Authored by:

Matt Kunke
Research Analyst

Date: November 10, 2021
Topic: Digital Assets

GLOBAL X ETFs RESEARCH

Bitcoin: The Basics

In October 2008, a mysterious whitepaper touting a potentially revolutionary monetary concept made its way to a cryptography mailing list. In a tidy nine pages, Satoshi Nakamoto, a pseudonym for an individual or perhaps a group of individuals, introduced the world's first decentralized peer-to-peer money system. The paper claimed that participants in this fully open system, available to anyone with an internet connection, would be able to exchange value globally at any time without the need for a trusted intermediary.

Several months later, in January 2009, the first version of Bitcoin software formally marked the creation of the Bitcoin network, referenced in this report with an uppercase "B." The network was the first application of blockchain technology, a fully transparent, shared, and continually reconciled distributed ledger that records transactions and tracks assets. The network's launch also marked the creation of bitcoin. Referenced in this report with a lowercase "b," bitcoin is a digital currency that's divisible, fungible, and easily transferable with a programmatically defined monetary policy that ensures its scarcity.

Bitcoin's Maturation: From Niche to Mainstream

Bitcoin arrived at an opportune time. Its launch coincided with the peak of the Global Financial Crisis (GFC), when many individuals lost trust in the large banks that held their money and the governments that set monetary policy. Bitcoin represented a new form of "hard money" that could not be adjusted or controlled by any centralized entity. This feature, and bitcoin's scarcity, resonated in the aftermath of the financial crisis as governments around the world implemented large quantitative easing programs that increased the supply of fiat currencies.

In the years that followed the GFC, bitcoin steadily gained credibility, but it largely remained a niche asset, prone to volatility and skepticism. Then the COVID-19 pandemic, and the federal stimulus it required, thrust bitcoin's most prominent features back into the spotlight. Eager investors seized the opportunity to participate in bitcoin and the cryptocurrency community more broadly. While its large price swings and detractors remain, bitcoin is more mainstream than ever and solidifying its foothold.

Today, there are 18.85 million bitcoins in existence, with a total market cap of $1.23 trillion. Roughly 280,000 bitcoin transactions are conducted on-chain daily, representing approximately $4.8 billion dollars in volume on average.[1]

BITCOIN PRICE (LOG SCALE)
Source: Blockchain.com. As of 10/21/2021.

What to Know About Bitcoin, Its Key Components, and How it Works

Because of its growing status and the potential investment implications, this report answers basic questions about bitcoin and how it functions.

- **What is bitcoin?** A more transferrable, digital version of gold.
- **What is the Bitcoin network?** The first truly open, permissionless, and trust minimized financial ecosystem.
- **What are nodes?** The computers that run Bitcoin's software and help secure the network.
- **How does mining work?** Special nodes solve a mathematical puzzle to create the chain's next block.
- **Why is defining the main blockchain critical?** It resolves issues that arise due to network latency.
- **When does true settlement occur?** When a transaction has a sufficient number of confirmations.

This report also discusses bitcoin's positioning in the economic environment by focusing on three broad questions.

- **What does bitcoin provide?** An independent source of trust and access to financial inclusion.
- **How should the regulatory environment for bitcoin be viewed?** As an evolving part of the story.
- **Why bitcoin now?** It's an asset built for these economic times.

Bitcoin: A More Transferrable, Digital Version of Gold

As a currency, bitcoin is a finite supply asset in a network of users who agree on its value as a form of money that can't be controlled or altered by a singular entity. Bitcoin, which represents the first application of Blockchain technology, exists as a ledger balance on the Bitcoin blockchain. Unlike traditional government-backed fiat currencies, bitcoin has no physical bills or coins.

Rather, bitcoin users have private keys, which can be thought of as an account password. Users also have public keys and addresses that are cryptographically derived from and linked to the private key. Importantly, a private key cannot be determined from a public key or an address. A user's address is analogous to a public username used to identify the destination of a bitcoin transaction. In essence, to spend bitcoin, a user needs the private key associated with the public key and the address where the bitcoin is held. For a user to receive bitcoin, they simply need to provide their bitcoin address to the sender.

DERIVATION OF PUBLIC KEYS & ADDRESSES

Source: Global X ETFs, Mastering Bitcoin: Programming the Open Blockchain.

Publicly showing your private key would seem to create a problem, though. Bitcoin is a digital bearer asset, which means that it's spent by any individual holding the private key. Being required to display the private key could conceivably allow anyone to steal the bitcoin in the associated address. However, spending bitcoin doesn't actually reveal the private key to the network. Spending bitcoin shows a digital signature that cryptographically verifies the signer owns the private key.

Digital signatures are derived from a user's private key and the proposed transaction information. And because public keys and addresses are derived from a private key, advanced mathematics can verify if the private key that created a digital signature is the same private key used to create a public key. This cryptographic relationship allows digital signatures to provide independent verification of bitcoin ownership on the network, providing bitcoin users the freedom to spend their bitcoin while preventing bad actors from spending someone else's bitcoin.

