FACTSHEET

Crypto Research

Bitcoin — 87%

BTC — $3,956.89

General description of the coinBitcoin is the first decentralized digital currency that works without a central bank or single administrator. Transactions in the Bitcoin network happen between users directly without an intermediary (Peer-to-Peer). These transactions are verified by network nodes (miners) through the use of cryptography and recorded in a public distributed ledger called a blockchain. Bitcoin was released as open-source software in 2009 by an unknown person or group of people under the name Satoshi Nakamoto.

FACTS

Category	Cryptocurrency	**Consensus Algorithm**	PoW
Website	bitcoin.org	**Blockchain**	Bitcoin
Year founded	2009	**Scalability**	7 TPS
Market Capitalization	68,878,292,608 USD	**All Time High**	19497.4 USD
Volume (24h)	5,028,069,239 USD	**All Time Low**	68.43 USD
Volume (30d)	37,087,170,239 USD	**ICO Price**	no ICO
Circulating Supply	17.537.812 BTC	**ROI past 30 days**	-37.94%
Total Supply	17.537.812 BTC	**ROI past 90 days**	-41.75%
Max Supply	21.000.000 BTC	**ROI past year**	-66.06%

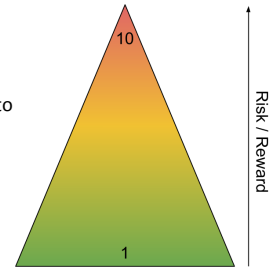
CHART

RISK/REWARD PROFILE

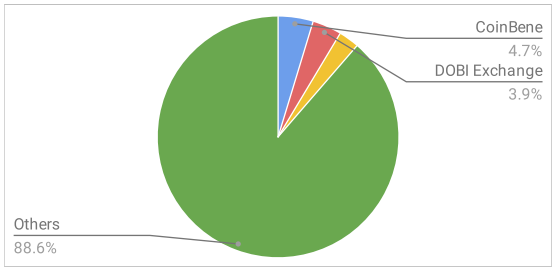
R/R Profile: 1

The risk/reward profile is adjusted to crypto currencies which represent a high risk investment in general.

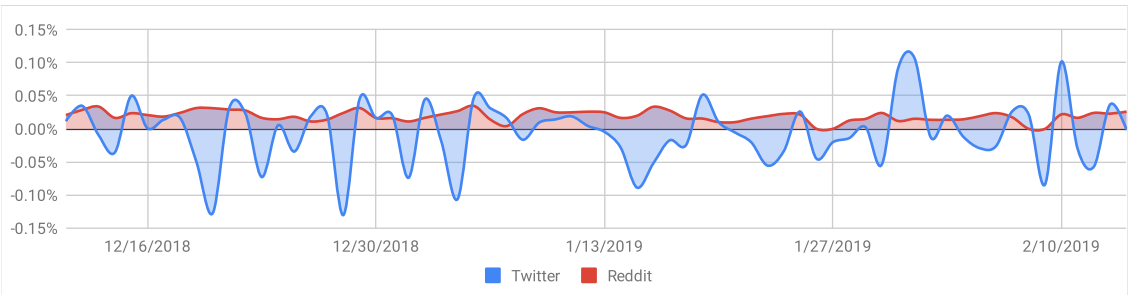
10: higher risk & higher reward
1: lower risk & lower reward



TOP EXCHANGES BY VOLUME



SOCIAL MEDIA & COMMUNITY



Bitcoin (BTC)

As of 14th February 2019

1. Strategy 89%

1.1. Objective

According to the Bitcoin whitepaper, the project intends to provide a peer-to-peer version of electronic cash allowing people to transact directly with each other with no need for intermediaries or third parties (e.g. financial institutions). Also, the lack of intermediaries combined with the non-reversibility of transactions should lower transaction costs.

