading for cryptocurrencies, investors may wish to gain exposure without holding the underlying asset. Furthermore, investors with traditional portfolios exposed to crypto may want to hedge the risk. Whether investors want to speculate on future prices or wish to offset risk, crypto-based derivative products offer a potential solution. The popularity of crypto

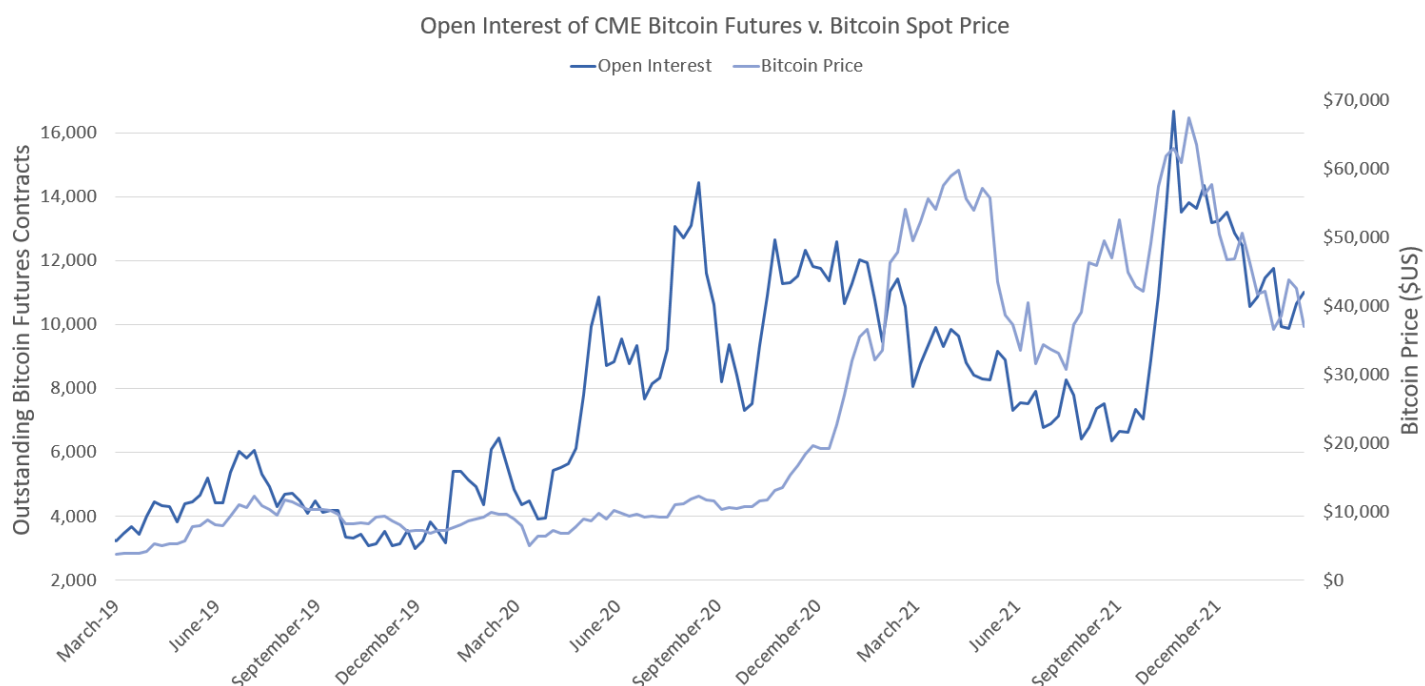
<sup>16</sup> See <https://www.binance.com/en/blog/all/your-essential-guide-to-binance-leveraged-tokens-421499824684900580> for more about Leveraged Tokens.

derivatives has grown after the October 2021 launch of the ProShares Bitcoin Strategy ETF (BITO) investing in Bitcoin futures<sup>17</sup>.

### Futures contracts

Cryptocurrency futures contracts allow investors to buy crypto at a certain price at a future expiration date. Regulated Bitcoin-based futures contracts have been available to investors since December 2017, first introduced by the CBOE Options Exchange group. They function in virtually the same manner as traditional futures contracts and are regulated by the Commodity Futures Trading Commission (CFTC). The Chicago Mercantile Exchange (CME) group released futures contracts shortly after CBOE in 2017. CBOE has since stopped offering cryptocurrencies futures, but CME futures are still available. Open interest in CME Bitcoin futures contracts reached an all-time high in November 2021, with over 16,000 outstanding (see Figure 14 Open Interest in Chicago Mercantile Exchange BTC futures and Bitcoin Spot Price).

**Figure 14 Open Interest in Chicago Mercantile Exchange BTC futures and Bitcoin Spot Price**



Source: CFTC Commitment of Traders, Bloomberg, Wolfe Research Luo's QES

### Options

Options trading is a growing segment of crypto investing. Bitcoin and Ethereum options operate fundamentally the same as traditional call and put options but with a digital coin as the underlying asset. Institutions with exposure to crypto-exposed equities can employ options to hedge. Monthly trading volume of Bitcoin options peaked in April 2021 at \$35 billion. Options could potentially limit downside risk (or lock in gains) from stocks like MicroStrategy Inc (MSTR) or Galaxy Digital Holdings (GLXY).

<sup>17</sup> See <https://www.bloomberg.com/news/articles/2021-10-20/proshares-bitcoin-etf-tops-1-billion-in-assets-in-just-two-days> for more.

These corporations regularly top our Bitcoin Exposure Screen<sup>18</sup>. Options can be traded on several major cryptocurrency exchanges like Binance, OKEEx, and FTX.

### *Perpetual Swaps*

A perpetual swap contract is a relatively new type of derivative product which has grown popular among retail investors. They function like futures contracts. However, unlike futures, perpetual swaps do not have expiration dates. The contract price is pegged to the spot price of the underlying asset and constantly adjusts<sup>19</sup>. A funding rate mechanism exists which requires traders to continually settle the contract. Retail investors use up to 125x leverage to trade perpetual swaps, amplifying their gains or losses.

## **CRYPTO EXCHANGES**

There are roughly 380 crypto exchanges available globally. Investors should consider several relevant aspects when choosing an exchange.

### *Cybersecurity*

Due to their large crypto holdings, exchanges are prime targets for cyber theft<sup>20</sup>. The first major hack on a crypto exchange occurred in February 2014. Mt. Gox, a Japan-based Bitcoin exchange, announced that it lost \$350 million worth of Bitcoins, or roughly 850,000 BTC (valued at \$36 billion today). Other notable crypto exchange hacks have affected the likes of Binance, Bitfinex, and KuCoin. However, ample improvements to security measures have been implemented since. The hallmark of a superb crypto exchange is its state-of-the-art cybersecurity to protect its users' holdings and personal information. Several top crypto exchanges also started to have crime insurance to protect cybersecurity losses.

### *Fees*

Exchanges typically charge deposit, withdrawal, trading, and network fees. There is no standardization of fees among exchanges. Each exchange accepts deposits through different means, but deposit fees are typically free for direct bank transfers. Credit cards, debit cards, and PayPal deposit transactions may incur costly fees. Withdrawing an account balance to fiat currency will generally incur a withdrawal fee based on the exchange and a blockchain network-related fee depending on the cryptocurrency traded.

Trading fees for swapping between two cryptocurrencies (including crypto-to-crypto and fiat-to-crypto) vary greatly between exchanges. These fees make up the bulk of exchanges' revenue. Trading fees are typically charged based on a maker-taker model of liquidity. Traders providing liquidity (i.e., makers) typically enjoy lower fees than those who take away liquidity (i.e., takers) from the platform. The maker-taker model incentivizes placing limit orders over market orders.

Network fees are flat fees incurred when withdrawing to a bank or sending cryptocurrency to another wallet. This flat fee varies based on congestion in the network but are relatively low for high volume traders. Bitcoin transaction fees are generally below \$5 since July 2021, but occasionally jumped to \$50 during times of extreme congestion (see Figure 15 Network Fees in the Bitcoin Network). This commonly occurs around regulatory events with Bitcoin. Ethereum has comparatively high transaction

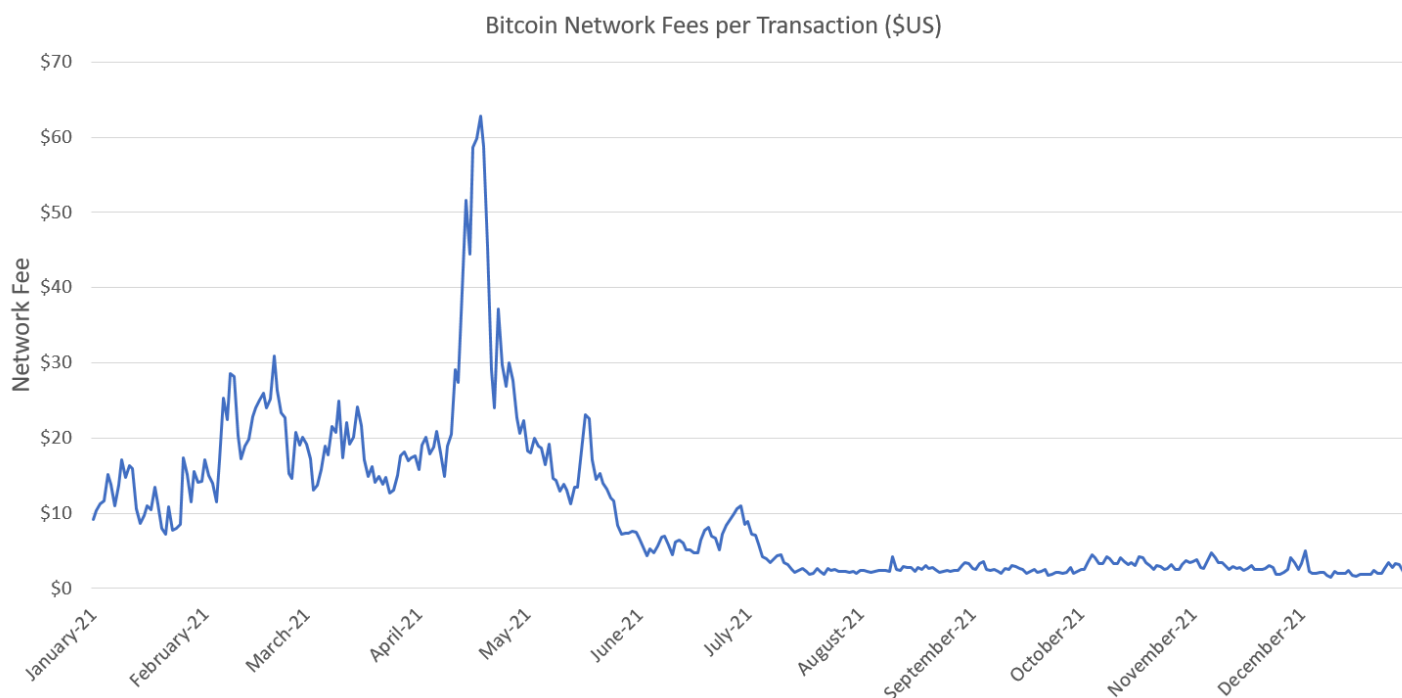
<sup>18</sup> See <https://www.coingecko.com/en/public-companies-bitcoin> for public companies holding cryptocurrency.