The Bitcoin Network: The First Truly Open, Permissionless, and Trust Minimized Financial Ecosystem

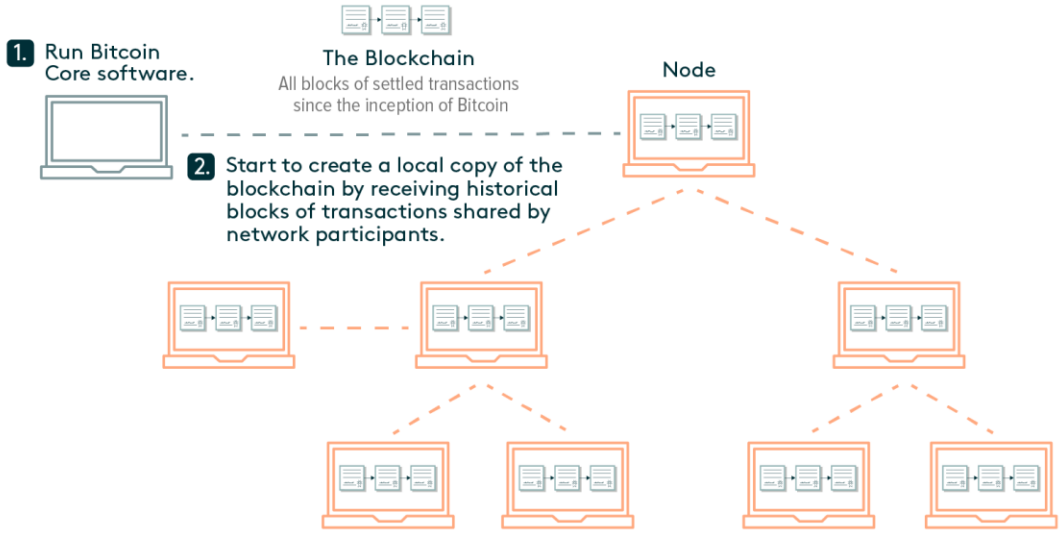
The Bitcoin network allows for the transfer of bitcoins on a peer-to-peer basis without an intermediary like a financial institution. The network utilizes fully transparent blockchain technology to facilitate the recording of transactions and the tracking of bitcoins. Network participants can find a consensus state, where they agree on the blockchain's distributed ledger, by following the protocol rules and independently validating transactions and blocks against the rules.

The network uses Bitcoin Core, an all-encompassing software package that allows full autonomy to participate. When a computer runs the software, it connects to other computers in the network, which are called nodes.

The computer then begins to receive all the blocks of transactions that occurred since the network's creation. The computer can then create its own complete copy of the distributed database of transactions, known as the Bitcoin blockchain. Bitcoin Core has a wallet application built into it, giving participants the ability to transact in bitcoin directly through the software. Wallets handle the management of key pairs, track bitcoin balances, and allow for the creation of digital signatures to spend bitcoin.

NETWORK OF COMPUTER NODES RUNNING BITCOIN CORE SOFTWARE

Source: Global X ETFs.



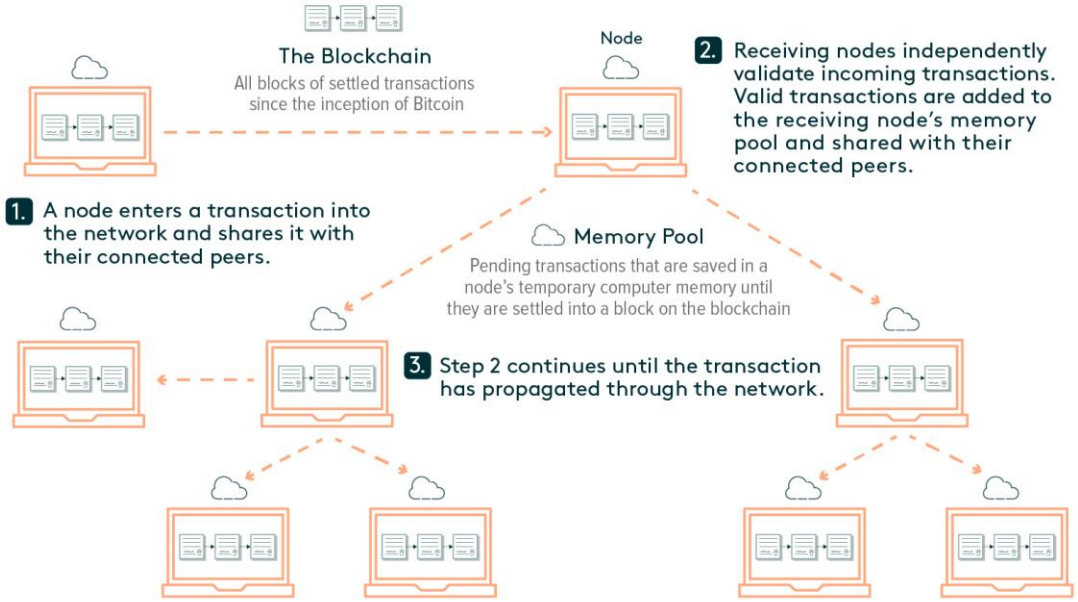
Nodes: The Computers That Run Bitcoin Core, Help Secure the Network

