An Introduction to Private Cryptocurrencies: Monero and Its Alternatives (v 0.5)

A new wave of decentralized, private, and digital cryptocurrencies will forever change the power structures of the world in which we live. They will give untold autonomy to the individual to live a unique life while also inextricably linkinging together the actions of all of humanity in a truly global society. As with any complex system, it's impossible to foretell the exact implications of such drastic societal changes, but the possibility for a radical update in how we live is exciting to say the least. In this essay, we will explore the philosophical and technological background of such currencies, with a particular focus on Monero, which I believe to be the frontrunner in this race. The essay will use the following structure centered around three questions:

1) Why is a global decentralized, private, and digital cryptocurrency important?

- Part I. Space to Be: Why Privacy Matters
- Part II. Sound Money: Conditions for Autonomy

2) What options exist to fulfill this role today?

- Part III: Intro to Monero and How It Works
- Part IV: Other Anonymous Cryptocurrencies

3) How can you get started using and advocating for such a currency?

- Part V: How to Buy, Store, and Use Monero
- Part VI: Concluding Thoughts

I do not claim anything here to be perfect or fact. I, like you, am merely an interested citizen exploring topics and technology that I find fascinating. All feedback, including corrections, counterarguments, and better technological explanations, is welcome. This is a living document that will improve based on the comments and ideas of many. Feel free to contribute your feedback here: **cypherperro [at] protonmail.com**

Please note that parts II - IV assume some basic knowledge of Bitcoin. Read here for a quick primer on Bitcoin's technology and impact.

Part I. Space to Be: Why Privacy Matters

What is privacy? Why does it matter?

I have found that most people have strong visceral reactions to these questions, but often struggle to explain why they feel the way they do, myself included. Here's my working hypothesis for why privacy matters: privacy is necessary for human experimentation or iteration.

As human beings who have tasted the fruit of knowledge, we have developed the ability to reason, to create abstractions, to plan, to consider possible worlds. These incredible feats have created the wonders of modernity, what most would deem “progress” -- agriculture, cities, aircraft, the Internet. They are also the source of all human suffering. When we desire to be something we are not, we can never be happy or content.

So how does this relate to privacy? Because you cannot determine who you are without the ability to experiment freely, to push boundaries, to test societally held norms. Think about your own speech. Do you feel different expressing yourself to strangers than to your friends than to your diary? Would you want every thought or action you’ve ever taken broadcast indiscriminately to the rest of the world?

I believe there are two answers to this question. Either you answered yes, in which case you believe in the ideal of radical honesty. This may be the best answer of all. You’re comfortable with saying or being exactly what you feel in in any individual moment, regardless of the consequences. Maybe that means you’re ok going to jail, ending a relationship, or even dying. And I’m actually open to the idea that living in radical honesty without fear of consequences is actually the ideal for which we all should strive. But for those who are not quite there yet, perhaps because they’re still experimenting with their thinking or because they don’t want a corporation, family, or society with whom they’re not sure they agree to restrict their livelihoods, they will likely prefer the ability to at least experiment in private.

And experimenting without fear of judgement (including your own) is critical to create anything new or different. To see the world as it really is. Say for example that you wish to experiment with a long held societal belief such as: the world is flat, we need bankers to orchestrate complex financial workings, that there is one divine entity whom all should worship as God, or that evolution is driven purely by chance.

A society that monitors and punishes heretics cannot make progress. To be clear, I am not arguing that any particular belief is bad or good, but rather that in order for society to know more about how the world (or each person’s individual existence) functions, one must be able to run experiments to find truth for oneself. If you are indoctrinated into believing someone else’s unfalsifiable truth or, worse, are completely restricted from creating your own experiments with truth to determine whether or not you agree with that belief, then new truths cannot be uncovered. Or at the very least they will be uncovered by far fewer people resulting in a much slower iteration cycle for humanity at large. And this cycle of iteration, of change, of re-birth is exactly what the universe does. It is the inner workings of evolution itself, the defining feature of existence.

So far, everything I’ve written is rather abstract. Let’s consider some real-world examples. Say you live in a country under rule by an oppressive regime where your access to information, networks, and ideas is heavily monitored and restricted. When you’re afraid to even access a

piece of information which may fundamentally alter your thinking about the world for fear of blacklisting or retribution, you are unconsciously limiting your own development as an individual. As the situation worsens, you may no longer have the means to organize with your fellow citizens to prevent living in a state where you are unable to listen to your favorite music, read your favorite books, or talk openly with your friends. You lose your individuality for false security under a monoculture state.

Or consider a more realistic scenario for those living in the West: you use a “free” social networking or search service that is wholly controlled by a for-profit corporation (hello, Facebook and Google!). Such corporations have the ability to track every interaction you make within (and often outside of) their service such that they can censor what information you receive and suggest what you purchase and with whom you interact. Some may actually like these services as it makes life “easier.” And that’s all well and good if you’re making the privacy for ease tradeoff knowingly, but how many know that apps like Facebook passively record your conversations today, even when you’re not using the app? How many fully understand the consequences of giving all of their data to corporations who have one motive and one motive only: make more money, even if that means using your data to create a product with cigarette-like addictive qualities? How many realize that these corporations will easily turn over this data to government regimes with whom you may disagree?

If all of these ideas still sound too lofty and abstract, think on this: would you want your worst enemy to have complete power to determine what is deemed safe or unsafe for you to think, read, or do? These extreme cases demonstrate most powerfully of all why privacy or freedom of thought matters.

A few caveats I would like to add: I do not consider myself a libertarian. In fact, I’ve found many self-proclaimed libertarians to be selfish and unpleasant company. I believe not only in individual agency and responsibility but even more so in the value of compassion. The golden rule I suppose.

I am also not naive enough to think that all people are inherently altruistic or good, though I think most are. There is no question that privacy or anonymity will help some bad people to do bad things. But I also recognize that many bad people do bad things today without such privacy. Many of these bad people and things are actually endorsed by powerful corporations or governments (e.g. genocides or recklessly accelerating climate change).

