SMITH+CROWN

ORIGINAL RESEARCH

Monero

Monero is an open source cryptocurrency that obfuscates every transaction's sending address, receiving address, and transaction amount in order to maximize user financial privacy.

Overview

Many electronic transactions in the existing financial system are structured such that hackers, spies, insiders, or other motivated third parties could discover a user's purchase history, spending habits, or financial relations. While many consider cryptocurrencies such as Bitcoin to offer an anonymous alternative, in reality, almost all are pseudonymous, as a record of each transaction is publically available on-chain and many participating wallet addresses can be de-anonymized with off-chain tools. As cryptoasset adoption grows, and exchanges and other intermediaries standardize KYC identification requirements, companies such as Chainalysis can further link transactions and wallet addresses to individual identities. Monero is a cryptocurrency network that provides guarantees against this de-anonymization process at the protocol level, facilitating fully private transactions. These privacy guarantees allow users to more freely engage in activities such as tax evasion, money laundering, and the use of darknet markets, making Monero one of the most hotly debated and controversial cryptocurrencies. The Monero network token, XMR, functions as a medium of exchange and potential store of value.

Monero launched in mid-2014 as an implementation of the CryptoNote protocol. There was no pre-mine or token sale of XMR and codebase development is facilitated by a group of independent, generally anonymous contributors, currently led by Riccardo 'fluffypony' Spagni. The Monero blockchain is secured by Proof of Work (PoW) mining using the CryptoNight hash algorithm. The Monero community has been resistant to allowing Application Specific Integrated Circuits (ASICs) mine on the network, out of concern that ASIC-dominated PoW networks become centralized over time. In April 2018, Monero hard-forked to implement a hash algorithm code change that rendered Bitmain's recently announced Monero ASIC miner obsolete. The block size is dynamic

Monero uses a combination of stealth addresses and ring signature technology to obfuscate transaction details among participants and the network. At a high level, parties to an XMR transaction cannot access each other's address or history, yet retain strong cryptographic guarantees that transactions are valid and XMR cannot be double-spent.

NOTABLE DEVELOPMENTS

April 2014
Monero initially released as an implementation of the CryptoNote protocol

July 2014
Poloniex becomes first major exchange to offer XMR trading pairs

August 2016
Popular Darknet market AlphaBay accepts XMR

May 2017
WannaCry Ransomware attack on Microsoft Windows OS uses XMR

January 2017
Ring CT feature launch, eliminates ability to link early XMR transaction histories

April 2018
Mining algorithm altered in scheduled hard fork to brick Bitmain ASICs

September 2018
WSJ alleges money laundering facilitated by XMR and anonymous cryptoasset exchange ShapeShift

October 2018
Bulletproof signature feature launch reduces on-chain data storage requirements for Monero's privacy features, drastically lowering transactions fees