After creating their own copy of the blockchain, nodes maintain an up-to-date copy of the chain, listening to their peers for new transactions and new blocks as they occur in real-time. Nodes help secure the network by independently validating all transactions and blocks against the protocol rules, only sending the valid transactions and blocks to their connected peers. Each node consistently updates the pool of validated but pending transactions known as the memory pool.

When a node receives a new transaction from one of their connected peers, the software independently verifies the validity of this transaction against a comprehensive set of criteria, including an evaluation of the digital signature. If the transaction is valid, the receiving node saves it in its temporary computer memory and sends the transaction to the rest of the nodes that it's connected to. Thereafter, this cycle repeats: A different peer listening for transactions, receives this transaction, validates it, and then sends it to their connected peers. This cycle is how information moves through the network on a peer-to-peer basis.

TRANSACTION PROPAGATION THROUGH THE BITCOIN NETWORK

Source: Global X ETFs.



Mining Nodes: Special Nodes that Solve a Mathematical Puzzle to Create the Next Block

All Bitcoin nodes independently verify transactions, but mining nodes are a special type that aggregate transactions into the blocks that are recorded onto the blockchain for settlement. In that sense, mining nodes are distinct because they create blocks on the chain. Blocks can be thought of as the settlement layer for transactions. Transactions are sent continuously between nodes and stored in temporary memory. At this point, they're essentially pending transactions until they settle on the blockchain when a miner includes them in a block.

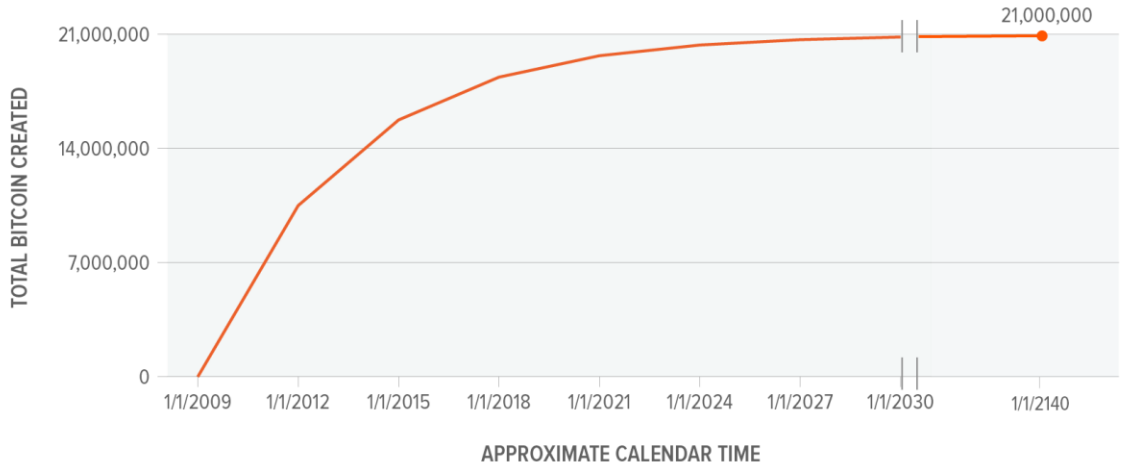
Mining nodes dedicate large sums of computational resources in a competition to be the first to solve a challenging mathematical puzzle. The solution to the puzzle is known as a Proof-of-Work. The puzzle is solved by brute force computation, where miners iterate different inputs through a cryptographic hash function searching for a rare output, or hash. The Proof-of-Work is difficult to find, but any node can trivially verify that the miner expended the computational resources to find the solution. In the same way that a transaction is only considered valid if it has a valid digital signature, a candidate block requires a Proof-of-Work to become a valid block.

Miners are financially incentivized to be the first to solve this puzzle. The miner who sends a new block with a valid Proof-of-Work first can claim the block reward and all the transaction fees inside that block. The block reward is a special transaction that allows the miner to send themself a fixed amount of newly created bitcoin. This process is referred to as mining because the block reward represents new bitcoin being generated for the first time, similar to new gold being mined from the ground.