<sup>19</sup> See <https://www.coindesk.com/learn/what-is-a-perpetual-swap-contract/> for more about perpetual swap contracts.

<sup>20</sup> See <https://www.gemini.com/cryptopedia/mt-gox-bitcoin-exchange-hacked> for more about the history of exchange hacks.

(gas) fees, which increase as the Ethereum Virtual Machine endures greater computational stress – sometimes over \$100 per transaction. This would deter some small volume retail traders from using Ether. On a side note, lowering fees is also the reason for Ethereum’s transition to proof-of-stake. Ultimately, high volume institutions will likely be unphased by flat network fees. Instead, they should be wary of percentage-based trading fees.

**Figure 15 Network Fees in the Bitcoin Network**



Source: Blockchain.com, Wolfe Research Luo's QES









### Exchange Comparison Table

Given the various considerations to note and products available, below is a table of several popular exchanges and their features (see Figure 16 Crypto Exchange Comparison Table). Cybersecurity ratings are sourced from CoinGecko and scored based on a penetration test, proof of funds, and availability of a bug bounty.<sup>21</sup> Only seven exchanges have an AAA security score. Liquidity scores are sourced from coin and exchange data aggregator CoinMarketCap<sup>22</sup>.

<sup>21</sup> See <https://www.coingecko.com/en/exchanges?view=cybersecurity> for the full list of the 100 exchanges rated by cybersecurity.

<sup>22</sup> See <https://support.coinmarketcap.com/hc/en-us/articles/360043836931-Liquidity-Score-Market-Pair-Exchange-> for CoinMarketCap's liquidity scoring methodology.

**Figure 16 Crypto Exchange Comparison Table**

Exchange	Cybersecurity Rating	Spot Trading Fee Schedule (Maker/Taker)	Coins Available	Liquidity Score	Product Offerings	Notes
 <b>BINANCE</b>	AAA	0.10%/0.10% → 0.02%/0.04%	397	801	Spot Futures Perpetual swap Options Staking OTC Desk	Highest liquidity; low fees; fee reduced by 25% if paid in Binance Coin (BNB); advanced trading interface on international version; US version exists with fewer features but not available in several states including New York and Texas.
 <b>KRAKEN</b>	AAA	0.16%/0.26% → 0.00%/0.10%	103	747	Spot Futures Staking OTC Desk	Low fees; 95% of deposits in cold storage; targeted to experienced crypto traders; hands-on support for institutions; not available in New York or Washington state.
 <b>COINBASE</b>   Pro	AAA	0.50%/0.50% → 0.04%/0.00%	141	715	Spot OTC Desk	High liquidity; high trading fees relative to peers Coinbase is the most reputed exchange in the US and publicly listed on the NYSE; ease-of-use; advanced charting features; private client for institutions through Coinbase Prime.
 <b>CRYPTO.COM</b>	AAA	0.40%/0.40% → 0.04%/0.10%	200	631	Spot Futures Options Staking OTC Desk	Best in class security; user interface is less user-friendly; largest insurance program in industry. Not available in the US.
 <b>GEMINI</b>	AA	0.10%/0.35% → 0.00%/0.03%	100	675	Spot OTC Desk	Popular exchange partner for asset managers; Gemini Prime offering custody services and institutional trading API.
 <b>FTX</b>	BBB	0.07%/0.02% → 0.00%/0.04%	301	746	Spot Futures Options Perpetual swaps OTC Desk	Best known for an expansive array of derivatives products; low fees; no funds insurance; US version exists with fewer features.
 <b>KUcoin</b>	BBB	0.10%/0.10% → 0.0125%/0.03%	585	585	Spot Futures Staking	Extremely low trading fees; trading fee reduced by 20% if paid in KuCoin Token (KCS); no funds insurance.
 <b>OKX</b>	BB	0.08%/0.10% → -0.01%/0.025%	325	491	Spot Futures Options Perpetual Swaps Staking	Largest array of derivatives products among all exchanges; low fees; no funds insurance.

Source: CoinGecko; CoinMarketCap; Wolfe Research Luo's QES

## CRYPTO EQUITY-LINKED PRODUCTS

Instead of trading and investing cryptocurrencies directly, investors can also gain exposure to this important asset class via equity-linked products, such as ETFs and private trusts. The ability to buy and sell ETFs directly from stock exchanges offers a significant advantage to many investors.

### *Cryptocurrency-Linked ETFs*

Investors can gain exposure to cryptocurrencies without trading on a crypto exchange. Crypto-linked ETFs/ETPs can be bought and sold on traditional stock exchanges. Crypto ETPs have surged from \$3 billion at the end of 2020 to over \$20 billion by December 2021, an increase of over 500%. One of the downsides of accessing cryptocurrencies via ETPs is that investors have to pay extra management fees.

Due to SEC regulation, US crypto ETFs cannot be based on spot prices. In October 2021, the ProShares Bitcoin Strategy ETF (BITO) – the first US Bitcoin-linked ETF investing in cash-settled Bitcoin futures was launched. BITO amassed over \$1 billion in AUM within two days of its release, breaking a record previously held by SPDR's Gold Shares ETF (GLD). Since then, several Bitcoin futures ETFs have cleared SEC approval and started trading. Several other countries including Canada and Switzerland have welcomed cryptocurrency spot based ETFs such as the Fidelity Advantage Bitcoin ETF (FBTC).

In Figure 17 Crypto ETF Comparison Table, we highlight several investable crypto-related ETF/ETPs.

This report is intended for Shubin Xie. Unauthorized redistribution of this report is prohibited.



Figure 17 Crypto ETF Comparison Table

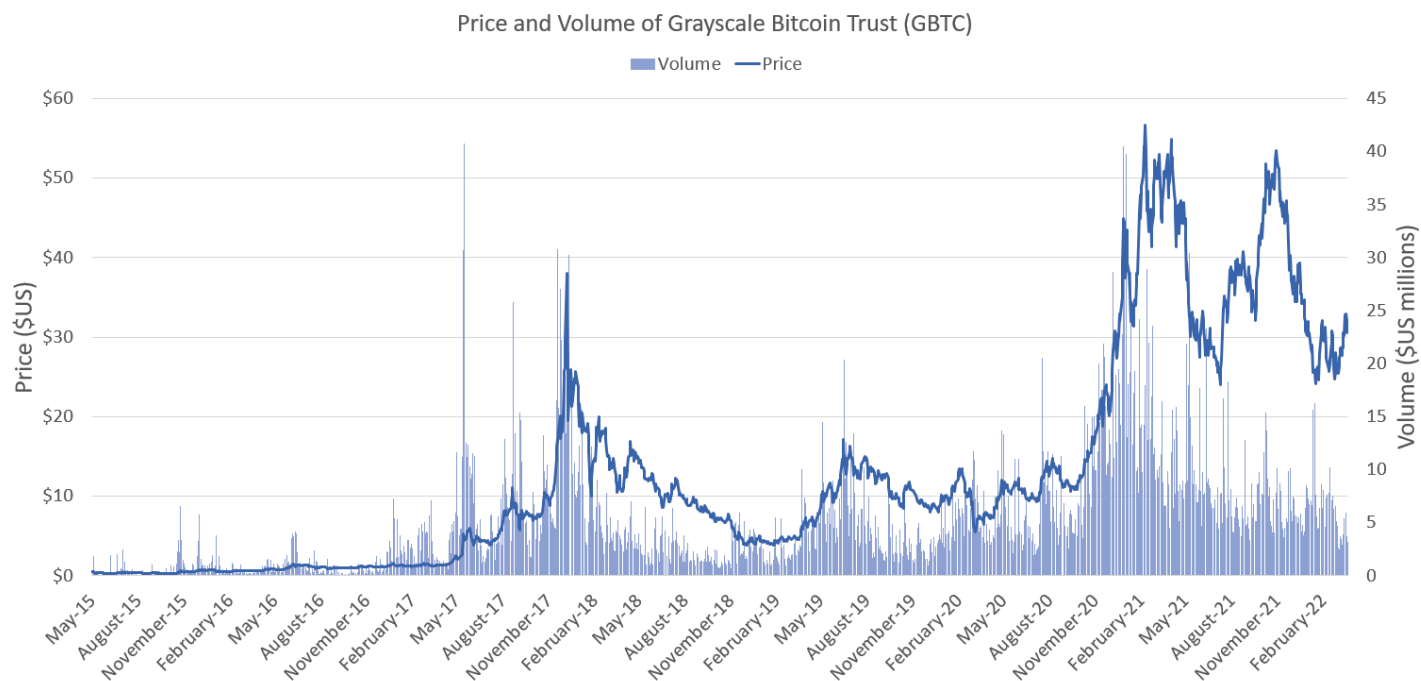
Crypto ETF/ETP	AUM (in USD)	Expense Ratio	Crypto Exposure	Exchange	Notes
ProShares Bitcoin Strategy ETF (BITO)	\$1 billion	0.95%	Bitcoin futures contracts 100%	NYSE	First Bitcoin-linked ETF available in the US; invests in Chicago Mercantile Exchange group Bitcoin futures
ETC Group Physical Bitcoin ETP (ETCE)	\$840 million	2.00%	Bitcoin 100%	XETRA	Holds physical Bitcoin directly; 100% of assets in cold storage
Fidelity Advantage Bitcoin ETF (FBTC)	\$45 million	0.40%	Bitcoin 100%	TSX	Holds physical Bitcoin tracking spot price, alternative to US derivatives-based ETFs
CI Galaxy Ethereum ETF (ETHX)	\$615 million	0.89%	Ether 100%	TSX	Holds physical Ether directly; 100% of assets in cold storage
ETC Group Physical Ethereum ETP (ZETH)	\$100 million	1.49%	Ether 100%	XETRA	Holds physical Ether directly; 100% of assets in cold storage
21Shares Crypto Basket Index ETP (HODL)	\$165 million	2.50%	Bitcoin 49.64% Ether 24.20% Polkadot 15.98% Solana 5.21% Terra 4.97%	SIX	Balanced exposure to 75% of cryptoassets market; cryptoasset share rebalances monthly to follow the ever-evolving crypto space; 100% of assets in cold storage
21Shares Solana ETP (ASOL)	\$90 million	2.50%	Solana 100%	SIX	Exposure to Solana — a cryptocurrency widely viewed as an environment-friendly competitor to Ethereum; 100% assets in cold storage
Ninepoint Bitcoin ETF (BITC)	\$60 million	1.45%	Bitcoin 100%	TSX	First carbon-neutral Bitcoin ETF; A portion of management fee offsets carbon footprint for Bitcoin holdings; 100% assets in cold storage