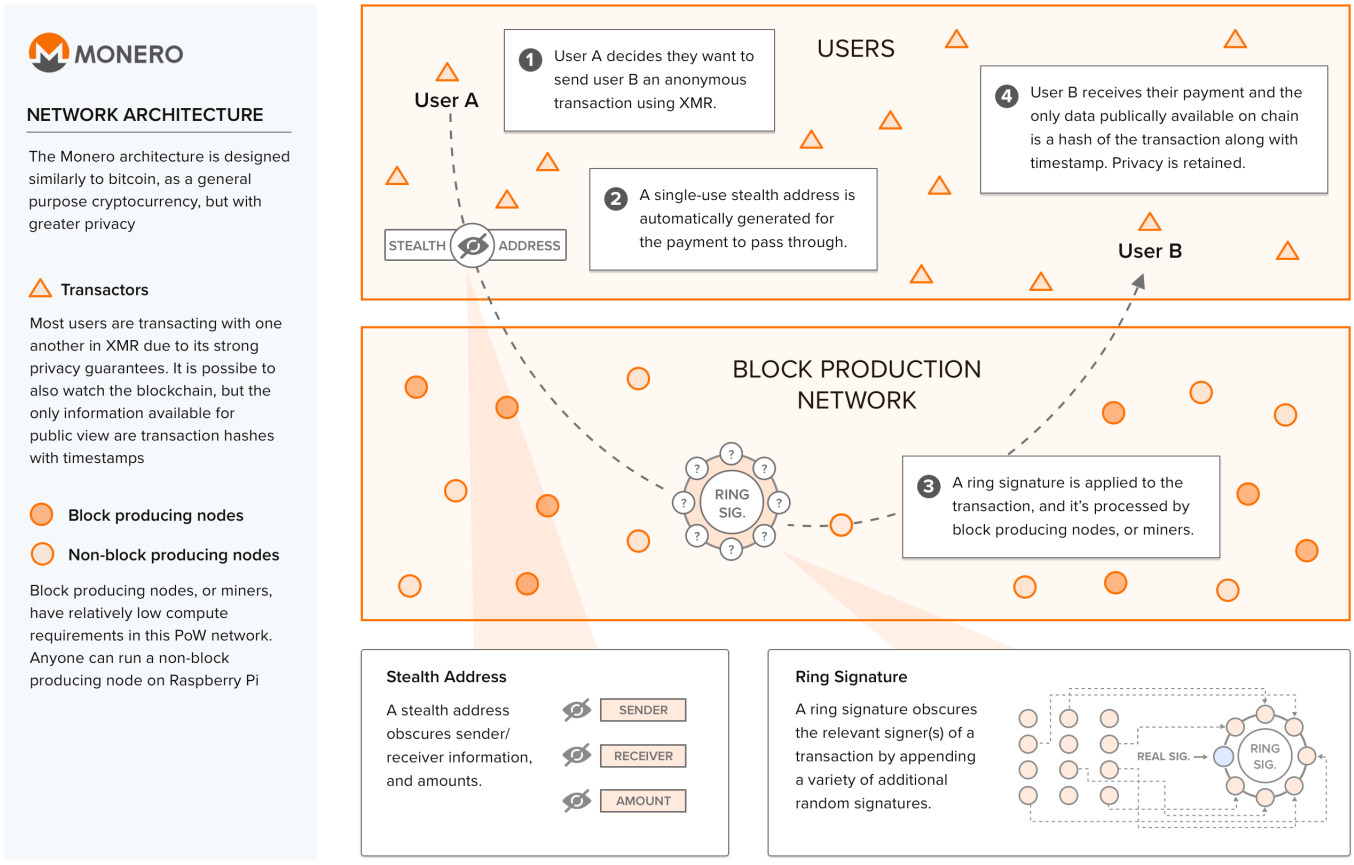
according to transaction demand and has a target block time of 1 minute. Monero employs a decreasing block reward structure to pay miners, which incentivizes their participation in securing the network and stabilizes at a 0.6 XMR reward per block in 2022. Monero uses a combination of stealth addresses and ring signature technology to obfuscate transaction details among participants and the network. At a high level, parties to an XMR transaction cannot access each other's address or history, yet retain strong cryptographic guarantees that transactions are valid and XMR cannot be double-spent.

Monero's Core Team facilitates development by vetting donation-soliciting proposals on the project's semi-official forum, allowing donors to anonymously back development initiatives. Monero is an open source cryptocurrency and the Core Team's relation to the project is not hierarchical. Although the Core Team is a set of distributed pseudonymous individuals with loose affiliations to the open source currency, the Team also supports the project in several substantial respects on the de facto Monero website. The Core Team coordinates donation-based development funding, manages the project's Github merges, and conducts scheduled hard forks every six months. Details on hard forks are announced via the Monero website. This practice of regular hard forking has made forks more a norm than exception with Monero and can speed up upgrade adoption periods. Monero has departed from the scheduled forking in certain cases, such as with the release of RingCT functionality.

The Monero Network

Broadly, the Monero cryptosystem is similar to that of other Proof of Work cryptocurrencies, such as Bitcoin. However, Monero also uses a combination of cryptographic techniques to provide strong privacy and fungibility guarantees for XMR transactions. At a high level, these techniques obscure wallet addresses, transaction amounts, and transaction history for all users. All Monero transactions are private by default, in contrast to the optional private functionality of zCash or Dash.