Currently, the block reward represents the creation of 6.25 new bitcoin, which equates to more than $400,000 today.[2] However, the block reward decreases by 50% every 210,000 blocks, or approximately every four years, until around 2140 when the block rewards will cease to exist. These halving events drive

bitcoin's disinflationary monetary policy. The next halving event is expected to occur in 2024 and reduce the bitcoin block reward to 3.125 bitcoin per block.

BITCOIN SUPPLY
Source: Global X as of Sep 30, 2021.

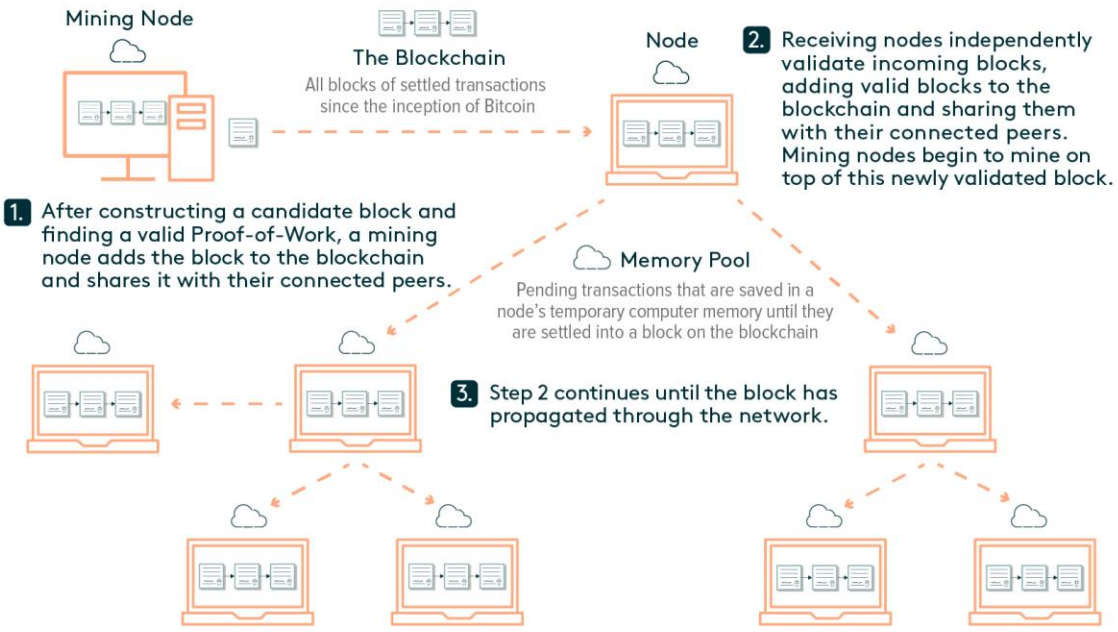


Also, when users transact on the Bitcoin network, they typically pay a small transaction fee to incentivize a miner to include their transaction in a block for settlement. Transaction fees can increase significantly during periods of high demand on the network because they represent bitcoin spenders bidding to have their transactions settled. For example, the average transaction fee in September 2021 was only $2.50, but it ranged from about $20–65 over a 10-day stretch in April 2021 when bitcoin first breached $60,000 and the network was congested.[3] Blocks generally have 1,500–2,500 transactions in them, so transaction fees are typically a small percentage of a miner's total compensation for solving a block.

Once a miner solves a block, they transmit the block through the network. Each node verifies the validity of the newly received block and then adds it to their copy of the blockchain. The receipt of a new valid block resets the mining game. All miners create a new candidate block and try to be the first to solve the puzzle connected to the newly received block.

BLOCK PROPAGATION THROUGH THE BITCOIN NETWORK

Source: Global X ETFs.



The Bitcoin Core software was designed so that this mining puzzle would be solved once every 10 minutes on average. The software does this by adjusting the difficulty of the puzzle approximately every two weeks to make it more (less) challenging as more (less) hash rate tries to solve the puzzle. As a result, unlike the mining of precious metals, the pace at which bitcoin is mined cannot be expedited. In other words, the increase in supply of bitcoin is fixed and independent of the demand for bitcoin. Increased investment in more mining rigs would only result in the puzzles becoming more computationally intensive to solve, keeping the bitcoin issuance rate constant.