Source: Wolfe Research Luo's QES

### Private Trusts

One pathway for accredited investors to gain exposure to digital assets is through private trusts. A cryptocurrency trust may sell private shares to investors who qualify based on income and net worth requirements. Unlike ETFs which incur management fees and expenses commonly reaching over 2%, private trusts can hold physical cryptocurrencies. The most popular cryptocurrency trust provider is Grayscale. The Grayscale Bitcoin (GBTC) and Ethereum (ETHE) Trusts are popular among investors. The total holdings of GBTC and ETHE are over \$23.2 billion and \$8.4 billion, respectively, as of May 6, 2022.

**Figure 18 Price and Volume History of Grayscale's Bitcoin Trust (GBTC)**

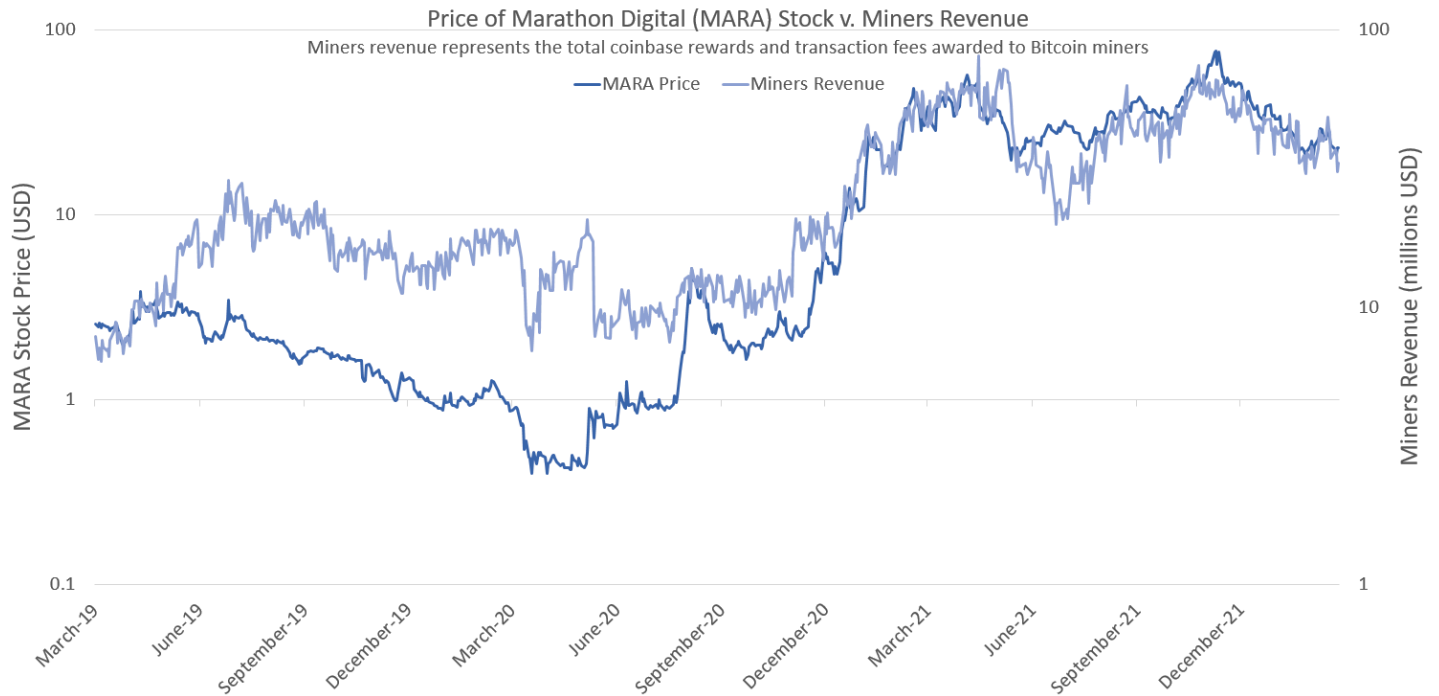


Source: Yahoo Finance, Wolfe Research Luo's QES

### ***Mining & Blockchain Technology ETFs***

Investors can also gain exposure to the crypto industry by investing in public companies with stakes in mining and blockchain applications. These companies often have crypto reserves on their balance sheets or are actively using or investing in blockchain technology. Examples include: Coinbase Global (the largest cryptocurrency exchange in the US), PayPal (committed to accepting Bitcoin transactions), and Marathon Digital (one of the largest Bitcoin miners and digital asset holding companies). The valuations of these companies are dependent on the profitability of mining and the prices of cryptocurrencies (see Figure 19 Price of Mining Company Marathon Digital (MARA) Compared to the Bitcoin Network Miners Revenue for an illustration).

**Figure 19 Price of Mining Company Marathon Digital (MARA) Compared to the Bitcoin Network Miners Revenue**



Source: Blockchain.com, Yahoo Finance, Wolfe Research Luo's QES

Figure 20 Mining and Blockchain ETF Comparison Table below is a list of ETFs investing in public traded companies investing in crypto or blockchain technology, as of May 6, 2022:

**Figure 20 Mining and Blockchain ETF Comparison Table**

Mining/Blockchain ETF	AUM	Expense Ratio	Top 3 Holdings	Exchange	Notes
Amplify Transformational Data Sharing ETF (BLOK)	\$800 million	0.71%	Silvergate Capital 4.85% CME Group 4.73% SBI Holdings 4.70%	NYSE	Invests in companies developing, researching, and using blockchain technologies; 47 holdings in total
Siren Nasdaq NexGen Economy ETF (BLCN)	\$165 million	0.68%	Coinbase Global 2.57% Mastercard 2.26% American Express 2.17%	NASDAQ	Alternative for investing in companies developing and using blockchain technologies; 63 holdings in total
First Trust Indxx Innovative Transaction & Process ETF (LEGR)	\$135 million	0.65%	JD.com 1.53% IBM 1.48% Mastercard 1.47%	NASDAQ	Invests only in companies materially committed to using blockchain technologies; 102 holdings in total
Bitwise Crypto Industry Innovators ETF (BITQ)	\$85 million	0.85%	Galaxy Digital 11.12% Microstrategy 9.64% Coinbase Global 8.67%	NYSE	Focuses on Bitcoin and crypto-trading venues, mining operations, mining equipment providers, and service providers; 30 holdings in total
VanEck Digital Transformation ETF (DAPP)	\$50 million	0.50%	Block Inc 9.37% Silvergate Capital 8.55% Coinbase Global 7.02%	NASDAQ	Tracks companies participating in digital asset economies and decentralized finance; 25 holdings in total

Source: Wolfe Research Luo's QES

## APPLICATIONS OF BLOCKCHAIN

In addition to cryptocurrencies, there are other important applications of blockchain. In this section, we briefly discuss a few of them – DeFi, NFTs, and Web3. We will also introduce the ESG implications and government regulations in this space.

### DeFi

A niche sector arising in the crypto space from smart contracts is DeFi or decentralized finance. DeFi is a segment of dapps replicating financial products and services, providing methods of financing, or earning interest on deposits without introducing a traditional bank or financial institution<sup>23</sup>. DeFi provide bank services, while individuals could potential profit (instead of banks). Smart contracts permit conditional transfers of money executed by code, ensuring repayment and fulfillment of obligations. Inventive developers have created products such as collateralized borrowing and insurance coverage against exchange hacks. Most DeFi activities take place on decentralized exchanges (DEXs), which are automated decentralized alternatives to centralized exchanges like Coinbase. DEXs have lower fees and no know-your-client (KYC) requirements. DeFi platforms source liquidity in a decentralized manner, by incentivizing individuals to provide liquidity in return for interest. This provides opportunities for liquidity providers.