Finally, I recognize that there is no such thing as utopia. Especially not one that’s planned from above for a complex system like human society. I believe that the best gift we can give humans is autonomy. Autonomy to discover their own inner voice and desire. Autonomy to experiment with different versions of themselves. Autonomy to be. This autonomy should, however, have limits or associated responsibilities as well. The debate between where one person’s autonomy ends and the rights of another begins is one of the oldest in political philosophy. It is, of course, driven heavily by one’s conception of the self (whether it is more individualistic like in the West

or more distributed like in the East). I do not think there is any way to design a system that answers this question correctly. The best we can do is run experiments and see how the system naturally grows or evolves. And I believe we must start by giving people more autonomy to experiment in their own lives. And that autonomy begins with digital privacy - privacy of information, communication, and commerce.

There is much to say about the realms of information and communication. And, indeed, these topics have been explored recently with a high profile thanks to the WikiLeaks and Snowden cases. We may revisit these topics in future essay, but for today, we will focus on the area which has received the least musing: commerce.

Part II. Sound Money: Conditions for Autonomy

In the realm of commerce, privacy is a great first step toward establishing individual autonomy. But it is not, in itself, sufficient. Truly autonomous individuals must have access to money that is, in the words of cryptocurrency analyst CryptoIzzy, "sound." Sound money is money that cannot be arbitrarily manipulated or censored by any outside party. Sound money must meet four conditions:

- 1) Medium of Exchange - you can exchange the money for goods and services. The more portable the money, the better.
- 2) Unit of Account - you can use the money to measure the cost of different goods and services. It must be uniform and divisible, meaning that you can subdivide each unit of money and that each comparable sub-division has the same value.
- 3) Store of Value - the money maintains its value over time, which means that there's a limited supply of it and that it can't perish.
- 4) Fungibility - each unit of the money must be identical to each other comparable unit of money. In the ideally fungible case, there is NO WAY to differentiate one unit from another. Note that such uniformity requires anonymity, as any identification can ultimately lead to differentiation.

Money with these four characteristics allows for societal experiments with autonomy as individuals are able to transact privately with a currency supply that cannot be arbitrarily manipulated, devalued, or sanctioned. To better understand these requirements, let's examine three potential candidates for sound money -- government issued fiat currencies (Dollars, Euros, etc.), Bitcoin, and gold.

Government issued fiat currencies meet conditions 1 and 2 - you can use them to buy almost any goods and services and subdivide them into to small amounts. In the case of physical cash (which is being phased out around the world in favor of digital money), it even mostly meets condition 4 - there's no practical way to tell two hundred-dollar bills apart, which is why the

majority of the world's illegal trafficking is done in dollars.[1] Fiat currencies do not, however, meet condition 3 (store of value) because central banks can print money indiscriminately, which is what causes inflation. Although this hasn't been a publicly visible issue in places like the U.S. (although an average of ~2% per year quickly compounds), one need only look to areas with hyperinflation like Weimar era Germany or modern day Venezuela to understand why fiat currencies do not meet this condition.[2]

Bitcoin meets each of the first three conditions - you can exchange it for goods and services (more and more every year), it's divisible to the hundred millionth place, and there will only ever be 21 million bitcoin in existence. Note that while Bitcoin does meet the condition for unit of account -- it is indeed uniform and divisible -- it does not meet the condition for fungibility because each unit of Bitcoin has a traceable history. Because each unit of bitcoin refers to a specific piece of the Bitcoin blockchain, you are never paying for something with bitcoin generally, but rather with an identifiable unit of bitcoin.[3] This means that someone with advanced blockchain analysis technology could uncover the identity of a Bitcoin user with only the digital breadcrumbs left behind by IP addresses, timezones, and other interactions with insecure third parties. In fact, it was reported in 2017 that the US government is already working with a large enterprise software company to do just that. All it would take is for this technology to fall into the hands of the wrong corporation or political administration to result in an edict banning anyone, under threat of censorship or violence, from accepting a particular chunk of bitcoin that had previously become "tainted" in their eyes.

Gold, which has been used as money for millenia, meets all 4 of the conditions above. You can use it to buy goods and services. You can melt it and re-shape it into small or large quantities. There is a limited supply of gold on the earth and there is no way to tell apart two bars of melted gold. The problem with gold is that it only exists physically, meaning it's hard to transport and

---

[1] Note: Dollar bills do have serial numbers, but it's impossible to see a complete history of how a dollar bill has changed hands, meaning you can at best know a few points in the dollar's life.

[2] Some readers have raised two potential criticisms of this argument that fiat currency does not meet the condition for "store of value": 1) inflation is low enough in most of the developed world to be irrelevant and 2) some inflation is good for society to encourage spending vs. hoarding. These are both valid points and while I don't claim to be an authority on economics, here are my initial responses: 1) inflation is traditionally low in developed countries - while this is true, A) even ~2% annual inflation can lead to huge wealth disparity in only a few decades (see CryptoIzzy's aforementioned essay showing how such a rate can result in < 1% of society controlling > 50% of the society's wealth in just a few decades). Note that it is mostly the classes who don't hold assets that keep value with inflation who are affected. B) Even if 2% inflation is acceptable, there's no reason to believe that any particular state or society is immune from turning into Weimar era Germany or modern day Venezuela. Global political and economic conditions can change much faster than we believe and it's naive to think that any group or state holds a special place in history. Re: 2) some inflation is good for society to continue spending -- I'm not certain on this point, but there are many economists who make this argument. If true, then some amount of very small, pre-programmed inflationary rules (i.e. not arbitrary inflation rates set by Central banks) should cover this concern. On page 12, I explain how Monero is trying to create just a such small and predictable amount of inflation. This seems like a good idea to test and I'm glad Monero is doing so.

[3] See here to for a more in-depth explanation of how the Bitcoin blockchain works

store. This physicality means there's an inherent limit to its velocity and adoption (e.g. there's no practical way for a farmer in Africa to send gold to an office worker in China).

In order to create a new candidate for money that meets all four requirements but that also can move rapidly among everyone in our global society, we need a currency that is:

- A) digital
- B) trusted and decentralized
- C) anonymous

Although there are several cryptocurrencies under development with aims to be just that, we will begin by examining Monero, which I believe shows the greatest promise today.

Part III: Intro to Monero and How It Works

Monero began in 2014 in a similar fashion to Bitcoin: with a message board post by an anonymous author. The initial version of Monero was called Bytecoin and began as privacy focused currency with a pre-mine, where the anonymous founder kept an initial allocation of the coins for him or herself. Philosophical disagreements led a group of crypto enthusiasts to ultimately fork the Bytecoin currency into a new currency called Monero, which retained a focus on privacy, but with no pre-mine. The word "Monero" means "currency" in Esperanto, a stateless language created in the 19th century with aims to become a new *lingua franca.*

The most notable feature of Monero is its community. Monero is an open-source project driven by technically proficient computer scientists and mathematicians more interested in ideology than any specific technology, as demonstrated by their adoption of four different technologies that together constitute Monero's privacy. You can find out more about Monero's team and open-source values here.