The Main Blockchain: Resolves Issues That Arise Due to Network Latency

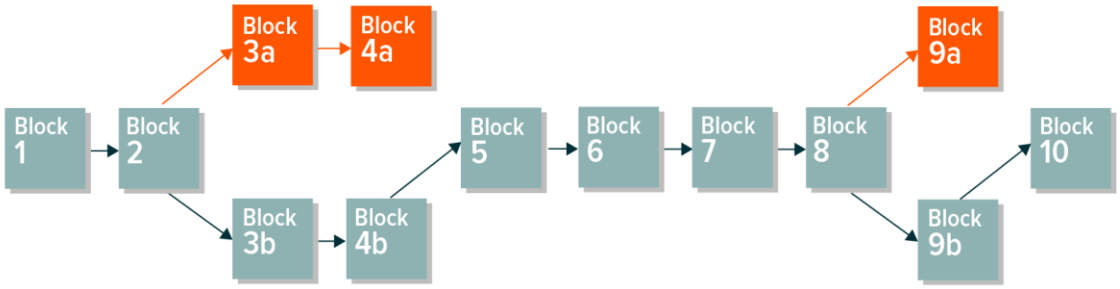
One issue that can arise is two miners solving the Proof-of-Work and sending valid blocks at nearly the exact same time. Given the nature of a global network where information flows through it from peer to peer, different nodes inevitably receive information at slightly different times due to network latency. The protocol solves this dynamic by requiring each node to identify the main blockchain as the longest chain, or more precisely, the chain with the most cumulative work on it. For example, if we assume Miner A and Miner B produce valid blocks at nearly the exact same time, Miner C may receive Miner A's block first and Miner D may receive Miner B's block first.

This scenario can create something called a temporary fork in the blockchain, which means that both blockchains are temporarily valid and the main chain is identifiable only after the hindsight of future blocks being added to one of the chains. But this scenario resolves quickly as miners select which chain to form subsequent blocks on. By default, miners work off of the first valid block they receive. So Miner A and Miner C mine off of one blockchain, and Miner B and Miner D mine off of the other.

The probability that both sides of the forked chain continue to solve the Proof-of-Work at the same time quickly goes to zero as more blocks are produced. As soon as one side finds the next block before the other, the chain that produced this block is considered the main blockchain and the other side of the chain is abandoned based on protocol rules. This protocol rule allows nodes to find consensus and agree on the

state of the blockchain and the transactions that occurred. The orange blocks in the illustration below are valid, but in hindsight they are not part of the main chain, which is illustrated in blue.

TEMPORARY FORKS IN THE BLOCKCHAIN
Source: Global X ETFs.



True Settlement & Immutability: When a Transaction Has a Sufficient Number of Confirmations

A transaction is often referred to as settled when it's included in a block. But because certain scenarios can cause the blockchain to fork temporarily and reorganize in the short term, certain conditions must be met for true settlement and immutability.

Only after a sufficient number of confirmations are received, meaning blocks added to the chain on top of the block that includes a specific transaction, can true settlement and immutability occur. A block with six confirmations following it is generally considered immutable, or unalterable. For small transaction sizes, one to three confirmations is often deemed safe. Given that blocks are linked together with each newly mined block referencing the prior block's hash, transactions become more secure and immutable as the number of blocks they're buried beneath increases.

For example, a malicious actor who wants to reverse a transaction that had six confirmations would need to go back six blocks to the block that contains the transaction that they want to manipulate. And then they would need to re-mine that block and the five other subsequent blocks on a forked chain, finding a valid Proof-of-Work for each of these six blocks. At the same time, all good actors following the protocol rules will be mining and extending the main blockchain as previously defined. To overcome the six-block deficit versus the main chain, the malicious actor would need to control more than 50% of the total network's computational power for a sufficiently long period.

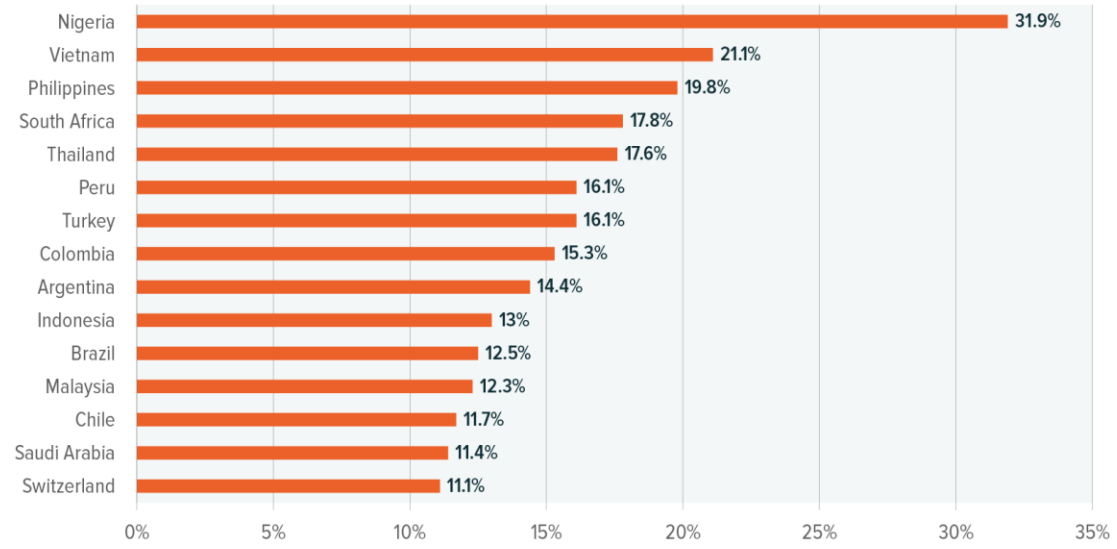
What Bitcoin Provides: An Independent Source of Access and Trust

The Bitcoin network is a financial ecosystem where participants don't need to trust a government to back the currency or to manage the money supply responsibly. For the developed world, the significance of this feature may be particularly difficult to understand, though recent economic crises may facilitate comprehension. Trusted financial institutions operating within strong regulatory frameworks that protect investors is not a privilege enjoyed equally around the globe, particularly in emerging economies.