1.2. Use Cases

To become a currency, we assume that Bitcoin needs to fulfill the characteristics of money:

Store of value: When looking at the store of value utility of Bitcoin it depends heavily on the timeframe one is measuring the success or failure. If the time frame is set to one or more years Bitcoin seems to have always preserved the value in dollar terms. When looking at shorter timeframes it depends on the entry and exit points which is why we believe Bitcoin fails here. However, the preservation of value using Bitcoin also depends on the currency or asset that is used to measure the performance. For people in Venezuela or Zimbabwe Bitcoin has proven to be a good store of value, even on shorter time frames.

Medium of exchange: Whether Bitcoin fulfills this utility depends on two variables: the amount of money that is sent and where it is sent to/from. Since Bitcoin fees are on average between 0.4 USD and 1.5 USD it is possible to send millions or even billions worth of USD cheap and instantly. On the other hand, the fees make Bitcoin is unsuitable for microtransactions for now. The shift to the lightning network is expected to provide a solution to this problem. Equally important, Bitcoin knows no borders, restrictions or capital controls.

Unit of account: Although the volatility of Bitcoin has declined since its inception and will deteriorate further with increasing market capitalization, it is still higher than with fiat currencies. We don't see Bitcoin becoming a unit of account in the near future as the volatility needs to decrease even more.

Whether Bitcoin is declared as a currency or not it is already used

- to send money globally and instantly for low fees
- as a safe haven in countries that suffer from (hyper)inflation (e.g. Venezuela, Zimbabwe)
- to avoid capital controls (e.g China)
- to avoid unpopular government action (e.g. Greece)
- to speculate

Future Use Cases: Theoretically, Bitcoin could be used as a settlement layer for all kinds of transfers of value like identities or securities.

1.1. Token

Bitcoin has the following use cases within the Bitcoin network:
Transfer of value: Bitcoin is used to transfer value from one person to another.
Store of value: Bitcoin can be stored within a wallet to preserve the value.
Fees: Users pay a fee to the miners for validating the transactions and securing the network.
Mining reward: The miners get a reward in BTC for securing the network. The history of Bitcoin has shown that all of the use cases make sense from a technical and token economical point of view.

1.2. Roadmap

There is no official Bitcoin roadmap but there are proposed improvements to the Bitcoin protocol contributed by the community.

Recent Improvements
SegWit in August 2017 - required to implement lightning network and increased scalability slightly Released Lightning Network beta to the mainnet.

These developments were big steps towards improving Bitcoin by increasing throughput and lowering transaction fees.

Proposed Future Improvements
Lightning Network: release of the final version
Sidechain Networks: allow other blockchains to connect to the Bitcoin network. Rootstock, for example, would add the functionality of smart contracts to Bitcoin. Other sidechain projects are Liquid Network or Drivechain.
MAST: allows smart contracts (allowed by side chains like Rootstock) to be split up into their individual parts; increases privacy and transaction; allows larger smart contracts
Schnorr signatures: proposal to replace Bitcoin's cryptographic algorithm for a more efficient one; allows aggregation of multiple transaction signatures into a single one; could reduce storage by around 25%; could allow development of smart contracts in the future
Bulletproofs: should improve privacy by concealing quantities of transactions Confidential Transactions: would keep the amounts of Bitcoin transactions visible only to participants in the transaction
Mimblewimble: is a proposal for a Bitcoin-like blockchain and claims to provide higher security, improved scalability, different cryptographic security and ASIC resistance. These improvements would come at the cost of scripts. Mimblewimble would likely be implemented as a side chain or as a separate altcoin.
Dandelion, Taproot and Graftroot: are expected to improve privacy even more.

1.3. Market

According to the whitepaper, Bitcoin attracts the market for electronic cash. However, since Bitcoin could also be used as a store of value, similar to gold, and as a settlement layer for securities the possible market Bitcoin attracts is outstandingly big.