How Monero Functions



Visual elements are for informational representational purposes only and do not accurately portray quantities or ratios of actors within the ecosystem

PRIVACY DETAILS

Stealth Addresses obfuscate account balances and transaction history. Intermediary addresses are created for one-time use in an XMR transaction. Neither party can see each other's transaction history, and the transaction histories of a particular XMR token cannot be traced.

Ring Signatures obfuscate which address sent XMR in a transaction. A ring signature is a type of digital signature that enables anonymous endorsement. Any member of a group of users that each have keys can perform a ring signature. One can thus infer, from a ring signed message, that someone in a particular group endorsed the message, even when one does not know who signed.

Ring signature keys for an XMR transaction mix the sender's valid transaction key with 5-10 unrelated keys ('mixins') from previous transactions, which are themselves obfuscated and not associated with the same wallet address. The entire ring signature confirms a valid transaction, but it is not possible to differentiate which key was the true signer and which were the unrelated keys. This architecture grants the true signer of a Monero transaction plausible deniability in any associated illicit activity. Early Monero wallets did not require the use of mixins, allowing some early transactions to be de-anonymized.

Ring CT signatures obscure transaction amounts for each entry in the ring signature, and were implemented as a protocol extension in a January 2017 hard fork that obscured transaction amounts for each entry in the ring signature, in addition to obscuring the transaction address. More information can be found in the original whitepaper.

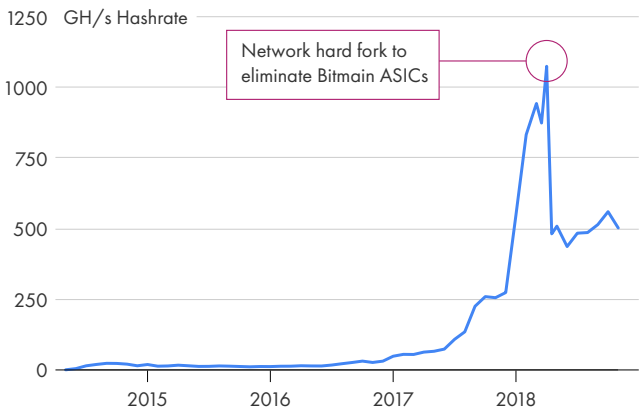
SCALING STRATEGIES

While the stealth address and ring signature technology affords strong privacy guarantees for users, it also contributes to a rapidly growing blockchain size, as encryption data for each transaction must be stored on chain. To address this issue and allow Monero transactions to scale, the network implemented bulletproof signatures in late 2018. Bulletproof signatures reduce the amount of information stored on-chain in the implementation of ring signatures, and the associated data structures scale logarithmically rather than linearly. At a high level, this proof technique allows the network to verify the validity of transactions and reject double-spends, using a simpler cryptographic proof than the previous RingCT implementation. Following the launch of bulletproof signatures, the average transaction fee dropped by 95%.

MINING AND NODES

Monero uses PoW mining to validate transactions and reach consensus on transactions' chronological order. Radeon produces most of the high-end GPU mining hardware used in mining XMR, and many miners use the XMR Stak mining software. GPU mining in general is viewed as more profitable, though some

Monero Network Hashrate



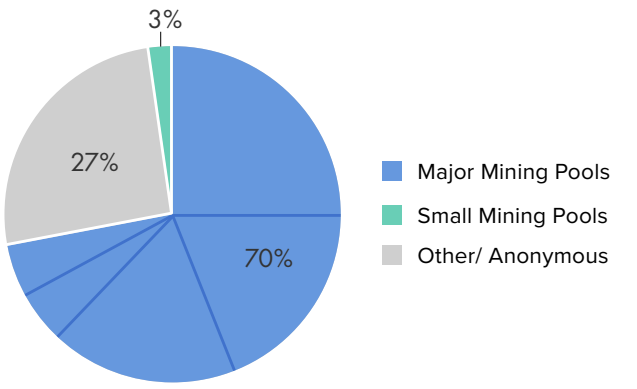
Source: BitInfoCharts

suggest CPU mining is feasible with Monero. Top line hardware, such as Radeon's XFX R9 295X2 graphics card, achieves a hash rate of 1800H/S at 500 W power consumption. Mining pools are commonplace and a breakdown of many pools' contribution to the network's total hashrate can be found here.