The rest of this section is a technical overview of Monero: TL;DR Monero uses 4 different technologies to hide the identity of the sender, the recipient, the transaction amount, and all IP addresses in a transaction. For those who would prefer to skip the technical details, you may move ahead to the next section which compares Monero to other anonymous cryptocurrencies.

Before we dive into the specifics of these four privacy technologies, let's first review the unique aspects of Monero's addresses and keys. Whereas Bitcoin provides only one public/private key pair, Monero is based on a completely different set of crypto fundamentals (drawn from the CryptoNote protocol) which features two public/private key pairs: a public/private spend key pair and a public/private view key pair. Let's define these key pairs and associated Monero addresses:

- Monero address - the Monero address is a 95 character string based on someone's public view and spend keys (see this technical explainer for more details). You can share this address publicly to receive Monero. For example, here's my Monero address:

  85KGQqMiYgEF4nKacFk2dUPz3LHcuAaSTbvZA93BHGcKRZYCR9Pyb5FCbzUXZbEN
  Pa2K71TBKtsT26tNPDfD7FN98HjxiA9

- Private Spend Key - This is the most important key - it allows anyone to send funds from your Monero wallet. It's also the first key that your wallet generates, often from a randomly generated mnemonic seed.[4] You can generate all of your other Monero keys from this private spend key. Therefore it is extremely important that you always keep this key private.

- Public Spend Key - this key is derived from your private spend key and comprises the first half of your Monero address.[5] It is used with the public view key to create a one time addresses where a sender can send you funds.

- Private View Key - Anyone with this key can see incoming transactions to your wallet (though they will not be able to see transactions sent from your wallet). It's therefore useful in situations like undergoing an audit.

- Public View Key - this key is derived from your private view key and comprises the second half of your Monero address.[6] It is used with the private view key to create the one time address where a sender can send you funds.

- Payment ID - a randomly generated 32 bit string that allows a sender to prove to a recipient that she sent specified funds. Using a Payment ID is optional and is typically used in transactions with online merchants or exchanges. In cases where you use it, the recipient would generate a one-time random payment ID which the sender would then append to their transaction to prove they've sent a specific transaction.

- Integrated Address - an integrated address uses your public address and a randomly chosen payment ID to create one new payment address. In addition to being more efficient than using a public address and a separate Payment ID, this new integrated address could also be used to obfuscate a user's public address if she so desired.

---

[4] A mnemonic seed is a random group of words that can be translated into a random 256 bit private key.
[5] Note that your key will appear different than what's in your address because your address converts your public view key into cnBase58, a fixed set of characters that makes it easier for humans to read the address and not mistake certain characters for each other, e.g. "O" for "0".
[6] The key and your address will also differ because the key is converted into cnBase58 to make the address.

Now that we've got the fundamental components of Monero addresses and keys down, let's examine the four technologies Monero uses to keep transactions private:

- 1) Ring signatures to protect the privacy of senders (untraceability)
- 2) Stealth addresses to protect the privacy of recipients (unlinkability)
- 3) Ring Confidential Transactions (Ring CTs) to obscure the transaction amount
- 4) Kovri to obscure IP addresses during transactions (note: Kovri is under development)

Note that I'll just cover the basics of how each feature works. If you would like to dive deeper, I recommend this excellent Monero explainer (complete with some helpful diagrams) from community veteran Justin Ehrenhofer.

1) Ring Signatures:

We'll begin with Ring Signatures, which hide the identity of a sender (known as untraceability). Recall that in an open, pseudonymous blockchain like Bitcoin, anyone can see the entire transaction history of any bitcoin output. That is, you can see every transaction that any address ever sends -- it's 100% transparent.

With ring signatures, instead of using one specific transaction output (TXO) from the sender's address, Monero selects a group of at least seven possible TXOs -- six decoys randomly selected from the entire Monero blockchain as well as the real output of the sender. This "ring" of seven outputs is used to create one signature such that it is impossible for an outside observer to know which of the outputs actually created the signature -- it just as likely could have been any of them. Because everyone's outputs are constantly being used as random decoys in the transactions of others, it is impossible for any third party, including miners, to determine from an analysis of past signatures which of the seven outputs was actually used in a specific transaction.[7]

[7] Note that some researchers have questioned whether or not the outputs in a ring signature are truly random or untraceable. These concerns revolve around two major potential weaknesses: A) rings with no decoys or small ring sizes can be used in a chain reaction to help identify outputs used in later transactions and B) the algorithm for selecting outputs is not sufficiently random and selects too many outputs created far in the past. Justin Ehrenhofer published a thorough response to these concerns (and others) here in March, 2018. His response outlines that Monero has already updated its software to address the vast majority of the concerns. In March, 2016, Monero upgraded its software to require a minimum ring size of 5 (and in April, 2018 they updated it again to require a minimum ring size of 7). In September, 2017, Monero underwent a hard fork to require mandatory use of RingCTs to hide transaction amounts and to update its output selection algorithm to ensure that at least half of the selected outputs in every ring were created in the last 2 days. Despite these massive improvements, Ring Signatures are still the weakest point of Monero's privacy. While they provide plausible deniability in most situations, there are still edge cases that can make certain transactions stand out. To that point, it's worth acknowledging that no privacy technology is ever perfect. New attack vectors are constantly uncovered or developed, making the goal of perfect privacy a constant dance of evolution. It's also important to remember that you need different levels of privacy for different threat models (i.e. you need different behavior depending on if your adversary is a single hacker, a medium sized business, or a powerful corporation or state). All in all,

This clever constant mixing of outputs is great for privacy, but creates a big challenge. How can we trust that an output is not being double spent (i.e. that a sender is not using the same Monero output multiple times)? Recall that Bitcoin was the first to solve this double spend problem using a proof of work mining system (see here for a refresher). In order for a proof of work blockchain to function, miners must be able to verify that a specific output has not been used before adding it to a new block.