The benefits of DeFi compared to traditional finance are accessibility, anonymity, low fees, speed, and 24/7 availability (since no human staffing is required). The sector has caught institutional attention as the total value of liquidity in DeFi protocols rose from \$20 billion in January 2021 to over \$250 billion by January 2022<sup>24</sup>. Detailed coverage of DeFi opportunities is out of the scope of this report. We only provide a brief overview on some of the main concepts below:

- **DEXs.** DEXs are platforms allowing users to swap varieties of cryptocurrencies, like a foreign currency exchange. They utilize smart contracts instead of a central intermediary like Coinbase. The advantages of DEXs are instant settlement of swaps and 24/7 service. DEXs do not take custody of holdings to trade like CEXs – leaving funds safe from orchestrated hacks. Liquidity for trades is held in smart contract wallets, and liquidity provisioning is decentralized. Exchange rates are determined by algorithms known as Automated Market Makers. Crypto arbitrage is associated with taking advantage of rate differences between DEXs. Uniswap, the largest DEX by market capitalization, surpassed Coinbase in trading volume for the first time in January 2022<sup>25</sup>.
- **Staking pools.** Staking pools are smart contract-based pools of funds which split staking rewards among participants based on their share of the pool<sup>26</sup>. The greater the aggregated funds in the pool, the higher likelihood of being selected to validate a block and receiving a reward (i.e., Proof-of-Stake). Pools lower the barrier to entry in staking by allowing individual investors to participate without meeting a minimum stake requirement. Crypto exchanges and DeFi providers with automated staking pools return steady amounts of interest to liquidity providers who lock up crypto deposits.

<sup>23</sup> See <https://ethereum.org/en/defi/> to read more about DeFi.

<sup>24</sup> See <https://www.theblockcrypto.com/data/decentralized-finance/total-value-locked-tvl> for figures.

<sup>25</sup> ibid

<sup>26</sup> See <https://academy.binance.com/en/glossary/staking-pool> for more about staking pools.

- **Lending platforms.** Lending and borrowing are made easy through smart contracts with most platforms requiring borrowers to overcollateralize loans for the safety of lenders<sup>27</sup>. A desired type of cryptocurrency is put into a pool of funds by lenders who earn interest. Borrowers can take money out for re-payment with interest. Borrowers commonly deposit collateral and take out a loan to capitalize on an opportunity requiring a different currency. Interest rates differ between borrowing and lending as well as between cryptocurrencies. The largest collateralized lending protocol on Ethereum is Aave. Recently, undercollateralized loans have risen on platforms like TrueFi and Maple Finance which offer loans to institutional borrowers who undergo a decentralized credit scoring process.
- **Yield farming.** As DEXs source liquidity in a decentralized manner, users are incentivized with a return for providing trading liquidity. Liquidity for a given cryptocurrency trading pair is locked in a special smart contract called a liquidity pool. DEX users pay trading fees to swap the coin pair using the pool. Liquidity providers receive portions of the fee proportional to their share of the pool. Yield farming annual percentage yield or APY can often reach double digit returns. However, gains are subject to fluctuations in cryptocurrency price while funds are locked in liquidity pools.
- **Decentralized insurance.** DeFi comes with risks. Smart contract failure from erroneous programming may render funds irretrievable. Crypto exchanges may have a programming exploit which leads to a hack. DeFi insurance platforms offer a decentralized method for protecting losses. They function by investors pooling resources to a smart contract to insure against specific events<sup>28</sup>. The largest decentralized insurance platform by market capitalization is Nexus Mutual at \$721 million.

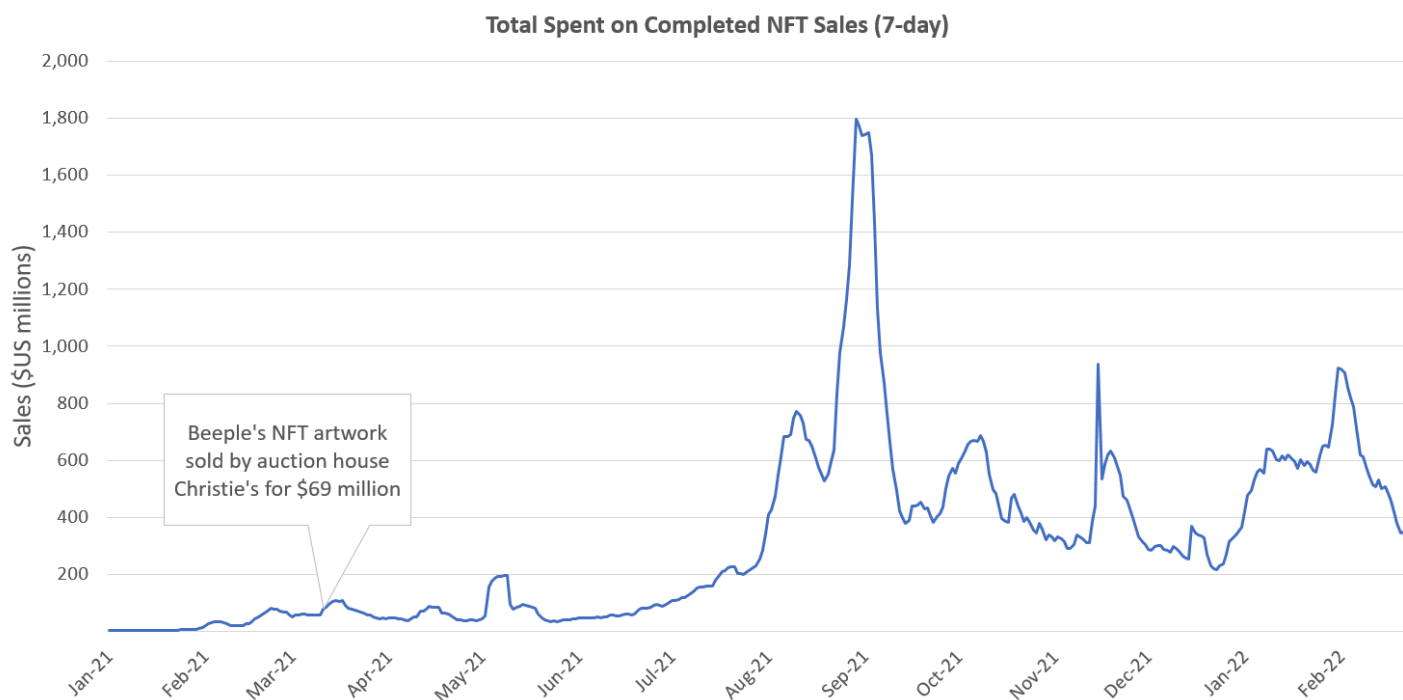
## NFTs

NFTs (Non-Fungible Tokens) – 2021's chosen dinner table topic of discussion – are digital records of ownership existing on a blockchain. They are typically created to give rights over pieces of digital or even physical assets. NFTs act as certificates of original ownership in a digital world where practically any image or file can be duplicated. For example, NFTs broke into the mainstream after a digital collage of 5,000 paintings by the artist Beeple was purchased for \$69 million, instantly making him one of the top three most valuable living artists. The total dollar value spent on NFT sales since January 1, 2021, is shown in Figure 21 Total Spent on Completed NFT Sales Since January 1, 2021.

<sup>27</sup> See <https://ethereum.org/en/defi/#lending> for more about decentralized lending.

<sup>28</sup> See <https://www.blockdata.tech/blog/general/defi-insurance-simply-explained> for more about insurance.



**Figure 21 Total Spent on Completed NFT Sales Since January 1, 2021**


Source: Nonfungible.com, Wolfe Research Luo's QES

The idea behind NFTs is in the name. Fungible objects are those which are practically identical to others and replaceable. US dollar bills, for example, are fungible. However, non-fungible objects are one-of-a-kind. They are valued differently based on unique features or attributes. NFTs are encoded on the blockchain as tokens, like utility or governance tokens, but contain a unique identifier distinguishing them from all other tokens.

NFTs are purported to return power back to artists who can sell artwork on a marketplace directly to customers. NFTs are the market of authentication and allow for a more direct revenue stream to the original author. NFT artwork is typically released in collections which tends to be more lucrative for artists of popular collections. Currently, CryptoPunks is the largest collection of NFTs by trading volume<sup>29</sup>. It has seen a lifetime trade volume of over 846,000 ETH, equivalent to over \$2.2 billion. The average sale price is 44 ETH or \$120,000. Regulatory concerns are rampant as NFTs of digital artwork create potential for abuse. For example, wash trading – selling an NFT to oneself to distort pricing – has proliferated as a means of laundering money and profiting from false valuations.

The total trade volume of NFTs on the Ethereum blockchain in December 2021 reached a whopping \$3 billion, up from \$12 million the prior year. In total, more than \$41 billion was invested in Ethereum-based NFTs throughout 2021. Currently, most existing NFTs apply to digital art, but the application of NFTs is vast. The future potential is to monetize digital items in gaming, replace physical property records, trading sport cards, concert or event season passes, as well as intellectual property rights. Propy, a real estate startup, sold the first NFT-backed physical property in the US for 210 ETH, valued at \$653,000. The winning bidder was awarded an NFT as digital proof of home ownership. Organizers

<sup>29</sup> See <https://opensea.io/collection/cryptopunks> to view the “CryptoPunks” collection on NFT marketplace OpenSea.

for the Coachella Music Festival also sold lifetime passes to the event as NFTs. 2021 was the year in which the phrase “NFT” was introduced to the world en masse. We may see more mainstream adoption in 2022.

## WEB3

Three iterations of the world wide web have come to fruition. The first iteration Web1 was a read-only version in which information was posted and users can read, but not write. Web1 was largely decentralized, as anyone could create a website and post content. The second iteration, Web2, is the version of the web which we are most familiar with – a world wide web in which most of the traffic is directed through a relatively centralized hub of popular websites owned by a handful of companies. Users on these websites can read as well as post content. These familiar websites, like Twitter or Facebook, offer their services in exchange for personal data. The centralized platforms of Web2 also enable the Big Tech companies to censor and control content as they please.

With the introduction of smart contracts and the Ethereum Virtual Machine, a new decentralized version of the web, called Web3, is being developed. It will offer similar outlets but with no central powers<sup>30</sup>. Like any dapp, the front-end can be written in any language – a Web3 application may look exactly like a Web2 app. The only difference is the front-end calls to a back-end smart contract, not a company’s server. In practice, this means Web3 sites cannot block users from the platform or censor content. Furthermore, no company exists behind a Web3 app to collect and sell personal data. Web3 sites also cannot be shut down with a denial-of-service (DoS) attack since interaction occurs through smart contracts instead of a central server. Decentralized alternatives to social media like YouTube and Twitter are only rudimentary implementations of Web3. Services such as confidential, decentralized cloud computing offer solutions to chronic data leaks from breaches of centralized cloud computing servers. This is an ideal, utopic state of Web3. In its current state, it is essentially a layer on top of Web2 with meta data on user ownership.