Monero's CryptoNight hashing algorithm has been hard forked to combat ASIC mining, which is perceived to have centralizing effects. Whether future forks, intended to prevent the re-emergence of secret ASIC mining, will be sufficient to discourage the practice, or whether concerns over ASIC-based 51% attacks prove overblown remains to be seen.

Monero full nodes can be run on a simple Raspberry Pi device, vastly lowering the computation requirements for storing and syncing the chain through the use of LMDB technology. Monero nodes are currently broadly distributed throughout the world, though the privacy-focused community of Monero likely means the real physical location of nodes is well hidden.

Hashrate Distribution November 2018



Source: MineXMR.com

The Cryptoeconomics of Monero

Monero follows a cryptoeconomic model similar to that of Bitcoin: block rewards subsidize mining activity, with a decreasing block reward designed to be overtaken by transaction fees. There was no premine or token sale.

XMR TOKEN FUNCTION

XMR is intended as a general-purpose private cryptocurrency. Users who hold Monero can send it to others on the Monero network. Holding XMR is not required to run a node, to mine, or to participate in the community.

XMR SUPPLY AND DISTRIBUTION

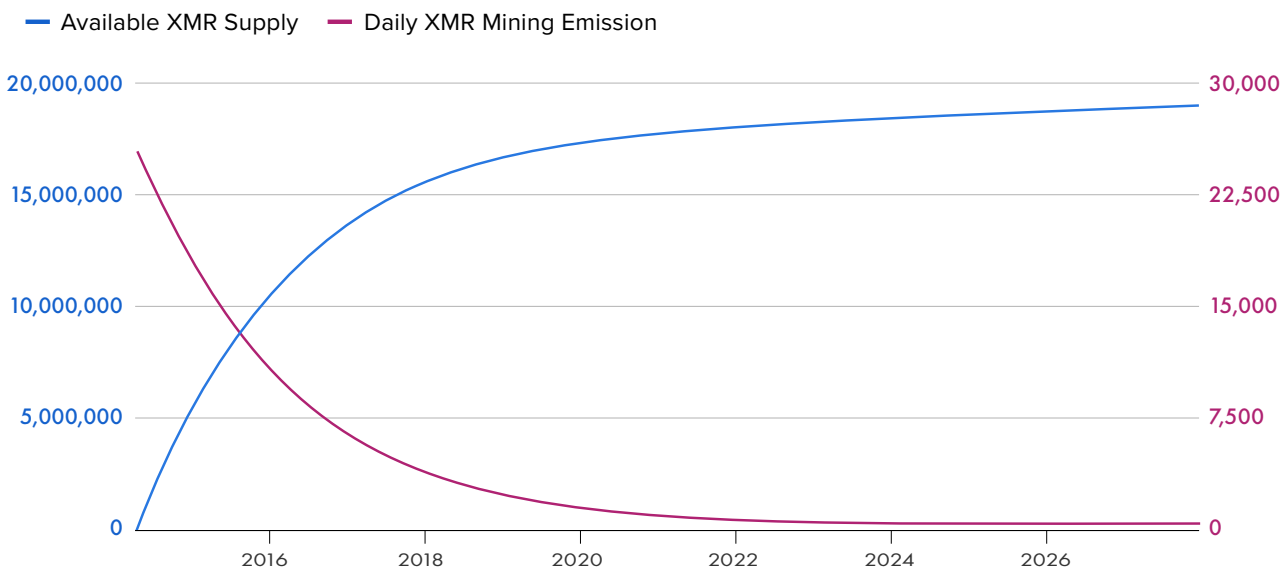
Monero does not have a fixed block size like Bitcoin, and instead employs a dynamic block size to adjust to variations in transaction demand. The maximum block size is set at twice the median of the last 100 blocks, and miners incur a penalty in block rewards if the block is greater than 60 kb. The penalty scales quadratically, such that minor deviations are not significantly punished; as the block size approaches twice the trailing median, the subsidy approaches zero. This approach allows the block size to gradually

Monero follows a cryptoeconomic model similar to that of Bitcoin: block rewards subsidize mining activity, with a decreasing block reward designed to be overtaken by transaction fees. There was no premine or token sale.

increase if the mining fees offset the subsidy. The Monero block reward was changed in 2016 when the network changed the target block times from one minute to two minutes. The per-block reward changed but the per-day emission did not.