Monero solves this problem by issuing a unique identifier for each transaction called a "key image." The process of creating a key image involves complex cryptography, but the important takeaway is that each output can create one and only one key image. Although it is impossible to tell which output created which key image, miners can verify that a key image from a specific transaction has never been used before, thus preventing doublespends.

2) Stealth Addresses:

Stealth addresses are used to protect the privacy of a recipient (known as unlinkability).

With Bitcoin, you conduct a transaction by sending some quantity of bitcoin to the public address of your intended recipient. Since the blockchain is public, the entire world can see which address received the transaction. With Monero, you never send to a public address. Instead, each transaction creates a unique one-time stealth address for the recipient.

Here's how it works: the sender's wallet uses the recipient's public view key and public spend key to generate a one time address where she sends Monero. The sender publishes this new public address and an identifying piece of data recognizable only to the recipient. The recipient uses her private view key and this identifying piece of data to check the entire Monero blockchain to see if any funds have been sent to an address for her. If she finds a stealth address intended for her, she will use her private send key to access the Monero and use it in a transaction. Creating this one time address also uses complex Elliptic Curve Cryptography. Check here if you're interested in the details.

The key idea is simple though: Monero is never sent to anyone's public address. Each transaction is sent to a unique one time address based on a recipient's public view and spend keys that only someone with the recipient's private view key is able to determine. This property means that no one will ever be able to associate a specific transaction with a specific user's Monero wallet, unless they know that user's private view key.

3) Ring Confidential Transactions (Ring CTs):

---

it seems that Monero has addressed the majority of the concerns with ring selection for now, but will certainly need to continue improving their software as future vulnerabilities are discovered.

Ring Confidential Transactions, known as Ring CTs, hide the transaction amount. When a user wishes to send Monero, she must make a public promise known as a Pedersen Commitment which commits to sending a specific quantity of Monero without revealing that amount. This is again rather cryptographically complex, but you can think of it as similar to a mass balance equation, where one proves that the total mass introduced into a system equals the total mass that results from the system. In this case, the sender is proving that the sum of her inputs, outputs, and transaction fee should all check out to 0.

Here's how it works: the sender's wallet will select both the actual outputs she's using as well as a random number and use these to create a new commitment number which is effectively a public key. Miners can check this public key to verify that the sum of her inputs equals the sum of her outputs, thus proving that no new Monero was created in the process. They also conduct what's known as a range proof to verify that all inputs were >0 to ensure she's not gaming the system with fictitious negative inputs.

The big idea behind Ring CTs is that transaction amounts are no longer publicly displayable on the network. Senders must make a cryptographic commitment providing just enough information such that the network of miners can confirm they sent the same non-zero amount of Monero they promised to send without ever actually knowing that amount. Although this feature is excellent for increasing privacy, storing range proofs takes a substantial amount of additional space (they constitute the majority of each current Monero transaction). This in turn increases the requisite space needed to run a full node or copy of the blockchain, allowing fewer people to do so and leading to increased network centralization. One exciting development on the 2018 Monero roadmap is bulletproofs, a new type of rangeproof that promises to reduce transaction size (and therefore future blockchain size) by 80%! You can read more about bulletproofs and their implementation in Monero here.

4) Kovri:

Kovri is a new implementation of the Invisible Internet Project (I2P) router that will hide IP addresses during transactions. Even if the user, recipient, and transaction amount are all anonymized, adversaries with sufficient resources can still determine information about transactors by collecting IP addresses, labels assigned to each device connected to the Internet. While you may be able to hide your IP address with a trusted VPN or Tor, there are serious safety concerns with both networks, including that you may forget to always use them.

The Monero community is developing Kovri as a default technology for Monero (although since it's open source, other cryptocurrencies or Internet traffic may access its API as well). Kovri uses what's known as garlic encryption and garlic routing to send traffic from one node to another in the network. At each hop between network nodes, the recipient of the message uses a private key to unlock what she's received revealing two further pieces of information - an encrypted message she cannot read, and the next IP address where she should send the message. Note that like onion routing used in Tor, recipients of this traffic never know the

history or final destination of the message, only the most recent sender and the next recipient in the network. Kovri's primary difference with onion routing/Tor is that you can bundle multiple messages to together (like in a clove of a garlic) such that you can leave one message to be unencrypted at one destination and continue sending the rest of the clove of messages through the network.

Kovri is not publicly accessible today, but is on the roadmap for 2018.

Monero's Other Unique Characteristics

So far, we've covered the technologies Monero uses to ensure anonymity for its users. To review, Monero includes Ring Signatures to hide sender identity by making signatures appear as if they could have originated from any of many potential senders in a group, stealth addresses to protect receiver identity by creating a one time public address for each transaction that only someone with the receiver's private view key can identify, Ring CT transactions to hide transaction amount, and (coming soon) Kovri to cloak IP addresses. Overall, this ever-expanding series of privacy protections bolsters my first and most important point about why I'm bullish on Monero. The decentralized team behind this project is comprised of technically competent, ideologically driven individuals who are on a mission to change the world. This commitment to ideology over technology means that Monero is able to embrace whatever current or future technologies or techniques best achieve the community's goal of creating private and fungible digital cash.

In addition to having anonymity built into its base layer, Monero shares a few other key differences with Bitcoin and other popular cryptocurrencies.

Dynamic Block Size

Bitcoin is currently capped at a block size of 1 MB (or ~500-2000 transactions / block depending on transaction size). This means that as network demand grows -- when more people want to send Bitcoin transactions -- but the space for such transactions remains fixed, the transaction fee inevitably increases. A few years ago, a transaction on the Bitcoin network cost only a few cents. During the height of the late 2017 Bitcoin boom, transactions could cost $50 or more during congested periods. Increasing the quantity of transactions the Bitcoin network can fit into a block requires either a hard fork, where 51% of nodes agree on a different set of rules for Bitcoin (note: these can be extremely contentious like with the Bitcoin Cash fork of 2017), or a technical hacks like Segregated Witness (Segwit) which reduce the amount of data needed/transaction in a block, thus indirectly increasing block size.

Monero takes a different approach with dynamic block sizes. Instead of having a fixed block size, Monero slowly changes its block size based on network demand. Here's how it works: the Monero network calculates the average block size over the last 100 blocks. If a miner chooses to create a block much larger than that average, then he is hit with a penalty proportionate to the

increase in kBs in the new block. This prevents miners from building unnecessarily large blocks (e.g. with their own spam transactions) or from the blockchain becoming too large too quickly for normal people to run full nodes (which leads to network centralization) while still allowing block size to increase slowly over time. See this blogpost from a Monero developer for details on how the dynamic fee is calculated.