Comparison of some of the potential markets:
Bitcoin Market Capitalization: 0.11 trillion USD
US Dollar: 1.5 trillion USD (7.3%)
Physical Money: 7.2 trillion USD (0.015%)
Gold Market Capitalization: 8.2 trillion USD (0.013%)
Narrow Money: 31.0 trillion USD (0.004%)
Stock Markets: 66.8 trillion USD (0.002%)

Compared to these markets, the market capitalization of Bitcoin seems tiny. However, it remains to be seen what percentage of those markets Bitcoin will be able to attract.

1.4. Competitors

Fiat currencies (USD, EUR, ...)
Fiat currencies have a longer history than Bitcoin and therefore enjoy more trust by people. Controversially, it has been shown several times that fiat currencies are not that stable at all and can collapse if they slip into high inflation and ultimately into hyperinflation. Inflation is also the reason for being a poor store of value. Depending on the distance, fiat transaction can be very slow and highly expensive. Finally, they underlie capital controls.

Gold
Gold has the advantage that it is more durable since the amount of Gold lost is pretty low and it can be discovered again. If the private key to a Bitcoin wallet is lost, it is lost forever as it is impossible to get access to that Bitcoin again. However, since the amount of gold getting lost is low the rate of deflation is lower as well. Also, Gold is more fungible than Bitcoin. If Gold is melted down, one ounce is essentially indistinguishable from any other ounce. Since it is possible to track the history of every Bitcoin it might be possible that people do not accept coins that have a history with illegal activities. This is called the tainted coin problem. With increased privacy, however, this problem can be solved. Also, gold is very slow and expensive to move compared to Bitcoin. Finally, Gold has a much longer history and therefore enjoys more trust. However, the longer Bitcoin exists the more people will believe that it is a permanent feature of the modern world just as it is the case with the internet.

Other Cryptocurrencies
There are several cryptocurrencies that try to outcompete Bitcoin. Most of them make trade-offs in the blockchain trilemma of security, decentralization, and scalability. In the past, Bitcoin always chose decentralization and security over scalability. We believe that this attitude is essential to becoming a successful digital currency. Hence, we don't see any cryptocurrencies that are able to compete against Bitcoin at the moment.

1.5. Innovation

Bitcoin was the first cryptocurrency and hence it was the first project to provide the following characteristics:

Portability: Bitcoin is the most portable store of value as it is (almost) instant, cheap to transfer and it knows no borders or capital controls.
Verifiability: In contrast to banknotes, Bitcoin cannot be counterfeited as they can be verified mathematically.
Divisibility: It is possible to divide every Bitcoin into a hundred millionth of a Bitcoin. While fiat currencies are quite divisible it is expensive to divide gold. Also, it is difficult or even impossible to divide gold into small quantities.
Scarcity: The code of the Bitcoin protocol does not allow more than 21 million Bitcoin to be mined.
Censorship Resistance: Bitcoin is decentralized and permissionless by design. This means that no entity can intervene and decide whether a transaction should be allowed or not. Therefore, it is impossible to implement capital controls on Bitcoin.
Transparency: With Bitcoin, no trust is needed as transactions are public and can be verified easily.

2. Team & Community 82%

2.1. Team/Advisors

First of all, it has to be said that Bitcoin is not run by a company. Neither it is run by a person - it is run by the Bitcoin community meaning everybody can contribute to the project.

The **Bitcoin Core Team** develops the Bitcoin core client (most used client) and contributes a lot to the development of Bitcoin. It consists of a large open source developer community with many casual contributors to the codebase. Within the team there are maintainers and contributors, each having their own functions. Maintainers are responsible for merging patches from contributors and act as a final check to ensure that patches are safe and in line with the project goals. Contributors, on the other hand, are the ones that proposed code changes, test, review, and comment on open Pull Requests. Everybody is free to join them and help to improve Bitcoin.