The Bitcoin network provides a mechanism for financial inclusion for unbanked and underbanked populations, particularly in countries struggling with political instability, corruption, or severe inflation. A February 2021 survey by market and consumer data firm Statista indicated that the top 10 countries with the highest frequency of cryptocurrency usage among their populace were all emerging market countries. Nigeria, with 32% of respondents indicating that they use bitcoin or cryptocurrency more broadly, led the way, followed by Vietnam at 21% and the Philippines at 20%.[4]

CRYPTOCURRENCY USAGE BY COUNTRY

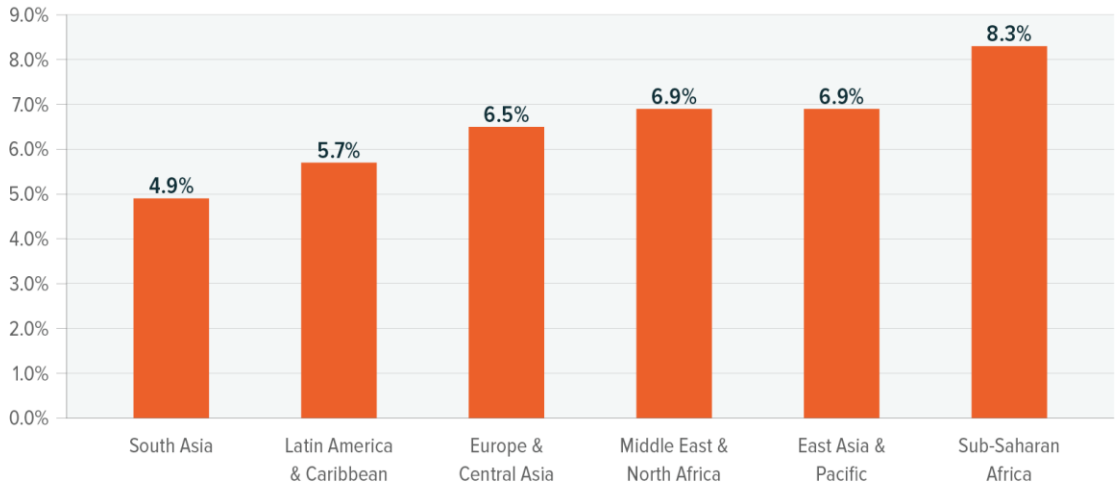
Source: Global Consumer Survey, as of Feb 28, 2021.



The remittance market is another key use case for bitcoin. Remittances make up a disproportionate amount of emerging market countries' GDP relative to their more developed counterparts. According to the World Bank, transaction fees reduce the average remittance sent globally by 6.4%. Fees can increase to more than 10% in some of the higher-cost remittance corridors.[5]

AVERAGE REMITTANCE COST BY REGION

Source: The World Bank, Remittance Prices Worldwide, available at http://remittanceprices.worldbank.org. As of 3/31/2021.



Using bitcoin to transfer wealth internationally could be a significant cost-saving measure for certain emerging economies. El Salvador, for example, is a country where roughly 70% of the population receives remittance payments. The government's decision to be the first country to adopt bitcoin as legal tender could be a notable test case. By one estimate, bitcoin could save the country $400 million per year in remittance fees.[6]

Regulatory Environment: An Evolving Part of the Story

Still in its infancy, bitcoin, like other digital assets, operates in an uncertain, patchwork regulatory environment that varies by country and jurisdictions within countries. For example, at the federal level, cryptocurrency regulations in the U.S. remain scant, but individual states have their own rules, some stricter than others. The New York State Department of Financial Services (NYDFS) has notably stricter regulations than most anywhere else in the country.

With varied regulations, classifications, and tax treatments around the world, assessing the regulatory landscape for bitcoin is difficult. In time, we expect more defined regulatory frameworks to develop. And the risk reduction that comes with clearer regulatory regimes could benefit bitcoin and encourage greater participation. As bitcoin's acceptance grows, failure to implement prudent regulations could stifle innovation in localities as companies determine how best to operate with bitcoin. For example, Kraken, one of the largest crypto exchanges in the U.S., ceased operating in New York after the state implemented the BitLicense framework in 2015.[7]

The risk of overbearing regulation is a consideration, but the decentralized and global nature of the Bitcoin network can mitigate the impact of regulatory overreach. The minimal price disruption that occurred following China's sweeping cryptocurrency ban in September 2021 is an example, in our view.[8]

Why Bitcoin Now: An Asset Built for These Economic Times

To understand bitcoin's growing appeal, an important consideration is that its formative years coincide with two historic economic crises with far-reaching political and social ramifications. These crises highlighted two of the biggest issues with the traditional financial ecosystem: mistrust and inaccessibility. But Bitcoin's main tenets solve for these issues.