Limited, But Not Fixed Supply

Bitcoin is based on deflationary economics. It has a fixed supply of 21 million coins that will ever be created. Miner rewards will continue to be cut in half every four years until the miner reward hits 0. Monero is based on dis-inflationary economics. This is similar to deflationary economics, but still allows for a small amount of new money to be created every year in perpetuity. Monero has an almost fixed supply of ~18.4 million coins. After the initial supply is created, Monero reaches an emission point where a fixed amount of 0.6 XMR is created as a miner reward every 2 minutes (when each new block is created) forever. In the first year, this small emission will create “inflation” of ~1% and decline every year beyond that until it is close to (but never reaches) 0%. Monero’s creators chose to include this small emission because there are legitimate concerns that a completely deflationary economy with no rewards beyond transaction fees for miners will eventually lead to Bitcoin fees going to 0 and the entire system collapsing.

ASIC Resistant Mining

An ASIC (application-specific integrated circuit) is a specialized circuit built for a specific application instead of general computing. This means that ASICs are really good at one thing and one thing only -- performing a specific computation -- just like your teakettle is really good at heating up water but nothing else. ASICs are popular in Bitcoin mining because they can run Bitcoin’s SHA 256 hash algorithm substantially faster than a normal central processing unit (CPU) or graphics processing unit (GPU). Monero’s CryptoNight hash algorithm differs in that it requires regularly accessing a meaningful amount of memory during the hashing process. The need to constantly access memory neutralizes the advantage of ASIC’s faster processing abilities meaning it is not cost effective to manufacture a Monero ASIC today. The impact of ASIC resistant currencies is that they decentralize securing the network as people with GPUs alone -- which are cheaper and more widely available than specialized ASIC hardware -- are able to effectively mine the cryptocurrency.

Part IV: Other Anonymous Cryptocurrencies

So far, Monero sounds pretty sweet! And, indeed, I believe it is. To give a fair assessment, however, I now want to cover a few competing private cryptocurrencies. It’s important to note that the crypto world moves fast with forks of old coins constantly creating new coins with new features. This is a non-exhaustive list of some of the major potential competitors to Monero today.

Bitcoin with Mixers

Overview: Services that mix people's bitcoin together to increase anonymity

The first popular cryptocurrency billed as anonymous was actually Bitcoin itself, but combined with third party mixing services that take Bitcoin inputs from multiple users and literally mix them together to fund different transactions. Imagine you and three strangers need to pay a total of four bills. Assuming you each put in what you owe (plus a fee for the mixer), the mixer will then mix all four inputs to ensure that the each bill is paid in full using a combination of the four inputs.

This solution has some merits, but is generally considered unsafe for several reasons. First, only sender data is obscured. Anyone attempting to conduct chain analysis still has recipient addresses, transaction amounts, and IP addresses to work with. Second, because mixing services are opt-in and not a default setting, the total anonymity set of all outputs using a mixer is small relative to all Bitcoin transactions. This smaller anonymity size means that A) it's easier for an adversary to break the anonymity and B) even if they can't break the anonymity, the adversary can at least identify and stigmatize any output that was used in a mixing service, claiming that it's more likely to have participated in illicit acts. So just sending your coins through a mixer can actually increase the chances of them being blacklisted in the future, even if you've done nothing illegal.

Finally, the biggest risk with these mixing services, of course, is that they are controlled by a third party. Any time you rely on a third party to keep your data secret, you've exposed your privacy to a source of breach.

Tumblebit

Overview: An anonymous, trustless Bitcoin payment hub

Tumblebit is an anonymous and trustless Bitcoin payment protocol proposed by a team of researchers at Boston University in 2016. Tumblebit allows payers and recipients to make rapid, anonymous off-blockchain payments that are ultimately settled on Bitcoin's blockchain. Tumblebit works similarly to mixer or tumbler services with one key difference. Tumblebit's tumbler replaces the centralized trusted third party responsible for receiving and executing payments with off-chain cryptographic puzzles such that it can never steal funds from senders or deanonymize any party.

Tumblebit accomplishes these feats with complex cryptographic tricks, but the main idea is that a sender can escrow some amount of Bitcoin with Tumblebit's tumbler and lock it up with a puzzle. The sender can then pay her intended recipient by giving him the solution to the puzzle. Take a hypothetical sender Alice and recipient Bob. Alice can escrow 1 bitcoin on the blockchain with Tumblebit's tumbler ("T"). T can then escrow 1 different bitcoin on the blockchain locked by a puzzle that T creates through interactions with Bob. T then interacts with Alice so that she can derive the solution to that puzzle. When ready, Alice can pay Bob by giving him the solution to the puzzle, ensuring that Alice ends up paying 1 bitcoin and that Bob ends up receiving 1 (different) bitcoin. Throughout all of this process, Tumblebit's tumbler can never steal funds or deanonymize any identity. You can read more details about Tumblebit's technology here.

While this protocol seems promising, it's important to note that it does not offer complete anonymity as transaction amounts and user IP addresses are still public. Tumblebit developers acknowledged the IP address weakness and had established a roadmap in 2017 to make it easier to use with Tor. Additionally, the best use case for Tumblebit may be as a sidechain with a main chain coin that has already implemented Ring CTs and Kovri or Lightning Network (which we'll discuss next).

Although this protocol is promising, it seems that Tumblebit development has slowed dramatically over the last year. A cursory glance at their Github repository shows little activity since 2017.

Bitcoin Second Layer (e.g. Lightning Network)

Overview: A network for small payments on top of Bitcoin that uses onion routing (like Tor)

One of the most talked about privacy improvements to Bitcoin is using a second layer like Lightning Network. The primary purpose of lightning network is actually to allow for much cheaper transactions, particularly for small purchases like buying a cup of coffee where even a $2 on-chain Bitcoin fee equals or is greater than the cost of the purchase itself.