Blockstream is a company that was founded by Adam Back, Gregory Maxwell, Peter Wuille and others and their objective is to provide funding for the development of Bitcoin Core. Many of the Blockstream members are also Bitcoin Core developers. Some of the most influential team members are the following:

Wladimir van der Laan (Lead Maintainer)
He took over the position from Gavin Andresen in April 2014 and is also a developer at the MIT Digital Currency Initiative. His role is to maintain the GitHub repository and he tries to stay anonymous.

Pieter Wuille (Core Developer)
Pieter is Bitcoin Core developer since 2011. He co-founded Blockstream and is the second most active contributor on GitHub. Also, he was responsible for the SegWit upgrade. Previously he worked at Google and has a Ph.D. in computer science.

Gavin Andresen (Ex-Lead Maintainer and Contributor)
Gavin has collaborated directly with Bitcoin creator Satoshi Nakamoto in developing its source code. Satoshi Nakamoto handed over the control of the source code repository on GitHub before he disappeared. Gavin is still writing, reviewing code and offering his opinions on technical matters and project priorities.

People who possibly inspired Satoshi and still influence Bitcoin to some extent:

Adam Back - developed hashcash
Wei Dai - developed b-money
Hal Finney - developed POW
Nick Szabo - developed Bit Gold

There are several other developers who contribute regularly to the GitHub repository.

The history of Bitcoin proofs that it has the best developers in the crypto space. Since the inception in 2009, Bitcoin had 99.9% uptime and has never been hacked. Although some people criticize the scalability, it has to be remembered that the priority of the Bitcoin community has always been decentralization and security. In addition, the developers propose and develop some of the most innovative solutions.

2.2. Partner Organizations

Since Bitcoin is not a company or an entity it is difficult to identify partner organizations. However, we believe that Blockstream and the other companies, as well as all of the contributors, could be seen as partners in the wider sense as they contribute all kinds of resources to Bitcoin. Also, companies accepting Bitcoin as a payment method can be seen as partners. Some companies that already accept Bitcoin as a payment method are Overstock.com, Subway, Microsoft, Reddit, Expedia, Bloomberg, Zynga and many more. Finally, we also see companies that offer Bitcoin trading as partner organizations.

2.3. Investors

With a dominance of around 50% of the cryptocurrency ecosystem it can be said that Bitcoin has received the highest amounts of funds. Different studies show that the percentage of people and entities, invested in Bitcoin is still relatively small compared to other assets. Moreover, various studies and polls show that investors are interested in investing in Bitcoin.

Some popular funds that invested in Bitcoin are:
- Polychain Capital Fund
- Pantera Bitcoin Fund
- Galaxy Digital Assets
- Grayscale's Bitcoin Investment Trust

2.4. Community

Even though Bitcoin does not have an official presence on the various social media platforms, the community is the biggest in the crypto scene. Bitcoin has their own forum Bitcointalk.com where all kinds of topics around Bitcoin and other cryptocurrencies are discussed.

2.5. Website

The website Bitcoin.org is well designed and features an introduction video that teaches the basics about Bitcoin. Additionally, the site helps the user to choose an appropriate wallet and how to buy Bitcoin.

2.6. Social/Environmental Aspects

Bitcoin has a positive social/environmental impact as it gives people, who don't have a bank account, access to the global financial system. Furthermore, it provides people whose currency suffers from hyperinflation and/or corrupt governments an alternative. However, these benefits do not come for free. To secure the Bitcoin network, miners have to invest in appropriate hardware that consumes a large amount of energy. Even though it is difficult to calculate the exact amount of energy consumption, it is estimated that the Bitcoin network needs almost as much electricity as Ireland. However, it has to be mentioned that it is more profitable to mine Bitcoin when energy is (almost) free and that it doesn't matter where Bitcoin is mined from a geographical point of view. This is why many miners already started to make use of excess energy like hydropower, which could not be used otherwise and turn it into Bitcoin. It is estimated that energy used for securing the Bitcoin network is already driven by more than 75% of renewable energy and we expect this figure to increase with rising competition among miners. Additionally, we expect some of the profits of Bitcoin mining to go into the development of more efficient mining hardware.