The mining penalty only activates if the block size exceeds a set constant, currently 60 kb. This parameter may be altered by the community, which allows the block reward to continue subsidizing mining and the network capacity to scale without relying on transaction fees. The network often runs above this penalty threshold. Since the Monero block size is dynamic, there is no explicit maximum

XMR Available Supply and Daily Emission



transaction capacity and it is instead limited by bandwidth and memory constraints of nodes. Some estimates place capacity at up to 1700 TPS, though there is concern that some nodes would be excluded from participation at this level.

GOVERNANCE

Monero, like Bitcoin, relies broadly on independent developer's contributions and network hard forking to govern core network changes. Monero's Core Team facilitates development by providing a discussion forum and vetting donation-soliciting proposals, allowing donors to anonymously back development initiatives. Between 2015 and October 2018, over 65,000 XMR of estimated 1.2 million USD value was raised and directed to initiatives that have since completed. The project also conducts regularly scheduled hard forks, making forking a norm rather than exception in the community.

HOW DOES MONERO CHANGE OVER TIME?

Monero's software changes occur via scheduled 'network upgrades', which are hard forks used to implement new features. While hard forks can be a rare occurrence in other chains or viewed with a certain stigma among some crypto communities, Monero's practice of regularly scheduling hard forks is not completely unique across the ecosystem, with chains such as Bitcoin Cash also utilizing this method of development. Monero's 'network upgrades' occur regularly in April and October. Three months prior to a new release, developers create a new release branch of the current Master on the project's Github page. Developers meet regularly via the project's Github and Slack channels and meeting minutes are publically released on the website. One significant implication of the practice is that anyone participating

> Regularly scheduled hard forks are thought by some in the community to be good practice, forcing users to make the security updates and bug fixes necessary for improving overall network health.

Overview of Monero's Governance Processes

	Proposal	Discussion	Decision	Checks & Balances
Software Upgrades	Anyone can propose functionality additions on forum.	The Monero Forum serves as a focal point.	Regularly scheduled hard forks.	Community adoption of forks.
Funding Allocation	Anyone can solicit via a proposal.	The Monero Forum Core Team vets proposals, and determines readiness for open donation.	Individual donors decide what projects to back.	Some projects use milestone based payments.
Personnel	There is a Monero Core Team, but the team's relation to the project is ambiguous. • There is no defined process for Core Team selection. • The Core Team has several powers: it can merge changes to codebase in Github, it can schedule hard forks, and it can vet funding proposals to better facilitate donor/developer pairing. • The community can check the Core Team's influence through hard forks.			

in the Monero ecosystem must pay attention to governance and discussion; there is no 'autopilot' as a node or miner.

Regularly scheduled hard forks are thought by some in the community to be good practice, forcing users to make the security updates and bug fixes necessary for improving overall network health. Others in the community are more critical of the process by which such software changes are approved or rejected. Developers for Monero 0, a fork of Monero, are explicitly critical of the current practice of scheduling hard forks, claiming: "We believe that Satoshi's proof-of-work is the only mechanism for decentralized consensus. The so-called 'network upgrades' that are centrally mandated by the Monero Project are a Trojan horse designed to compromise the effectiveness of proof-of-work in the Monero network."

HOW DOES THE FORUM FUNDING SYSTEM WORK?

Monero's Forum Funding System is a process for proposing new ideas for Monero features, tasks, or services, vetting those ideas into concrete proposals and soliciting anonymous donations to fund development work. Stages in the process include:

- **Idea Generation**
  Ideas for a feature, task, or service are pitched and discussed in an initial forum.
- **Open Tasks**
  After ideas gain support on the forum, the proposals are moved to a second forum where developers or other teams who would implement the idea create pitches— detailed descriptions

that explain how the idea will be implemented and that identify project milestones.