Lightning network works with two transactions on the Bitcoin blockchain - one to open a channel and one to close it. These open channels then create a new network on top of Bitcoin where users can send IOUs (which cancel out without needing to actually be logged on the blockchain) among anyone else with whom they're connected by open channels. For example, if I have a channel open with my local cafe, I can not only use that channel to pay them for my coffee, but also I can use that chanel to pay anyone else with whom they're connected, which means I can pay my friend Pablo who frequents that same shop through their channel as if I were using Venmo or Paypal.

Exploring this tech further definitely requires its own deep dive (if interested, you can start here), but from a privacy perspective Lightning Network is interesting because it uses onion routing (the same technology behind private browsers like Tor) to send transaction data along several hops or nodes in a network before the money reaches its final destination. At each step along this network, the temporary recipient of the funds only knows the hop that came immediately before and the hop where the money is going next. And because all hops look the same, it's impossible to tell if the money you received is coming from the original sender or a random network node just as its impossible to tell if the address where you're sending it next is the final destination.

This technology will greatly increase Bitcoin's privacy, but will still not provide sufficient anonymity for fungibility. The reason is simple: even if the actual transactions on the lightning network are routed privately, there are still leaks from the on- and off-ramp transactions with the Bitcoin blockchain. Whichever address is opening or closing a channel can ultimately be identified for all of the reasons we discussed above. This means that although second layer networks are helpful, the only way to create true privacy or anonymity is at the base layer of the blockchain itself.

Dash

Overview: A lightweight currency with a built-in option to mix your inputs with others'

Dash originated as a currency called Darkcoin in 2014. Dash has a feature where its coins can be mixed together (like in the bitcoin mixer example above) directly on the Dash blockchain. Although the option to obscure sender data may be better than nothing, it still carries the same problems as the mixers above.

Again, only sender data is obscured while receiver data, IP addresses, and transaction amounts are not. Furthermore, Dash uses a network of a special class of nodes called “masternodes” to do the mixing. These masternodes have access to input and output data from mixes. If these masternodes were malicious, or more likely, spied upon by a powerful third party tracking IP addresses and transaction times, then it’s possible that all privacy could be compromised. The Dash community’s response to this concern is that private transactions use a chained approach where these transactions are sent through multiple masternodes to achieve better privacy. But with a limited number of masternodes and low private transaction volume, it seems reasonable that a well equipped adversary could break this anonymity with the data they have (and the same probably applies even with much higher transaction volume as well).

Furthermore, the low private transaction volume is largely a result of the fact that privacy is an opt-in feature for Dash, meaning that the default setting, which the vast majority of users choose, are completely open transactions. This means that some small percentage (<1%) of Dash transactions actually use the privacy feature, creating an extremely limited anonymity set and compounding all privacy concerns.

Zcash

Overview: A fork of Bitcoin that uses a brand new privacy feature that requires a trusted setup

Zcash is a legitimately interesting cryptocurrency -- it’s a fork of Bitcoin (it starts with Bitcoin’s same codebase) and adds a novel cryptographic technology called zk-Snarks (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge). Zero knowledge proofs allow one party to prove to another that she has knowledge of some specific value without revealing what that value actually is. For example, someone sending 10 Zcash in a transaction can construct a proof showing that conditions for a successful transfer were met (e.g. the sum of inputs equalled the sum of outputs, the sender used a private key with access to the unspent Zcash transaction output, and that the unspent Zcash transaction output had not been spent before) without actually revealing any of the specific data from the transaction. Normally, this proof would require multiple rounds of messaging between the prover and the verifier to successfully make this case. zk-Snarks, however, are a new implementation of this zero knowledge technology that allows the proof to be created in just one message (i.e. sufficiently succinctly and quickly to be used on a blockchain).

This technology is extremely exciting and could change the entire field of cryptography. There are, however, some critical (and I believe deal-breaking) weaknesses with this technology and Zcash as a cryptocurrency. Most importantly, the only known way to implement this zk-Snarks technology today requires a trusted setup where a private key is created that could be used to mint unlimited amounts of the cryptocurrency without anyone knowing. Zcash tried to get around this vulnerability

by conducting a crazy setup process in the desert. You can read all of the wild details about this trip here. But for a crypto-purist, starting with a dependency on other humans defies the whole point of the field (trust in trustless systems). Zcash developers are planning to overcome this weakness in the future with a more widely distributed creation ceremony in which the the public can participate (and if they trust themselves, then they should trust the system). But until this happens successfully, this is too big of a problem to overcome. And even if the new ceremony does include a large group of people (including possibly you or me), it still feels antithetical to trust potentially unknown unknown human errors when an anonymous cryptocurrency like Monero, which never requires any setup ceremony, exists today.

What's more, there a few other critical weakness with Zcash. First, anonymity is not a default setting. As with Dash, the majority of transactions are completely public. The main reason that anonymity is not a default is because these zero knowledge proofs are relatively large and would drastically increase the size of the blockchain if everyone used them, meaning fewer people could run nodes and thus make the system more centralized. Since <1% of all transaction volume hides all data (sender, recipient, amount), the size of hidden transactions is relatively small. Second, and this is a bit of a personal bias, Zcash is controlled by a U.S. corporation (unlike Monero and Bitcoin, which are decentralized, open-source projects). Not all corporations are bad, but as most have had the displeasure of witnessing in their own working life experiences, companies are driven by profit motive above all else and are also generally subject to government surveillance. I find it hard to trust completely in the anonymity of any system that is even partially controlled by a corporation.

Grin / MimbleWimble

Overview: A promising development phase currency that aims to offer both privacy and scalability

Grin is a novel cryptocurrency based on a new protocol called Mimblewimble. It is still under development and not yet available to the public. At a high level, Grin aims to offer both privacy (although likely less than Monero) and scalability, so that it can be used as a fungible currency for any size transaction. It offers Monero's equivalent of Ring CTs (obscuring the transaction amount) and stealth addresses (providing unlinkability) without an equivalent for ring signatures (which means it doesn't automatically provide untraceability). There are tricks you can use establish untraceability by adding your transaction to others before sending it to the network, but this requires a large user base to prove effective. This means that Grin will likely be one of the most private cryptocurrencies available, but not match Monero's level of privacy. It does, however, offer one major advantage over Monero. It's lack of ring signatures and use of a novel technology called "cutthroughs" (explained below) means that it has a substantially smaller blockchain (on the order of a few GBs instead of 50+ GBs and growing for Monero). This means that Grin could A) offer much cheaper transaction fees and B) become much more decentralized as it's much easier and cheaper for an average user to run a full node.