2.7. Events

There are several Bitcoin conferences all over the world. Bitcoin.org lists all of the upcoming events.

3. Technology 89%

3.1. Technical Innovation

In 2008 Satoshi Nakamoto, whose identity is still unknown, published the solution to the long-standing problem called the Byzantine General's Problem (aka Double Spending Problem). This paper was the description of Bitcoin which was then developed in 2009. This allowed, for the first time in history, for value to be transferred quickly, at great distance and in a completely trustless way from one person to another. The technologies Satoshi used where not new, however, the way he combined blockchain with a peer-to-peer network and proof-of-work was very innovative. It allowed the creation of the first cryptocurrency and was one of the first real-world use cases for blockchain. Since 2009, over 1900 other cryptocurrencies where developed with Bitcoin as an inspiration or model. In contrast to the widespread opinion that Bitcoin has not been very innovative since then, the opposite seems to be the case. The past and proposed future improvements of the Bitcoin protocol are very innovative and are developed by the best programmers in the crypto space. We believe that Bitcoin is as innovative as possible taking into account that their first priority is security and decentralization.

3.2. Technical Details

The consensus algorithm of Bitcoin is called proof-of-work where miners have to invest in infrastructure and spend electricity to validate and record transactions. In return, they are rewarded with a block reward (if they solve the block) and transaction fees. Currently, this consensus mechanism allows Bitcoin to process only seven transactions per second which is not enough for becoming a digital version of cash. The development of Bitcoin is an ongoing and probably never-ending process. The last major updates were the implementation of SegWit and the launch of the lightning main net. Although the lightning network (LN) is in beta status and has not reached full adoption yet, the volume of Bitcoin sent through the lightning channels is growing continuously. We believe that the scalability of Bitcoin will improve tremendously with more and more volume flowing into the much faster lightning network. In addition, the LN also allows enhanced privacy and lower transactions fees. Since Bitcoin has the longest history and the highest market capitalization, the reward for hacking the network has to be the highest as well. Therefore, we believe that Bitcoin is exposed to the heaviest attacks in the crypto space. And yet, Bitcoin has not been hacked since it's inception and it had 99.9% uptime. Hence, we conclude that Bitcoin is the most secure asset of all crypto assets.

3.3. Wallets

There are several wallets available to store the private key on Windows, Mac, Linux, Android and iOS. Some of the most important ones are:

Online Wallets: Coinbase, Blockchain, Xapo
Offline Wallets: Bitcoin Core, Mycelium, Samurai, Electrum, Armory
Hardware wallets: Ledger, Trezor, KeepKey
Paperwallet: lets users print the private key on paper. The security and user-friendliness depends strongly on the wallet.

3.4. GitHub Progress

Bitcoin is ranked on place 22 when looking at the GitHub activity over the past twelve months. The total GitHub activity shows that Bitcoin has the most active GitHub repository by far, with 536 contributors and 35k stars. Besides the core development team, the community pushes the project forward as well. While the process of implementing new features is quite slow compared to other projects, this leads to much higher security of the network.

4. Token Economics 88%

4.1. Supply

Circulating Supply: 17.537.812 BTC (83.51%)
Total Supply: 17.537.812 BTC
Max Supply: 21,000,000 BTC

Inflation: 2018: 4.0% (estimate)
2019: 3.9% (estimate)
2020: 2.6% (estimate)
2021: 1.8% (estimate)
2022: 1.8% (estimate)

Deflation: Sending a Bitcoin to a non-Bitcoin address or losing the private key results in a permanent loss of that Bitcoin. Hence, the token economics have a deflationary aspect. Estimations on the amount of Bitcoin lost reach from 3 million up to 6 million BTC meaning that 14.3% up to 28.6% of the maximum supply could be removed permanently.