- **Funding Required**
  Adopted ideas whose pitches gain support in the community are moved to the Funding Required forum, where donors can choose to back projects using XMR.
- **Work in Progress**
  Ideas that receive sufficient funding are moved to the Works in Progress forum, where progress is monitored and discussed.
- **Completed Work**
  Projects that are completed are move to the Completed Work forum, which provides a record for funds raised.

WHO AND WHAT IS THE MONERO CORE TEAM?

Monero is an open source cryptocurrency and the Core Team's relation to the project is not straightforward. Although the Core Team is a set of distributed pseudonymous individuals with loose affiliations to the open source currency, the Team also supports the project in several substantial respects on the de facto Monero website. The Core Team coordinates donation-based development funding, manages the project's Github merges, represents the project in press interviews, and conducts scheduled hard forks every six months. The Core Team is currently lead by Riccardo 'fluffypony' Spagni. There is not a public, defined process for adding or removing members of the Core Team. The team did announce that it has internal requirements, one being 'sufficiently active', and that former team member 'tacotime' stepped down for this reason.

In theory, any developer could hard fork Monero's open source code to implement new software features and release the new fork as Monero. Monero's Core Team is, in respects, just a team of developers that has been successful in getting their hard forks to be identified with Monero. Developers and the community—most influentially, exchanges, nodes, miners, and users— can exercise oversight over the Core Team in the sense that any other team of developers could, in principle, create a new hard fork that becomes identified with Monero. Likewise, the community could also refuse to adopt the Core Team's latest set of software changes while also getting the old chain, rather than new, to be identified as the Monero.

In theory, any developer could hard fork Monero's open source code to implement new software features and release the new fork as Monero. Monero's Core Team is, in respects, just a team of developers that has been successful in getting their hard forks to be identified with Monero.

While, in principle, any other development team could offer its own set of 'network upgrades', whether such efforts could, in practice, achieve the same adoption and perceived project continuity is another question. The Core Team's influence over Monero's direction was perhaps most vividly demonstrated when Riccardo "fluffypony" Spagni possibly influenced XMR's price through a fake 'major updates' announcement. The incident raised concerns over price manipulation and insider trading, and suggests, despite the team's attempts to distinguish itself from the project, that the community may not view the Core Team's actions in the same light as other developers'.

For further details, an informative overview and analysis of Monero's governance can be found here.

Monero vs. Key Crypto Projects

RELATIVE TO BITCOIN

Monero resembles Bitcoin in its vision as a general purpose cryptocurrency, but has default private transactions, stronger fungibility guarantees (that is, each XMR is identical and indistinguishable for all other XMR), and may be less susceptible to centralization of mining.

- Both currencies possess similar architecture and attack vectors, broadly.
- There are stronger fungibility and privacy guarantees in Monero. Bitcoin is not designed to offer privacy features; each Bitcoin is publicly associated with both its current owner's Bitcoin address and a history of all addresses that previously owned it. This makes it possible to 'blacklist' Bitcoins in a way that is not possible with XMR.
- Monero's PoW mining is less susceptible to centralization through its emphasis on ASIC resistance. Monero's hash algorithm is designed to be memory intensive and difficult to develop ASICs for, but the Monero network's overall ASIC-resistance is more manifest in its community's commitment to changing the hash algorithm through hard forking, as they did when Bitmain developed an ASIC for the original Cryptonight hash algorithm.

RELATIVE TO ZCASH

Monero resembles zCash in its vision as a general purpose privacy-focused cryptocurrency, but Monero has default privacy, no formal governance or funding model, and no lingering questions about its trusted setup.

- All Monero transactions are private by default, whereas zCash is designed to offer optional private transactions with zk-SNARK technology.
- zCash's privacy guarantees and emission through zk-SNARKs are dependent on the trusted setup's efficacy, in which a distributed group of zCash team members and external parties generated the cryptographic keys needed to initialize the network. If the secrets used to generate these keys were not properly destroyed, they could be used to de-anonymize zCash transactions or mint new zCash now or in the future. Though this scenario can never be disproved, there is no compelling evidence to date that the trusted setup has been compromised.
- zCash's Foundation and founder reward provides a more centralized governance structure and more regular funding for implement new features compared to Monero's donation system and minimal structure.