- Bitcoin is a decentralized network that allows participants to exchange value globally without a trusted governing body or financial intermediary.
- Blockchain technology allows network participants to find a consensus state on the distributed ledger by following a fully transparent set of protocol rules.
- The digital currency is readily divisible, fungible, and transferable with a programmatically defined monetary policy that ensures its scarcity.
- And to participate, all it requires is an internet connection.

These attributes increasingly resonate with individual investors and, significantly, in mainstream financial circles. Investment banks and hedge funds now allocate financial and human capital to bitcoin. Companies are starting to include bitcoin on their balance sheets. Even universities are investors. Also bringing credibility to the space is a flourishing ecosystem of regulated bitcoin derivatives that has developed.

In October 2008, the biggest mystery wasn't Satoshi Nakamoto's identity; it was what space bitcoin could eventually occupy in the global economy. Thirteen years later, Nakamoto's identity remains unknown, but bitcoin continues to gain legitimacy as it becomes more familiar. After all, the potential to own a verifiably scarce asset with an increasing network of global users will typically find an audience with investors.

—

Glossary

Terms listed in the order in which they appear.

Cryptography: The broad study of techniques for secure transmission of information in the presence of adversarial behavior. See Public-key cryptography.

Bitcoin network: A peer-to-peer network of computers running the Bitcoin Core software. The Bitcoin network allows for the transfer of value (bitcoins) without the need for a trusted intermediary.

Blockchain (chain): A peer-to-peer shared and continually reconciled distributed ledger that facilitates the recording of transactions and tracking of assets without the need for a trusted intermediary. Participants in the network, called nodes, propagate transactions and blocks to be verified by other nodes according to the network's rules. Transactions are aggregated into blocks that record the time and sequence of transactions. Blocks are linked together with the prior block to form a chain, which grows linearly with the addition of each subsequent block. Blocks are added to the chain every 10 minutes on average.

bitcoin: A digital bearer asset that exists entirely as a ledger balance on the Bitcoin blockchain. It is the native cryptocurrency of the Bitcoin network.

Cryptocurrency: A digital currency in which transactions are verified and records are maintained by a decentralized system relying on cryptography rather than a trusted third party.

On-chain: Refers to transactions that occur on the actual blockchain. For example, when transacting on a centralized crypto exchange like Coinbase, for example, the centralized party simply moves bitcoin around on a ledger that they maintain for all their customers. These transactions don't actually result in a transaction on the blockchain until the assets are withdrawn from the platform.

Private key: Represents ownership of the digital bearer asset bitcoin; it is analogous to an account password. The private key is used to create digital signatures to verify bitcoin ownership. Anybody can take an addresses' bitcoin if they were to find the associated private key.

Public key: Mathematically derived from a private key. To spend the bitcoin associated with it, the key must be made publicly available. Digital signatures are validated against the public key, verifying if a prospective spender controls the private key associated with the public key. Separately, the public key is used as the input to a cryptographic hash function to generate the address.

Address: Mathematically derived from a public key; it is analogous to a public username that is used to identify the destination of a bitcoin transaction.

Digital signatures: Mathematically derived from a private key and a transaction's hash. A digital signature proves ownership of a private key and the associated public key without having to reveal the private key. Digital signatures allow for the independent verification of bitcoin ownership on the network, providing bitcoin owners the freedom to spend their bitcoin while preventing bad actors from spending someone else's bitcoin.

Bitcoin Core: The open-source computer software that implements the Bitcoin protocol and all aspects of the Bitcoin network.

Node: A computer that is running Bitcoin Core to maintain its own copy of the blockchain. Nodes participate in the security of the network by independently validating all transactions and blocks against the protocol rules, only sending the valid transactions and blocks to their connected peers.

Public-key cryptography: Also known as asymmetric cryptography, it utilizes two distinct but mathematically connected keys, one for encryption and one for decryption. This is the specific cryptography utilized in the Bitcoin network where the public key is used to receive bitcoin, and the private key is used to sign transactions to spend bitcoin.

Peer: Nodes in the network that have a direct connection to each other.

Memory Pool: Also known as the mempool, it refers to the pool of validated but pending transactions stored by nodes on their local computer memory prior to being settled into a block.