Youthful developers are increasingly seeking Web3 opportunities over Big Tech firms. 2021 saw the highest number of active monthly Web3 developers at 18,416.<sup>31</sup> Furthermore, 45% of the full-time developers in Web3 joined startups in 2021 (see Figure 22 Electric Capital Developer Report 2021 – Monthly Active Developers in Web3), so there is much more to come from this flourishing industry.

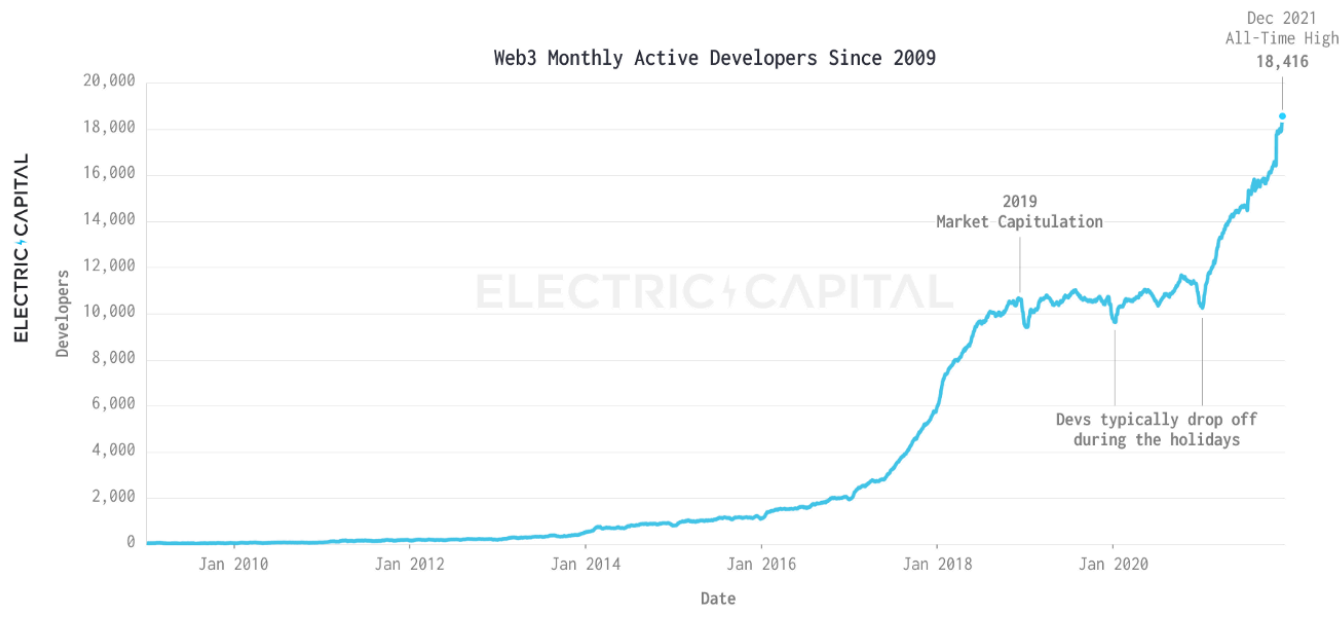
<sup>30</sup> See <https://ethereum.org/en/developers/docs/web2-vs-web3/> for more about Web3 and its pros and cons.

<sup>31</sup> See <https://www.electriccapital.com/resources> for more.

Figure 22 Electric Capital Developer Report 2021 – Monthly Active Developers in Web3

12

## THERE ARE NOW **18,416** MONTHLY ACTIVE DEVELOPERS IN WEB3



Source: Electriccapital.com

## ESG CONCERNS AND CRYPTO REGULATIONS

As detailed in [Green Alpha](#) (see Luo, et al [2021]), ESG practices have grown central to many asset managers' portfolios. The three pillars of ESG – environment, social, and governance – have also garnered attention and debate in the crypto world.

Bitcoin's meteoric rise in 2021 brought all eyes on the environmental impact of proof-of-work mining. Recall each Bitcoin transaction consumes 1,173 kilowatt-hours (kWh) or \$176 of electricity – enough to power an average US household for 6 weeks<sup>32</sup>. Spent mining hardware is also discarded after usage, producing thousands of tons in electronic waste.

The crypto world has responded in unity. Tesla suspended acceptance of Bitcoin in payment for its electric vehicles and is searching for a greener crypto alternative. Recently, it is rumored that Tesla is eyeing the comparatively environmentally friendly Dogecoin instead. Ethereum will also upgrade its infrastructure to proof-of-stake consensus this year, estimated to consume a fraction of energy required. Ninepoint released the world's first carbon-neutral Bitcoin ETF on the Toronto Stock Exchange in January 2021, dedicating a portion of its management fee to offsetting its carbon footprint. Furthermore, the Viridi Cleaner Energy Crypto-Mining & Semiconduct ETF (RIGZ) was created as an

<sup>32</sup> See <https://www.moneysupermarket.com/gas-and-electricity/features/crypto-energy-consumption/> for more

ETF that invests in environmentally friendly crypto businesses. While still emerging as an important segment of the crypto space, environmentally friendly opportunities are bountiful for investors.

Attention is also being raised toward the social ESG pillar in the blockchain and Web3 world. Among 378 crypto startups founded between 2012 and 2018, only one company had an all-female founding team. Furthermore, only 31 had a relatively even mix of male and female employees (see Joseph [2019], available [here](#)). To address the clear gender gap, several organizations have been formed such as Women in Blockchain, Diversity in Blockchain, and the Black Women Blockchain Council.

Governance is addressed inherently through the introduction of decentralizing blockchain technology. Decentralized autonomous organizations (DAOs), for example, are organizations sharing a central pool of funds and governed by democratic voting among all stakeholders. Fundholders are issued governance tokens. Voting is weighted by tokens held. Blockchain transparency prevents tampering with voting. Numerous DAOs currently hold over \$1 billion dollars in assets. While DAO structure currently pertains most to crypto startups, it also has implications for the future business structures of traditional companies. A new law signed on July 1, 2021 in Wyoming, provides legal recognition for DAOs as a business structure. Governance tokens for DAOs may be traded like equities in the future.

### *Regulatory Landscape*

The crypto world is rife with illicit activities such as not-so-uncommon hacks of crypto exchanges, altcoin pump and dump schemes, and fraudulent Initial Coin Offering projects. Criminals have become increasingly sophisticated in hiding their tracks as privacy-centric cryptocurrencies like Monero and transaction-obscuring DeFi protocols like Tornado Cash have grown popular. The likes of destabilizing financial systems, supporting money-laundering, and directly hindering carbon neutrality goals are only a few reasons cited for flat-out crypto bans in nine countries – including China. At the other end of the scale, El Salvador became the first country to adopt Bitcoin as legal tender in June 2021.

Most parts of the world are in crypto regulatory limbo – most governments are struggling to understand the crypto space. Those with regulatory frameworks are yet to catch up to more advanced DeFi products. The US House Committee on Financial Services hosted crypto CEOs and experts in a recent hearing on cryptocurrencies. This puts crypto investors on edge as announcements of crypto regulatory events have historically caused sizeable drops of Bitcoin and altcoin prices. For example, China's crypto ban in May 2021 caused Bitcoin's price to drop from \$58,958 to \$31,576, down 46%. The treatment of crypto varies widely from country to country. It is imperative for investors seeking entry in the crypto space to be aware of their respective government's position.

In countries where cryptocurrencies are regulated, securities or financial services regulators often come to mind. Crypto exchanges are typically held to strict know-your-client (KYC) standards for investigators to track money laundering. Transfers to exchanges over certain thresholds are often subject to suspicious activity reporting and anti-money laundering (AML) laws. Cryptocurrency profits are taxed at the capital gains rate. Also, Crypto miners may need to report mined cryptocurrency as taxable income. Ultimately, each country aims to maintain control over financial flows within its jurisdiction. In any case, cryptocurrencies are heavily restricted when perceived as posing a threat to the state.

Covering the specific regulations for every country is beyond the scope of this report, but a helpful and comprehensive list of government policies related to crypto by country can be found in the Law Library of Congress<sup>33</sup>.

This report is intended for Shibin Xie. Unauthorized redistribution of this report is prohibited.

---

<sup>33</sup> See <https://tile.loc.gov/storage-services/service/ll/gldr/2021687419/2021687419.pdf> for the document.

## CRYPTO DATA SOURCES

As we continue to develop our cryptocurrency database and analytical models, we have been researching the various data sources in this area. In this section, we outline a few data providers that we find useful.

### EXCHANGES

Hundreds of cryptocurrencies and market data sources are available to investors. Data aggregators provide price, volume, and supply data for thousands of coins. Access to historical data is essential for research and investing. The ones that we focus tend to offer data access via Python APIs. Some providers also provide Excel add-ins.