4.2. Coin Distribution

Coin holdings of the top wallets:
Wallet 1: 1.0% (Binance)
Wallet 2: 1.0% (Bitfinex)
Wallet 3: 0.6% (Bittrex)
Wallet 4: 0.6% (Huobi)
Wallet 5: 0.6% (Bitstamp)
Other Wallets: 96.2%

The coin distribution is very good compared to other projects where a few wallets hold the majority of the coins.

4.3. Reward Structure

Staking Reward: none
Mining Reward: The Bitcoin block mining reward halves every 210.000 blocks. Currently, a miner gets 12.5 BTC for mining a block. The next halving will take place in May 2020, reducing the reward to 6.25 BTC per block.
Masternode Reward: none
Profit Sharing: none

4.4. Cost Structure

Transaction Cost: The average transaction fee depends on the price of Bitcoin and fluctuated between 0.45 USD and 1.5 USD from July to September 2018. In December 2017 it reached a high with an average of 55 USD per transaction. When looking at the fees, it is clear that they are way too high for a currency that aims to be used as digital cash for everyday transactions. However, with developments like lightning network in the pipeline fees are expected to decrease to almost zero.
Other Cost: High electricity cost and expensive mining hardware.

5. Conclusion Total Score: 87%

Bitcoin was the first cryptocurrency, established in 2009 when the first block (genesis block) was mined. Due to the long history, investors seem to be most confident with investing in Bitcoin resulting in a market dominance of about 50% of all crypto assets. However, this dominance does not only result from the longest history.

Bitcoin seems to have earned the first place in several ways. First, Bitcoin has one of the largest communities, not only by users and promoters but also by developers. Having the best developers leads to the best and most innovative solutions as well as to the highest security possible. Also, the trade-off between security, decentralization, and scalability makes it unique in the crypto space. There is no other cryptocurrency that has secured billions of USD worth of Bitcoin over such a long time.

However, Bitcoin does not only compete against other crypto projects, but it also competes against fiat currencies, gold and other assets. When comparing Bitcoin against its competition it becomes clear that Bitcoin has major advantages when it comes to portability, speed of transactions, verifiability, divisibility, scarcity and censorship resistance. This is why people in countries with volatile currencies like Venezuela or Zimbabwe see an alternative in Bitcoin.

When looking at the downsides of Bitcoin, it has to be mentioned that the current scalability will not allow Bitcoin to become electronic cash. A negative side effect of network congestion is that fees rise during these times. However, the problems of scalability and high network fees seem to be definitely solvable with second layer solutions like the lightning network. Since this network is already live, we believe that these problems will be solved with more and more transactions happening on the lightning network.

The amounts spent on electricity and mining hardware to secure the network are quite high and cannot be denied. While energy consumption is still high, this also leads to developments of new and less energy intense mining hardware. Although Bitcoin could be censored in some states leading to exchange shutdowns, we believe it is very unlikely that several or even all states would censor Bitcoin at the same time, what would be the only thinkable scenario to restrict Bitcoin. Since many countries already stated their more or less positive opinion on Bitcoin, we believe that this would be an unrealistic scenario.

Bitcoin also has the risk of publishing vulnerable code that could lead to an insecure network. While this risk could have been a problem in the early days of Bitcoin, there are now several security steps including code audits before the updates are distributed.

What makes Bitcoin interesting from an investors point of view are the numerous opportunities and possible use cases that exist for this new asset. The low market capitalization and the deflationary effect make it even more attractive. Bitcoin has the fundamentals to provide a solution to collapsing currencies and capital controls. If Bitcoin manages to become a settlement solution for other value transfers the potential market capitalization is even bigger. It remains to be seen how Bitcoin will perform in a financial crisis. If people start to trust in Bitcoin and lose faith in fiat currencies Bitcoin could probably do well in times of financial turmoil.

In short, we see the opportunities outweigh the threats by far, especially when considering the low market capitalization compared to other assets or asset classes.