According to Grin's introductory guide, the currency shares a few other key core ideals with Monero:

- It's open-source, community funded, and free from a pre-mine or ICO
- It's private by default (making it fungible)

- It only uses proven elliptic curve cryptography that has existed for decades (unlike new theoretical technologies like zk-Snarks)
- It's ASIC resistant using a new memory intensive proof of work scheme called Cuckoo Cycle designed to encourage mining decentralization

Mimblewimble aims to achieve these ideals with three key properties: 1) there are no transaction amounts - every transaction uses RingCTs like Monero, 2) there are no addresses, only outputs -- each interaction between two parties is currently conducted directly between wallets via IP address, and 3) "cut-throughs" allow nodes to verify that past transactions balance in such a way that new coins were never created but do not require storing the majority of prior data from the blockchain. Because of cut-throughs, nodes need only store: A) the total amount of coins mined on the chain, B) the complete set of unspent outputs, and C) some very compact data about past transactions known as kernels. This means that you can theoretically have an anonymous blockchain that is highly scalable and never requires more than a few GB of space to run a full node.

Grin sounds extremely promising! It is, other than Monero, the only other privacy focused cryptocurrency project that really excites me. That said, Grin is still in the development phase and will likely not be ready for real world use until 2019. In the medium term, I believe there is a strong chance for Monero and Grin to work together, similar to the way that Bitcoin and Litecoin work today. Monero would be your super redundant "tank" of a blockchain for the most immutable privacy and Grin could be used for the majority of day-to-day transactions. Some Monero messageboards have likened Monero to a savings account and Grin to a checking account. In fact, the Monero community is so interested in Mimblewimble themselves that they are actively considering implementing their own version of Mimblewimble as a Monero sidechain (a separate blockchain that is pegged to the Monero chain, such that you could easily swap coins between chains).

I find the Grin project so interesting that I plan to publish a later deep dive on its technology and implications. Stay tuned!

Part V: How to Buy, Store, and Use Monero

Now that we've discussed why private cryptocurrencies are important and why Monero appears to be the leading private coin, you may be wondering how you can start participating in the Monero community. To start, you should begin by using some Monero yourself.

Buying and storing Monero can be a bit of a challenge. I believe this initial setup difficulty is the biggest reason Monero has yet to become a top 5 coin by market cap. Fortunately, many dedicated people are working to solve these problems as we speak. For now though, we'll walk through how you can get your hands on some Monero in under an hour.

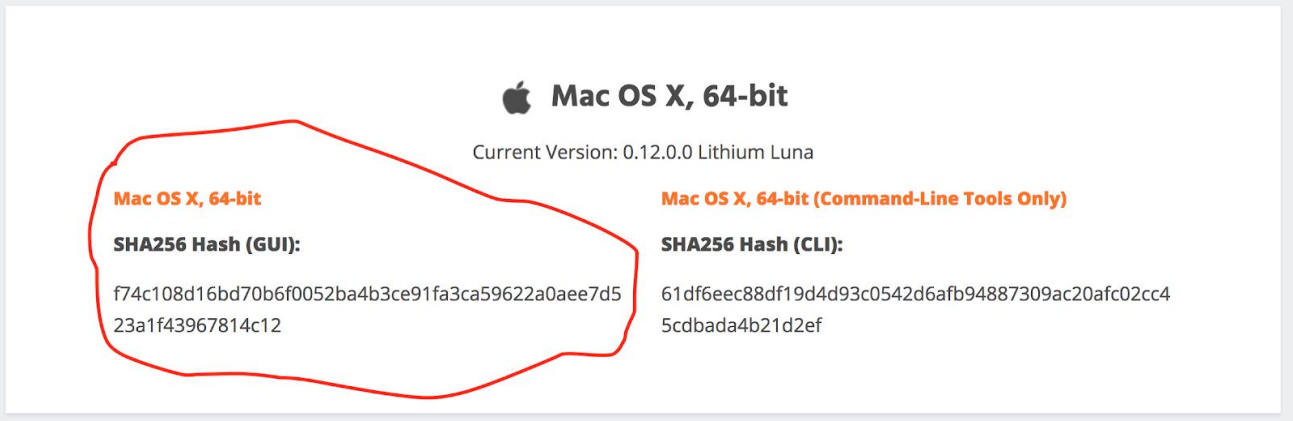
Let's begin with a few options to buy your first Monero:

A) Buy directly with USD or Euros on an exchange called Kraken.[8] Note: approval time to start trading on Kraken can take a while.

B) Buy using a decentralized exchange like Bisq or local Monero meetup site Local Monero, where you need to actually meet a seller in person to exchange fiat currency for Monero. These options are both interesting, but require you to trust independent sellers in a still nascent industry.

C) Buy one of the reserve cryptocurrencies like Bitcoin, Ethereum, or Litecoin and convert it into Monero. I believe this is the fastest and easiest way for most people to get started with Monero. First, you need to buy one the reserve cryptos on a reputable exchange. I recommend Gemini for buying BTC/ETH in the United States and Bitso in Mexico. You can then either move your BTC/ETH/LTC/etc. to a crypto only exchange like Bittrex or Binance or do a quick conversion without an exchange using a site like shapeshift.io[9] where you simply enter the amount of BTC you want to send (with a refund address that's your public address for your BTC wallet) along with your Monero wallet address (note: you don't need to use the payment ID, just the base address). I recommend doing a small transfer first to make sure it works before moving any meaningful amount.

Now, how to store your new Monero. Unfortunately, there aren't a ton of user friendly wallet options available today. I recommend starting with the official Monero GUI (Graphical User Interface) wallet. You can download it here. See below for what Mac users should download.



See this excellent in-depth guide on how to set up and use your Monero GUI wallet.

Note that if you're running a full Monero node (i.e. you downloaded and are hosting a copy of the entire Monero blockchain), it can easily take days to finish your sync. This can be especially stressful if you send funds to your new wallet and then see a balance of 0 while it's syncing. Don't worry! This is normal and is probably the most common concern posted on the Monero

[8] Exchanges like Kraken serve as intermediaries between individual cryptocurrency buyers and sellers.
[9] Shapeshift.io is an instant exchange that allows users to conduct instant transfers without registration (meaning they don't collect any user identifying information).

forums. There are many good reasons to run a full node including supporting the community, increasing your own privacy, and ensuring the accuracy of your copy of the blockchain. If you're just running short on time, then I recommend using the new "bootstrap" feature in the latest GUI release that allows you to point to a remote node (meaning someone else's hosted copy of the blockchain) while you download a complete copy of the blockchain yourself so that you can eventually run a full node. The aforementioned GUI guide will walk you through how to do this.