Coin-related market data typically includes price, volume, return, market capitalization, and other metrics. Futures, options, and perpetual swaps data can be commonly found from the same data aggregators. A few of the more well-known providers for coin and market data include:

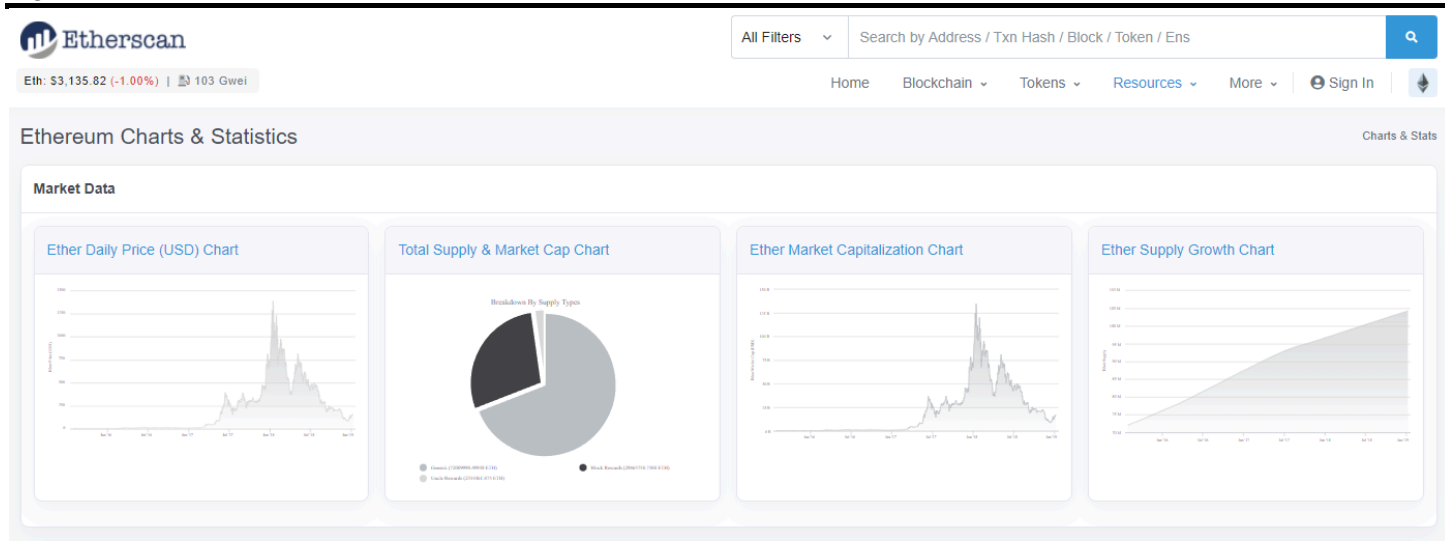
- **CoinMarketCap** covers 9,174 unique coins with API access for coins, derivatives, exchanges, and global crypto data.
- **CoinGecko** covers 12,400 coins with API access for crypto exchanges, derivatives, and crypto holdings by public companies.
- **Nomics** provides historical data for 38,497 tokens and 548 exchanges With API access reputed as one of the industry's best. They are the first provider to list 90% of crypto assets.
- **CryptoCompare** offers transaction data from 250 exchanges and a suite of digital asset indices. It also allows custom building of indices and provides an API for historical data and crypto news articles.
- **Cryptosheets** supports Excel plug-in for accessing data from hundreds of crypto data providers. It also enables integration with other data aggregators such as CoinGecko and CryptoCompare.

### NAVIGATING THE BLOCKCHAIN WITH BLOCKCHAIN EXPLORERS

As blockchains are public, their contents are viewable by anyone with a node in the network. On-chain data is taken directly from blockchains. These metrics are unique to the crypto world. The relationship of on-chain data to cryptocurrencies is like fundamental data to companies. Websites which collect on-chain data from blockchains for users to sift through are called Blockchain Explorers. Specific transactions or the contents of blocks are searchable on these sites (see Figure 23 User Interface of an Ethereum Blockchain Explorer for an example). More importantly, Blockchain Explorers aggregate statistics for transactions, wallets, and mining in each network and present them in charts – an ideal venue to construct systematic crypto factors. A separate Blockchain Explorer exists for most major cryptocurrencies such as Bitcoin, Ethereum, and Dogecoin. Datasets can generally be downloaded as a csv file or retrieved via an API.



Figure 23 User Interface of an Ethereum Blockchain Explorer

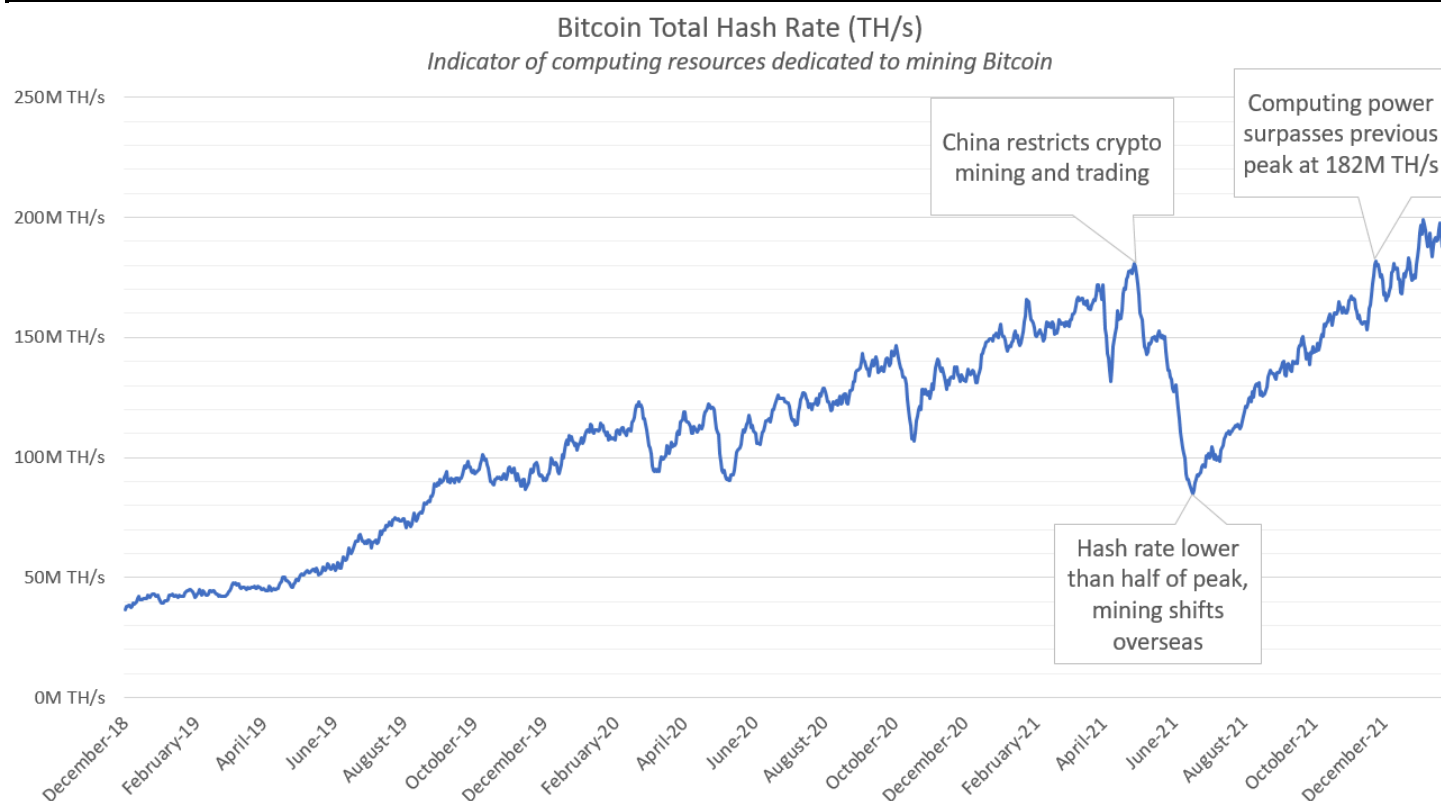


Source: Etherscan.io

A few examples of useful indicators from on-chain data include:

- **Confirmed transactions per day:** Number of confirmed transactions in the past 24 hours
- **Mempool size (in bytes):** Aggregate size in bytes of all pending transactions awaiting confirmation in the mempool
- **Fees per transaction:** Average transaction or gas fees in US dollars
- **Total Hash Rate:** Estimated number of terahashes calculated per second by the network (for proof-of-work currencies like Bitcoin). This indicates computing resources dedicated to mining (see Figure 24 An example of on-chain data from a Blockchain Explorer for an example).
- **Miners Revenue:** Total value in US dollars of coinbase rewards plus transaction fees paid to miners per block
- **Total Unique Addresses:** Total distinct number of wallet addresses on the blockchain

**Figure 24** An example of on-chain data from a Blockchain Explorer



Source: Blockchain.com, Wolfe Research Luo's QES

Several important Blockchain Explorers along with their respective cryptocurrencies are listed below:

- **Bitcoin:** Blockchain.com
- **Ethereum:** Etherscan.io
- **Binance Coin:** BscScan.com
- **Solana:** Solscan.io
- **Ripple:** XRPScan.com
- **Cardano, Litecoin, Dogecoin, Ripple, Monero, and more:** Blockchair.com

### **On-Chain Metrics**

Another type of crypto data provider goes beyond the raw on-chain data to create new metrics for researchers. Their metrics are used for investment research, developing cryptocurrency indices, structured products, and tracking macro crypto asset trends. Metrics may cover both native coins and tokens. Several reputable institutional-grade data providers are listed below:

- **Glassnode** combines on-chain data with price and supply metrics to offer a suite of market indicators related to mining.

- **Messari** offers dashboards, fundamental charts and screeners for cryptocurrencies. Data includes volatility metrics and staking-related statistics. Research reports are also provided on DeFi, Web3, and specific protocols.
- **The Block Crypto** offers market, derivatives, and blockchain metrics along with aggregated Stablecoin and DeFi market data. They also provide Google Trends and social media-based data metrics for crypto.
- **CryptoQuant** summarizes on-chain data along with market, network, crypto exchange statistics, and mining indicators.
- **Coinmetrics** is an open-source project facilitating collaboration among researchers and data providers to develop and track new cryptocurrency network indicators. They also offer several crypto asset indices for institutions.

## ALTERNATIVE VENDORS

There are also many other alternative data providers with unique insights in the crypto space:

- **Into the block** provides insight into DeFi network activity, lending, DEX-related metrics, and protocol-specific metrics like whale concentration (high volume traders), token correlation to Bitcoin, total liquidity, fees, and user metrics.
- **Skew** offers data for both Bitcoin and Ethereum futures and options including relevant indicators like put/call ratios. They also offer indicators from social media sites like Twitter and Reddit.
- **LunarCRUSH** provides metrics related to social media engagement with specific cryptocurrencies on Twitter, Youtube, and Reddit.
- **Santiment** offers a range of market metrics, social network data, wallet activity, and exchange activity tracking.
- **DeFi Pulse** provides DeFi indicators like total value locked in DeFi protocols, lending market data, and a DeFi Pulse Index, market cap-weighted index tracking performance of DeFi tokens.
- **DeFi Llama** summarizes statistics by DeFi protocols and presents a dashboard for exploring stats categorized by blockchain network.
- **State of the Dapps** offers statistics related to the dapp ecosystem including daily active users, smart contracts, new dapps per month, and data on dapp project tokens.
- **NonFungible** tracks all NFT marketplaces on the Ethereum blockchain to provide market data and metrics for valuing individual NFTs.