Mining nodes: A special subset of nodes that aggregate transactions together into the blocks that are recorded onto the blockchain for settlement. Mining nodes compete to be the first to solve a challenging mathematical puzzle based on a cryptographic hash function. Miners dedicate large amounts of computational resources to brute-force calculate the result of different inputs through a cryptographic hash function as quickly as possible.

Proof-of-Work: The solution to the challenging mathematical puzzle based on a cryptographic hash function that miners compete to solve. Due to the properties of cryptographic hash functions, the Proof-of-Work is incredibly difficult to find, but any node can trivially verify that the miner expended the computational resources to find this solution. The Proof-of-Work helps resolve disagreements when two blocks are mined simultaneously, and it protects the network by making historical blocks prohibitively expensive to manipulate.

Cryptographic hash function: A one-way function that can be used to map data of an arbitrary-length to a deterministic fixed-length result. Cryptographic hash functions include these key properties: 1) They are repeatable; for any input, the resulting output (hash) is always the same. 2) They are one-way functions where it is impossible to derive an input from a given output. 3) The optically random nature of the function makes it impossible to tailor an output by making small adjustments to an input. The mining process relies on computing the result of a cryptographic hash function repeatedly as fast as possible to achieve a certain output. These functions are also used to derive an address from a public key.

Hash: The output of a cryptographic hash function.

Candidate block: A block of pending transactions that a miner is attempting to add to the blockchain by finding a valid Proof-of-Work. After a Proof-of-Work is found, a candidate block becomes a valid block and is added to the chain. At this point, miners form a new candidate block, and they try to be the first to solve the puzzle connected to the newly received block and add the next valid block to the chain. Miners typically form candidate blocks by selecting the transactions in the memory pool with the highest transaction fees.

Block reward: A special transaction that allows the miner to send themself a fixed amount of newly created bitcoin as a financial incentive for solving the block. Currently, the block reward is 6.25 bitcoin per block. The block reward is the only way for new bitcoin to be created.

Transaction fees: A small transaction fee to incentivize miners to include their transaction in a block for settlement. Transaction fees are typically minimal, but they can become sizable in periods of severe network congestion.

Halving: Decreases the size of the block reward by 50%. Halving events occur every 210,000 blocks, or approximately every four years. The next halving event is expected to occur in 2024 and reduce the bitcoin block reward to 3.125 bitcoin per block.

Difficulty: A measure of how difficult it is to mine a bitcoin block at a particular point in time. The Bitcoin network was designed for blocks to be mined every 10 minutes on average, so the difficulty increases (decreases) as the computational power behind miners increases (decreases) to ensure that blocks continue to be mined every 10 minutes on average. The difficulty adjusts every 2,016 blocks, or approximately every two weeks on average. The software simply takes the ratio of the expected number of minutes it should take to mine 2,016 blocks (20,160 minutes) versus the actual number of minutes it took to mine the last 2,016 blocks, and it adjusts the previous difficulty upward or downward by this ratio.

Hash rate: An estimate for the total computational power securing the Bitcoin network at a point in time. It is measured as the number of hashes per second that all the miners in the network are computing in

aggregate. The Bitcoin network hash rate reached a peak of approximately 180 quintillion hashes per second in 2021.

Main blockchain (main chain): The blockchain that took the most cumulative work to mine based on the difficulty of the underlying blocks. Typically, the main chain has the most blocks.

Fork: A blockchain that diverges from a single chain into two different chains. These chains share the same history but reach a point where their newer blocks cease to be the same. Temporary forks occur when two miners mine a block simultaneously but the protocol rules result in this converging back on a single main chain. More permanent forks tend to occur when changes to the protocol rules are being made, or when there is community disagreement on the protocol rules, resulting in multiple forked versions of the software being run.

Immutability: The state or condition of being unchangeable.

Confirmations: The number of blocks added to the blockchain after a particular transaction was included in a block. The first confirmation is when a transaction is included in a block. An additional confirmation is added every time a new valid block is mined onto the chain.

1. Blockchain.com, as of Oct 21, 2021.
2. Coinmarketcap.com, as of Oct 21, 2021.
3. Blockchain.com, as of Oct 21, 2021
4. Statista Global Consumer Survey, as of Feb 28, 2021
5. Remittance Prices Worldwide, “Remittance Prices Worldwide Quarterly”, as of Mar 31, 2021
6. CNBC.com, “El Salvador’s new bitcoin plan could cost money providers like Western Union and others $400 million a year, says President Bukele”, as of Sep 9, 2021
7. Blog.kraken.com, “Farewell, New York”, as of Aug 9, 2015
8. Coinmarketcap.com, as of Oct 21, 2021

not be used for trading purposes. Please consult a financial advisor or tax professional for more information regarding your investment and/or tax situation.

Bitcoin is largely unregulated and bitcoin investments may be more susceptible to fraud and manipulation than more regulated investments. Bitcoin and bitcoin futures are subject to rapid price swings, including as a result of actions and statements by influencers and the media.