If you're running short on hard drive space, however, then you can also choose to get your wallet up and running by pointing it to a remote node indefinitely. Here's how to do that. Note that pointing to a remote node will offer you less privacy than running your own node. If having the highest level of privacy possible is important to you, then you should run your own.

One of the biggest knocks on Monero at the moment is the lack of a compatible hardware wallet. This is because, unlike many other popular crypto assets, Monero is not built from the same fundamental building blocks as Bitcoin. It is an entirely unique set of software with a different means of creating public/private key pairs meaning it requires substantial resources for a wallet to integrate support for Monero. That said, Ledger is planning to include Monero in Q1/Q2 of 2018 and the Monero community is self-funding a reasonably priced hardware wallet as well.

Once you've bought your first Monero and stored it in a wallet, there are several ways that you can help support the community. Here are just a few ideas:

- Use Monero to buy legal goods and services to help normalize its use
- Help merchants who do not yet accept Monero to do so by pointing them toward services like GloBee or the open-source code for Monero integrations if they're comfortable with Wordpress, WooCommerce, etc.
- Join or host a Monero meetup in your city
- Join Monero channels on Reddit, StackExchange, IRC / Slack, and join for a worldwide monthly coffee chat (check the Reddit for details about the next session)
- Educate, educate, educate! Word of mouth is the best way for any movement to spread
- For more ideas of how to get involved with the community, check this Reddit post

Part VI: Concluding Thoughts

So far in this paper, we've examined: why privacy is important, what it means to be sound money and why Monero meets that standard, how Monero works, some potential alternatives to Monero, and how to buy, use, and store Monero. I will now conclude with some deeper thoughts about potential dangers that Monero and similar anonymous cryptocurrencies could pose as well as some risks that Monero faces today.

The reality is no one knows what will happen when we introduce completely anonymous digital currencies like Monero into the world. On the one hand, they will facilitate an increase in liberty and the beauty of free human expression and experimentation. They will also facilitate the darker side of human nature with acts of violence that are reprehensible and sad. But the reality is like opening Pandora's Box: once these anonymous, decentralized currencies are out of the bag (and they already are), we cannot stop them. We can only work to create an environment where more people are primed and prepared to use these tools for creating positivity instead of suffering. And when dealing with a complex system like a society or economy, I believe that facilitating such experimentation is the only way to grow and evolve.

I also believe that the most important challenge of our generation is how to increase human cooperation and help our individual minds merge toward a larger hive mind or organism. It is only by working together as one group that we can achieve truly great feats like exploring the stars or feeding everyone on the planet.

The biggest question in my mind is whether we can use a hybrid of both anonymous and publicly auditable means of commerce and organization so that individuals can conduct experiments but also ensure that these experiments don't go far enough to kill ourselves in the process. My best current guess is that we may end up with a worldwide anonymous, decentralized cryptocurrency or cryptocurrencies and lots of new "states" of varying sizes and configurations competing for citizens. Opting into one of these states would require paying for services using a fully transparent coin chosen by that state (perhaps Bitcoin or pegged to Bitcoin). The reality is that I don't have a great answer to this question. I welcome the thoughts of others on how the proliferation of anonymous cryptocurrencies can and will play out. Based on these ideas, perhaps we'll examine this question in more depth in our next paper.

Finally, I want to address a few concerns from readers who have commented that this essay seems overly optimistic about Monero. To be clear, I did not start as a Monero fan by any means. I actually entered the cryptoworld because of my interest in Ethereum's smart contracts, then became fascinated by Bitcoin as a store of value, and finally became interested in private cryptos as a class before settling in on Monero as the most interesting project to date.

That said, things change fast in the world of cryptocurrency. While the Monero community appears to be the most idealistic and technically competent at the moment, that could change over time as developers leave for other projects or the community splits into factions and hard forks the coin so that the resulting new coins have different sets of rules and features (as we've seen recently with Bitcoin and Bitcoin cash). Because the majority of the developers and community members are currently anonymous, there is also no way to know that they are not potentially malicious actors posing as good-willed idealists. For all we know, a rogue state or the NSA could be behind it all.

And even if the community is sincere and remains intact, there are still some major challenges facing Monero today, including:

- How can Monero remain decentralized and usable as a currency if the size of the blockchain keeps growing to TBs?
- How can Monero gain mainstream adoption if it retains a stigma as a Dark web currency used just for drugs and illegal activities?
- What happens to Monero if another project like Bitcoin, Ethereum, Grin, Zcash, etc. is able to add sufficient mandatory privacy while also solving problems of scalability and adoption?
- What happens when future technologies (e.g. quantum computing) break the privacy measures that Monero employs today?

I believe that there are currently reasonable answers to each of these questions:

- Monero is already reducing blockchain size by 80% with a new technology called bulletproofs and has plans to scale to currency level usage with 2nd layer networks like the Lightning Network or a MimbleWimble sidechain.
- Monero community members are already working with mainstream merchants to use Monero for perfectly legal activities (see Project Coral Reef and Globee for examples). Note that Bitcoin also started with such a Dark web stigma before mainstream adopters started using it.
- No other project has trustless privacy built into the currency at the base layer yet. If that changes over time, so be it. A new currency will take Monero's place.
- All cryptocurrencies face risk from future technological breakthroughs. As long as the Monero community remains committed to ideology over technology, then they too can adapt their technology and hard fork the coin to create a new version of Monero when necessary.

But all of this is just speculation for now. If a weakness is found in Monero or another private cryptocurrency offers better functionality or more widespread adoption, then I will gladly update my thinking on Monero at that time. It is also critical to remember that no privacy technology is 100% perfect. New technologies and attack vectors are constantly created or discovered. It's helpful to think of the movement for privacy as a sort of dance - everything is constantly moving, changing, evolving. Therefore, I reiterate that my primary interest in Monero stems not from any specific technology or feature, but rather from what appears to be a community ready to adapt and grow.

Thank you for the time you've invested in reading this document. Please feel free to share with others who may find it useful. All feedback is appreciated:
cypherperro [at] protonmail.com