## Textual Data

In the traditional financial world, NLP (Natural Language Processing) is increasingly used to analyze market sentiment and buzz. Unstructured textual data offers a treasure trove of information for NLP-savvy quants. As text from the internet covers virtually any topic, web scraping is adaptable to all assets and cryptocurrencies are no exception. Unstructured textual data may therefore be one of the most valuable resources to crypto analysts.

Instead of navigating an ocean of crypto-related news articles on the internet, cryptocurrency news aggregators already collect relevant news and offer APIs. CryptoPanic is a popular crypto news

aggregator which lists crypto news articles. The feed is categorized by trending, rising, and hot posts with comments and reactions for each post. It offers an enterprise version of its API to pull the data, and features a real-time news sentiment indicator, custom news source quality filters, and full historical data for related coin prices.

As detailed in [A Battle Between Retail and Institutional Investors](#), we use web scraping, NLP algorithms, and parallel GPU computing to process information on the Reddit platform to quantify retail stock participation. Reddit also houses numerous cryptocurrency-related communities – some with millions of subscribers frequenting daily discussion threads to get their fill of crypto news. Quants keen on web scraping may find Reddit an invaluable NLP resource for keeping ahead of the retail segment in the crypto space. A few subreddit communities to note are [r/Cryptocurrency](#), [r/Bitcoin](#), [r/Dogecoin](#), and [r/Ethereum](#).

## QES RESOURCES

### *Bitcoin Exposure Screen (BELLA)*

In [Measuring Stock-Level Exposure to Bitcoin](#), we introduce two methods to measure company-level exposure to Bitcoin as well as provide tools to manage risk exposures to the cryptocurrency asset class. First, we regress daily stock returns against Bitcoin (after accounting for equity market and industry). We apply a robust regression with elastic net penalty to deal with dimensionality and spurious regression. Out-of-sample performance of the Bitcoin beta is strong; however, some of the top ranked Bitcoin beta stocks may not have an intuitive link to the crypto market.

To supplement the statistical approach, we conduct a textual analysis on management presentations and conference calls by probing for cryptocurrency-related words within company call transcripts – leveraging our Natural Language Processing tools. The two approaches are highly complementary, and we combine them into a composite score coined Bella (Bitcoin Exposure Language Learning Analysis). As is shown in Figure 25 QES Bitcoin Exposure Screen, 29 of the top 30 stocks with the highest exposure are directly or indirectly involved in Cryptocurrencies or blockchains. Clients interested in receiving a weekly Bella screen can contact us at [Luo.QES@wolferesearch.com](mailto:Luo.QES@wolferesearch.com).

Figure 25 QES Bitcoin Exposure Screen

#	Ticker	Company Name	GICS Sector	GICS Industry	Market Cap (\$MM)	Involvement*
<b>Stocks with the Highest Bitcoin/Crypto/Blockchain Exposure - 03/01/2022</b>						
1	HIVE	Hive Blockchain Technologies Ltd	Information Technology	Software	\$ 834.5	✓
2	RIOT	Riot Blockchain Inc	Information Technology	Software	\$ 2,008.7	✓
3	BBKCF	BIGG Digital Assets Inc	Information Technology	Software	\$ 159.2	✓
4	COIN	Coinbase Global Inc	Financials	Capital Markets	\$ 29,615.7	✓
5	MSTR	MicroStrategy Inc	Information Technology	Software	\$ 4,129.2	✓
6	BRPHF	Galaxy Digital Holdings Ltd	Financials	Capital Markets	\$ 1,277.3	✓
7	BITF	Bitfarms Ltd	Information Technology	Software	\$ 705.8	✓
8	DMGGF	DMG Blockchain Solutions Inc	Information Technology	Software	\$ 78.5	✓
9	SLNH	Soluna Holdings Inc	Information Technology	Electronic Equipment, Instruments & Components	\$ 147.4	✓
10	HUT	Hut 8 Mining Corp	Information Technology	Software	\$ 1,018.8	✓
11	CLSK	CleanSpark Inc	Information Technology	Software	\$ 439.6	✓
12	SI	Silvergate Capital Corporation	Financials	Banks	\$ 3,894.0	✓
13	GROW	U.S. Global Investors Inc	Financials	Capital Markets	\$ 72.8	✓
14	MOGO	Mogo Inc	Financials	Consumer Finance	\$ 174.8	✓
15	KHRIF	Cyberpunk Holdings Inc	Financials	Capital Markets	\$ 19.2	✓
16	BNXAF	Banxa Holdings Inc	Information Technology	IT Services	\$ 90.8	✓
17	PHUN	Phunware Inc	Information Technology	Software	\$ 289.5	✓
18	XNET	Xunlei Ltd	Information Technology	Software	\$ 114.5	✓
19	WKEY	Wisekey International Holding Ltd	Information Technology	Semiconductors & Semiconductor Equipment	\$ 55.7	✓
20	MARA	Marathon Digital Holdings Inc	Information Technology	Software	\$ 2,601.7	✓
21	NILE	BitNile Holdings Inc	Industrials	Electrical Equipment	\$ 84.3	✓
22	V	Visa Inc	Information Technology	IT Services	\$ 358,418.6	✓
23	CAN	Canaan Inc	Information Technology	Technology Hardware, Storage & Peripherals	\$ 832.4	✓
24	MA	Mastercard Inc	Information Technology	IT Services	\$ 349,897.6	✓
25	FRMO	FRMO Corp	Financials	Capital Markets	\$ 421.7	✓
26	PYPL	PayPal Holdings Inc	Information Technology	IT Services	\$ 130,399.0	✓
27	NVDA	NVIDIA Corporation	Information Technology	Semiconductors & Semiconductor Equipment	\$ 609,625.0	✓
28	NXTD	Nxt-ID Inc	Information Technology	Software	\$ 22.6	✓
29	IBKR	Interactive Brokers Group Inc	Financials	Capital Markets	\$ 6,497.1	✓
30	REKR	Rekor Systems Inc	Information Technology	Software	\$ 208.0	

\*: ✓ indicates the Company is involved in Bitcoin, cryptocurrencies, or blockchains.

Source: Bloomberg Finance LLP, FTSE Russell, CoinMarketCap, CoinDesk, Wolfe Research Luo's QES

### Multifactor Risk Models for Cryptocurrency

In [Multifactor Risk Models for Cryptocurrency](#), we discuss cryptocurrencies' consideration and use as protection against inflation. We also construct an Investable Crypto Index (ICI), using data tracing back to 2013 from CoinGecko, to measure the size and opportunity of the cryptocurrency market. To be considered for the index, a digital coin must satisfy stringent market cap and trading liquidity requirements. As of the end of February 2022, there are 242 cryptos in the index, totaling \$1.71 trillion market cap (see Figure 26 Features of the Investable Cryptocurrency Index (ICI) A and B).

Figure 26 Features of the Investable Cryptocurrency Index (ICI)

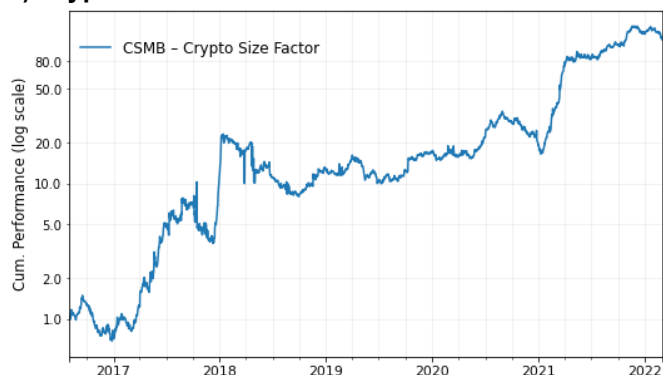
**A) Coverage of Investable Crypto Index**



**B) Market Cap Coverage of Investable Crypto Index**



**C) Crypto Size Factor Cumulative Performance**



**D) Crypto Momentum Factor Cumulative Performance**



Source: CoinGecko, Wolfe Research Luo's QES

We also develop two multifactor risk models for cryptocurrencies. The first intuitive three-factor model mirrors the Fama-French three-factor model for equities using market, size (see Figure 22C), and momentum (see Figure 22D) factors. The other is based on a statistical approach (PCA). Both models are statistically significant and economically meaningful – explaining a significant portion of cross-sectional variations of the crypto market – allowing us to quantify the role of cryptos in inflation hedging.



## BIBLIOGRAPHY

- Buterin, V. [2013]. "A Next-Generation Smart Contract and Decentralized Application Platform", Ethereum Whitepaper, available [here](#)
- Catalini, C., Gans, J. [2018]. "Initial Coin Offerings and the Value of Crypto Tokens", MIT Sloan Research Paper, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3137213](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3137213)
- Catalini, C., Gortari, A., Shah, N. [2021]. "Some Simple Economics of Stablecoins", MIT Sloan Research Paper Forthcoming, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3985699](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3985699)
- Hilary, G. [2020]. "Blockchain and Other Distributed Ledger Technologies, An Advanced Primer", SSRN Working Paper, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3740067](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3740067)
- Joseph, S. [2019]. "State of Diversity and Inclusion in Blockchain", Diversity in Blockchain, December 23, 2019, available [here](#)
- Jussa, J., Wang, S., Luo, Y., Li, X., Zhong, J., Martin, H., Rohal, G., Liu, S. [2021]. "A Battle Between Retail and Institutional Investors", Wolfe Research Luo's QES, January 29, 2021, available [here](#)
- Luo, Y., Rohal, G., and Wang, S. [2021a]. "Green Alpha", Wolfe Research Luo's QES, March 2, 2021, available [here](#)
- Luo, Y., Jussa, J., and Wu, K. [2021b]. "Measuring Stock-Level Exposure to Bitcoin", Wolfe Research Luo's QES, July 8, 2021, available [here](#)
- Nakamoto, S. [2008] "A Peer-to-Peer Electronic Cash System", Bitcoin Whitepaper, available [here](#)
- Rasmussen, R., Lawant, D., Hougan, M. [2021] "Decentralized Finance (DeFi): A Primer for Professional Investors", Bitwise Investments, November 16, 2021, available [here](#)
- Wu, K., Luo, Y., Jussa, J., Wang, S., Li, X., Rohal, G., Martin, H., Liu, S., Elledge, D. [2021]. "Multifactor Risk Models for Cryptocurrency", Wolfe Research Luo's QES, December 9, 2021, available [here](#)

## DISCLOSURE SECTION

### Analyst Certification:

The various Wolfe Research, LLC analysts who are primarily responsible for this research report certify that (i) the recommendations and opinions expressed in this research report accurately reflect the research analysts' personal views about the subject securities or issuers and (ii) no part of the research analysts' compensation was, is or will be directly or indirectly related to the specific recommendations or views contained in this report.

