Monero FAQ (from ChainTalkTV AMA)

1. When was Monero founded?
    a. Monero was created in 2014 as a fork of a project called “Bytecoin” by a small community of developers. Monero is not a fork of Bitcoin, and uses an entirely new codebase called “Cryptonote” that has evolved into the Monero protocol.
2. Does Monero have employees/is Monero created (or funded) by a company?
    a. Monero is not a company (and has no company behind it/funding it), but is a decentralized open-source project. Anyone is welcome to contribute to the project, and the community comes together to fund contributors that show their value to the project via ccs.getmonero.org.
3. How would you describe Monero in one sentence?
    a. Monero aims to provide real privacy, by default, enabling the future of digital cash while protecting each users right to financial privacy.
4. How many community members are there in Monero?
    a. Hard to say specifically as the Monero community is so diverse, but here are some rough numbers (as of 07/2020):
        i. Reddit: 175,000 members
        ii. Twitter: 320,000 followers on the “official” account @monero
        iii. IRC: 500 members
        iv. Discord: 500 members
        v. Telegram: Unknown at this time, as there are several TG groups run by community members.
5. What is the role of the Monero community in the project?
    a. The Monero community is entirely in charge of Monero as a project as all contributions, funding, and decisions are made by and for the Monero community.
6. What technology does Monero use to provide privacy to it’s users?
    a. Monero provides privacy by default via a set of technologies termed “Dandelion++”, “RingCT” and “stealth addresses” (among others):
    b. RingCT: this technology hides all amounts sent and received on-chain, as well as hides which output is actually being spent among (currently) 10 others. This requires no coordination (unlike CoinJoin) and happens entirely via the protocol itself.
    c. Stealth addresses: this technology hides sender and receiver addresses on-chain by letting the sender generate a one-time address using the receiver’s public key, so no actual addresses are ever published to the blockchain.
    d. Dandelion++: This technology helps to hide the sender’s IP address when sending Monero by using a special method of relaying transactions to other nodes.
7. How can Monero be used today?
    a. Users can use Monero with any Monero wallet and get the default privacy guarantees with no extra effort. It can be used just like Bitcoin or any other cryptocurrencies to transfer funds, pay for things, or protect wealth against inflation.
8. Where can people use Monero?
    a. There are many places that take Monero, and a good list of merchants can be found here:

        i. https://web.getmonero.org/community/merchants/
9. Why do we need coins that preserve privacy like Monero?
    a. Bitcoin enabled pseudonimity online, which many thought would be sufficient, but we have since learned that it is easy to trace users on Bitcoin. This can lead to censorship of users, funds being "tainted" (worth less than other funds because of their history), and malicious attacks by others who learn how wealthy you are.
    b. Cryptocurrencies need privacy as a default assurance to make sure that they remain censorship-resistant, allow for free spending without surveillance (like cash), and allow users to not have to worry about whether their funds are "tainted" (like cash).
    c. Monero is digital cash for a cashless future.
10. In our lives, privacy needs to be protected many times, but sometimes it needs to be open and transparent. Will anonymous coins be used improperly in places that should not be used? What do you think?
    a. As these networks are meant to be censorship-resistant and permissionless, all of them could be used in ways that could be deemed illegal in some jurisdictions. This is a side effect of a permissionless network and is not something that should be able to be stopped.
    b. Currencies outside of cryptocurrency are also used for "illegal" activities, but that doesn't discount the value that they bring to our lives by allowing us to transact online safely and without censorship or surveillance.
    c. Monero users can choose to reveal their transactions using what is called a "view key", and so are able to allow governments, tax agencies, and business partners to see transactions as needed. This is called "opt-out" privacy and allows users to remain private by default and only disclose the information they need to.
11. What if Monero is used by "bad guys" to do illicit things?
    a. Many other existing currencies (like USD) are used for illicit activities like funding terrorism, but that doesn't invalidate the value they bring to the world.
    b. As mentioned above, Monero has no power or ability to control or monitor the way that Monero is used, as it is a censorship-resistant and permissionless currency, similar to cash.
    c. The Monero community has actively tried to help prevent and alleviate illicit uses of Monero, like the Monero Malware Response Workgroup:
        i. https://mrw.getmonero.org/
12. How does Monero compare with other "privacy coins" like Zcash and Dash?
    a. Monero is private by default, which means that *any* user on the network gets strong privacy guarantees without any extra effort or cost to the user.
    b. I like to refer to this as "real privacy" instead of "potential privacy", as optional privacy (like in Dash and Zcash) fails to see adoption and usage, and has many ways you can ruin your own privacy going in and out of their privacy tools.
    c. Zcash has very strong privacy tools, but as it is opt-in (instead of opt-out) like Monero, it sees little to no usage.
    d. A great resource on these comparisons can be found here:
        i. https://twitter.com/JEhrenhofer/status/1273013390580109321?s=20

13. It seems like Monero operates differently than a lot of projects. How does the community-based model work, and what role do entities like the Monero Research Lab play?
    a. The Monero community is entirely self-funded via a tool known as the CCS (ccs.getmonero.org), and so all developers, research lab members, and paid community leaders are funded by the donations of others in the community. This means that the community has full oversight on what goes on in the project and each member is able to fund (or not fund) whoever and whatever they wish.
    b. The Monero Research Lab is a key part of how Monero functions and is a set of researchers who work to create and improve on the technology used in Monero (and other cryptocurrencies) via detailed cryptographic and mathematic work. They are also entirely funded by community donations.
14. What are the benefits of mining Monero?
    a. Anyone with a personal computer can mine Monero, as Monero is an ASIC-resistant coin. The best tool for mining Monero is currently a program called “XMRig”, which can be found here: xmrig.com
        i. It’s important to note that this isn't just another supposed ASIC-resistant algorithm; it was built from the ground up and audited four times by separate auditors.
    b. Monero is best mined with CPUs (not GPUs), and so is approachable by all users who own a normal computer.
    c. More info can be found here:
        i. https://web.getmonero.org/get-started/mining/
15. What is the difference between Monero mining compared to Bitcoin?
    a. Bitcoin mining is controlled by ASICs, and so is out of reach for most users. Monero uses an algorithm called “RandomX” to allow anyone with a computer to have a meaningful share of the network when mining, which means they get rewarded with their fair share of the block reward.
    b. This approach to mining further enables decentralization and censorship-resistance, as more entities are mining Monero in more diverse locations around the world, with more diverse hardware.
16. Does Monero support decentralized applications (dApps)?
    a. There are no “dApps”, specifically, but there are many tools built using Monero like minko.to, and an upcoming project called Tari (https://www.tari.com/) which will be for digital assets and non-fungible tokens (like tickets and collectibles).
17. How is Monero working to improve adoption?
    a. Improving adoption is up to the community, so it relies on community members talking to their favorite merchants about accepting Monero and talking to their friends about the benefits of a coin like Monero over Bitcoin and others.