RELATIVE TO DASH

Monero resembles Dash in its vision as a general purpose privacy-focused cryptocurrency, but it has stronger privacy guarantees, default privacy, and no on-chain governance.

- Monero has stronger privacy guarantees by default and has no masternode intermediaries, who may be able to collude to de-anonymize private send transactions that they process.
- Dash is designed to offer optional private send functionality, though this functionality has been recently de-emphasized.
- Dash's treasury based decentralized autonomous organization (DAO) offers a funding source for project development that is not dependent on courting donors or investors, provides a codified process for community informed funding decisions, and to some extent disambiguates teams' and contractors' relations to the project.

Prospects and Challenges

In the long run, Monero's adoption as a general-purpose, legally compliant cryptocurrency for individuals and licensed businesses is improbable, as most monetary authorities globally appear to be antipathetic to anonymous transactions. Success for Monero will likely involve being the de facto currency for black market, darknet, and fringe private transactions globally. This is still a massive market, as darknet markets and grey markets (i.e., tax evasion & money laundering) are widely demanded and used, but remain difficult for law enforcement to comprehensively shut down.

Yet, in the near term, Monero is in many ways a model cryptocurrency: the project offers a highly functional, secure, decentralized cryptocurrency with clear use cases, widespread community support, and a fluid team of active developers. While the likely endgame for Monero is as a currency for activities deemed illegal (though money laundering alone is still a trillion dollar market), it is also possible that it gains more general adoption amongst privacy-focused users and investors. Monero may particularly appeal to philosophical proponents (often drawing from cypherpunk, libertarian, and anarchist ideals) of the original conception of Bitcoin and cryptocurrencies more broadly, as it offers a highly functional network broadly similar to that of Bitcoin. For a user or individual investor who sees value in Bitcoin broadly but is dissatisfied by its approach to issues such as centralization of mining or privacy, Monero may offer a compelling alternative.

RISK FACTORS

Monero's long-term ability to succeed as a black and grey market currency could be undermined should any of the following occur:

- **The underlying Monero cryptography breaks.** One instance of de-anonymization could reduce confidence among the community and have significant destabilizing effects.
- **A government entity shuts down the network for the network's role in facilitating large-scale money laundering, financing terrorism, or related activity.** A government sponsored 51% attack is a potential attack vector. Monero's focus on maximal ASIC resistance through repeated hard forks could prove helpful here, as control of mining power can be more distributed and more resistant to a coordinated attack.
- **Adversarial attacks on network edges succeed in de-anonymizing Monero transactions.** While the Monero privacy layers are comprehensive within the network, external touch points, such as IP addresses or physical privacy risks, may be able to de-anonymize transactions. Monero is not a comprehensive or 'full-stack' financial privacy solution.
- **Entities or platforms that provide liquidity could shut down or not support XMR markets so as to avoid regulatory risk.** Without a liquid market, it is not clear how much an XMR is worth, undermining its use as a currency, and it could be more difficult for would-be users to acquire. Gemini is an early example of a regulated centralized exchange choosing to list zCash, but perhaps only could do so compliantly because zCash has selective transaction disclosures. It is not clear that XMR access could be facilitated through a DEX solution.

MARKET OUTPERFORMANCE SCENARIOS

XMR may outperform the broader market for cryptoasset investments in the following scenarios:

- **Fungibility concerns with BTC or other cryptoassets.** As a censorship resistant, non-sovereign store of value & medium of exchange, XMR's value proposition is broadly similar to BTC, though with higher privacy and fungibility guarantees. Institutional investors may have concerns with BTC fungibility and public association with illicit transactions, motivating demand for XMR as an alternative. While Monero as a network is associated with illicit use, a particular XMR token cannot be directly tied to this. There is no distinction between 'clean' and 'dirty' Monero. Institutional investors still seem unlikely to pick up XMR, given the network's public perception, but wealthy individuals could accumulate XMR without fear that any particular XMR could be identified as 'dirty.'
- **Black or grey market demand.** Continued or increased demand for private, 'off-shore banking' services could influence XMR's value, and increase in demand would perhaps be precipitated by a broad financial crisis, geopolitical instability, or national trends towards mass-surveillance states.