### Other Disclosures:

Wolfe Research, LLC does not assign ratings of Buy, Hold or Sell to the stocks it covers. Outperform, Peer Perform and Underperform are not the respective equivalents of Buy, Hold and Sell but represent relative weightings as defined above. To satisfy regulatory requirements, Outperform has been designated to correspond with Buy, Peer Perform has been designated to correspond with Hold and Underperform has been designated to correspond with Sell.

Wolfe Research Securities, Wolfe Research Advisors, LLC and Wolfe Research, LLC have adopted the use of Wolfe Research and The Wolfe Daily Howl as brand names. Wolfe Research Securities, a member of FINRA ([www.finra.org](http://www.finra.org)) and the National Futures Association, is the broker-dealer affiliate of Wolfe Research, LLC. Wolfe Research Advisors, LLC is the SEC-registered investment adviser affiliate of Wolfe Research, LLC. Wolfe Research Securities and Wolfe Research Advisors, LLC are responsible for the contents of this material. Any analysts publishing these reports are associated with each of Wolfe Research, LLC, Wolfe Research Securities and Wolfe Research Advisors, LLC.

The Wolfe Daily Howl is a subscription-based service for Institutional investor subscribers only and is a product of Wolfe Research, LLC. The products received may contain previously published research which has been repackaged for Wolfe Daily Howl subscribers. The types of services provided to you by Wolfe Research, LLC, vary as compared to that provided to other external clients of Wolfe Research. Wolfe Research, LLC, its directors, employees and agents will not be liable for any investment decisions made or actions taken by you or others based on any news, information, opinion, or any other material published through this service.

The content of this report is to be used solely for informational purposes and should not be regarded as an offer, or a solicitation of an offer, to buy or sell a security, financial instrument or service discussed herein. Opinions in this communication constitute the current judgment of the authors as of the date and time of this report and are subject to change without notice. Information herein is believed to be reliable but Wolfe Research and its affiliates, including but not limited to Wolfe Research Securities, makes no representation that it is complete or accurate. The information provided in this communication is not designed to replace a recipient's own decision-making processes for assessing a proposed transaction or investment involving a financial instrument discussed herein. Recipients are encouraged to seek financial advice from their financial advisor regarding the appropriateness of investing in a security or financial instrument referred to in this report and should understand that statements regarding the future performance of the financial instruments or the securities referenced herein may not be realized. Past performance is not indicative of future results. This report is not intended for distribution to, or use by, any person or entity in any location where such distribution or use would be contrary to applicable law, or which would subject Wolfe Research, LLC or any affiliate to any

registration requirement within such location. For additional important disclosures, please see <https://www.WolfeResearch.com/Disclosures>.

The views expressed in Wolfe Research, LLC research reports with regards to sectors and/or specific companies may from time to time be inconsistent with the views implied by inclusion of those sectors and companies in other Wolfe Research, LLC analysts' research reports and modeling screens. Wolfe Research communicates with clients across a variety of mediums of the clients' choosing including emails, voice blasts and electronic publication to our proprietary website.

Copyright © Wolfe Research, LLC 2022. All rights reserved. All material presented in this document, unless specifically indicated otherwise, is under copyright to Wolfe Research, LLC. None of the material, nor its content, nor any copy of it, may be altered in any way, or transmitted to or distributed to any other party, without the prior express written permission of Wolfe Research, LLC.

This report is limited for the sole use of clients of Wolfe Research. Authorized users have received an encryption decoder which legislates and monitors the access to Wolfe Research, LLC content. Any distribution of the content produced by Wolfe Research; LLC will violate the understanding of the terms of our relationship.

This report is intended for Shubin Xie. Unauthorized redistribution of this report is prohibited.

## DISCLOSURE SECTION

### **Analyst Certification:**

The various Wolfe Research, LLC analysts who are primarily responsible for this research report certify that (i) the recommendations and opinions expressed in this research report accurately reflect the research analysts' personal views about the subject securities or issuers and (ii) no part of the research analysts' compensation was, is or will be directly or indirectly related to the specific recommendations or views contained in this report.

### **Other Disclosures:**

#### **Wolfe Research, LLC Fundamental Stock Ratings Key:**

Outperform (OP):	The security is projected to outperform analyst's industry coverage universe over the next 12 months.
Peer Perform (PP):	The security is projected to perform approximately in line with analyst's industry coverage universe over the next 12 months.
Underperform (UP):	The security is projected to underperform analyst's industry coverage universe over the next 12 months.

Wolfe Research, LLC uses a relative rating system using terms such as Outperform, Peer Perform and Underperform (see definitions above). Please carefully read the definitions of all ratings used in Wolfe Research, LLC research. In addition, since Wolfe Research, LLC research contains more complete information concerning the analyst's views, please carefully read Wolfe Research, LLC research in its entirety and not infer the contents from the ratings alone. In all cases, ratings (or research) should not be used or relied upon as investment advice and any investment decisions should be based upon individual circumstances and other considerations.

#### **Wolfe Research, LLC Industry Weighting System:**

Market Overweight (MO):	Expect the industry to outperform the primary market index for the region (S&P 500 in the U.S.) by at least 10% over the next 12 months.
Market Weight (MW):	Expect the industry to perform approximately in line with the primary market index for the region (S&P 500 in the U.S.) over the next 12 months.
Market Underweight (MU):	Expect the industry to underperform the primary market index for the region (S&P 500 in the U.S.) by at least 10% over the next 12 months.

#### **Wolfe Research, LLC Distribution of Fundamental Stock Ratings (As of May 10, 2022):**

Outperform:	54%	10% Investment Banking Clients within the previous 12 months
Peer Perform:	38%	9% Investment Banking Clients within the previous 12 months
Underperform:	8%	4% Investment Banking Clients within the previous 12 months

Wolfe Research, LLC does not assign ratings of Buy, Hold or Sell to the stocks it covers. Outperform, Peer Perform and Underperform are not the respective equivalents of Buy, Hold and Sell but represent relative weightings as defined above. To satisfy regulatory requirements, Outperform has been designated to correspond with Buy, Peer Perform has been designated to correspond with Hold and Underperform has been designated to correspond with Sell.

Wolfe Research Securities and Wolfe Research, LLC have adopted the use of Wolfe Research and The Wolfe Daily Howl as brand names. Wolfe Research Securities, a member of FINRA ([www.finra.org](http://www.finra.org)) and the National Futures Association, is the

broker-dealer affiliate of Wolfe Research, LLC. Wolfe Research Securities is responsible for the contents of this material. Any analysts publishing these reports are associated with each of Wolfe Research, LLC and Wolfe Research Securities.

The Wolfe Daily Howl is a subscription-based service for Institutional investor subscribers only and is a product of Wolfe Research, LLC. The products received may contain previously published research which has been repackaged for Wolfe Daily Howl subscribers. The types of services provided to you by Wolfe Research, LLC, vary as compared to that provided to other external clients of Wolfe Research. Wolfe Research, LLC, its affiliates, officers, directors, employees and agents will not be liable for any investment decisions made or actions taken by you or others based on any news, information, opinion, or any other material published through this service.

The content of this report is to be used solely for informational purposes and should not be regarded as an offer, or a solicitation of an offer, to buy or sell a security, financial instrument or service discussed herein. Opinions in this communication constitute the current judgment of the authors as of the date and time of this report and are subject to change without notice. Information herein is believed to be reliable but Wolfe Research and its affiliates, including but not limited to Wolfe Research Securities, makes no representation that it is complete or accurate. The information provided in this communication is not designed to replace a recipient's own decision-making processes for assessing a proposed transaction or investment involving a financial instrument discussed herein. Recipients are encouraged to seek financial advice from their financial advisor regarding the appropriateness of investing in a security or financial instrument referred to in this report and should understand that statements regarding the future performance of the financial instruments or the securities referenced herein may not be realized. Past performance is not indicative of future results. This report is not intended for distribution to, or use by, any person or entity in any location where such distribution or use would be contrary to applicable law, or which would subject Wolfe Research, LLC or any affiliate to any registration requirement within such location. For additional important disclosures, please see <https://www.WolfeResearch.com/Disclosures>.

The views expressed in Wolfe Research, LLC research reports with regards to sectors and/or specific companies may from time to time be inconsistent with the views implied by inclusion of those sectors and companies in other Wolfe Research, LLC analysts' research reports and modeling screens. Wolfe Research communicates with clients across a variety of mediums of the clients' choosing including emails, voice blasts and electronic publication to our proprietary website.

Copyright © Wolfe Research, LLC 2022. All rights reserved. All material presented in this document, unless specifically indicated otherwise, is under copyright to Wolfe Research, LLC. None of the material, nor its content, nor any copy of it, may be altered in any way, or transmitted to or distributed to any other party, without the prior express written permission of Wolfe Research, LLC.

This report is limited for the sole use of clients of Wolfe Research. Authorized users have received an encryption decoder which legislates and monitors the access to Wolfe Research, LLC content. Any distribution of the content produced by Wolfe Research, LLC will violate the understanding of the terms of our relationship.

This report is intended for Shubin Xie. Unauthorized redistribution of this report is prohibited.