CRYPTOCURRENCY

The Future Of Money & Blockchain Technology
CRYPTOCURRENCY

The Future Of Money & Blockchain Technology

FILIP KARINJA
Table of Contents

Introduction..................................................................................................................................................
Chapter One: What Is Cryptocurrency? ........................................................................................................
Chapter Two: Benefits Of Cryptocurrency...................................................................................................
Chapter Three: Types Of Cryptocurrency .....................................................................................................
Chapter Four: What Is Blockchain Technology ............................................................................................
Chapter Five: How To Obtain Cryptocurrency Coins ....................................................................................
Chapter Six: Where Is Cryptocurrency Headed ............................................................................................
© Copyright 2017 by Filip Karinja - All rights reserved.

It is not legal to reproduce, duplicate, or transmit any part of this document in either electronic means or in printed format. Recording of this publication is strictly prohibited.
Introduction

With the age of computers and the Internet revolution has come many tremendous changes to how daily transactions and activities are processed across the world. Messages are now sent almost instantaneously through email, text messaging, Web-based messaging, and chat applications. Individuals and families can stay in touch with each other through video chat right from their mobile devices or computers. Multinational companies are able to hold meetings with their staff and colleagues on the other side of the world through virtual office setups and video conferencing programs that only a couple of decades ago would have been clunky or unreliable to use.

As the digital age has taken over, another aspect of daily life that has seen major changes is financial transactions. Consumers are now able to manage their wealth right from their home computers or mobile phones through online banking, with access to their checking or savings accounts, credit lines, and bill payment systems. Information is readily available to entrepreneurs, bank managers, tellers, insurance brokers, and other financial services professionals, speeding up the process of providing basic information and services to their clients.

The decentralization of information and access in the financial sector has also led to innovations in currency itself, leading to the rise of cryptocurrency. Cryptocurrency first came into mainstream consciousness in 2009 with the rise of Bitcoin, although there were already several attempts before this venture to decentralize currency and use digital database servers to facilitate transactions globally. Bitcoin, however, was the first big success of the cryptocurrency story and continues to be the leading provider, and its popularity also brought forth much discussion about cryptocurrency and how it can change the future of finances and global money transactions as it makes inroads into the scene.

The main attraction of cryptocurrency, which is freedom from the control, oversight, or dependence on established financial institutions such as central banks and governing authorities, catapulted cryptocurrency (Bitcoin, in particular) to popular demand and spawned other similar ventures wanting a slice of the pie. As attitudes in many areas of the world have been leaning towards more personal control and less oversight from the “big banks” and government control, cryptocurrency is forecast to continue its upward trajectory as an alternative form of peer-to-peer financial option for various transactions.

If you have considered cryptocurrency or have heard about it and considering trying it out to see if it fits your needs, this book will give you the basic information you need to know regarding cryptocurrency and what it offers.
Chapter One: What Is Cryptocurrency?

Simply put, cryptocurrency is digital or virtual currency making use of the security features of cryptography. Currency is generally easy to understand, but perhaps you are not as familiar with cryptography, which is the utilization of various security protocols for securing information and preventing the access or interference of outside parties or the general public. Cryptography is commonly used in many machines, programs, or devices we use daily, such as automated teller machines, e-commerce websites, online banking sites, and computer passwords.

In cryptocurrency, digital currency is secured using the encryption techniques of cryptography, and transactions are performed between users or “peers” with the additional confirmation feature known as mining. All transactions are added and stored in a record-keeping feature known as a public ledger.

The website CryptocurrencyFacts.com explains the term public ledger as such: "All confirmed transactions from the start of a cryptocurrency’s creation are stored in a public ledger. The identities of the coin owners are encrypted, and the system uses other cryptographic techniques to ensure the legitimacy of record keeping. The ledger ensures that corresponding “digital wallets” can calculate an accurate spendable balance. Also, new transactions can be checked to ensure that each transaction uses only coins currently owned by the spender. Bitcoin calls this public ledger a 'transaction blockchain'."

Regarding transactions in the cryptocurrency sense, the site explains, "A transfer of funds between two digital wallets is called a transaction. That transaction gets submitted to a public ledger and awaits confirmation. When a transaction is made, wallets use an encrypted electronic signature (an encrypted piece of data called a cryptographic signature) to provide a mathematical proof that the transaction is coming from the owner of the wallet. The confirmation process takes a bit of time (ten minutes for bitcoin) while “miners” mine (ie. confirm transactions and add them to the public ledger)."

Mining is another term you will come across a lot in learning cryptocurrency, as explained by CryptocurrencyFacts.com: "In simple terms, mining is the process of confirming transactions and adding them to a public ledger. In order to add a transaction to the ledger, the “miner” must solve an increasingly-complex computational problem (sort of like a mathematical puzzle). Mining is open source, so anyone can confirm the transaction. The first “miner” to solve the puzzle adds a “block” of transactions to the ledger. The way in which transactions, blocks, and the public blockchain ledger work together ensures that no one individual can easily add or change a block at will. Once a block is added to the ledger, all correlating transactions are permanent and a small transaction fee is added to the miner’s wallet (along with newly created coins). The mining process is what gives value to the coins and is known as a proof-of-work system."

Sounds a bit overwhelming? Mariella Moon, writing for Engadget.com, wrote this brief explainer in a 2015 article: "Imagine that you're an actual miner with a pickaxe in your hand, and there's a big boulder in front of you with golden coins hidden in its very center. To get to the gold coins, you'll have to chip away at the boulder: The better your equipment is, the faster you can go. Unfortunately, you're not the only one trying to get to the center of the boulder, and it's a race
between you and other miners with better, more high-tech pickaxes. That's why the best way is to pal up with other people to get to the very center of the boulder and divide the loot. As time goes by, though, you'll notice that boulders become harder to break and the gold coins in the center become fewer in number."

Moon added, "That's but an oversimplification of the process, of course, but it should give you an idea of how it works. The boulder in this case represents a block or a big bunch of transactions miners have to verify and solve. Each piece of rock a miner chips away represents a verified transaction, and the gold coins represent the bitcoins a miner can earn and introduce into the circulation."

Another writer for Engadget.com, Daniel Cooper, wrote a more in-depth piece on Bitcoin and cryptocurrency, particularly comparing it to popular electronic payment systems such as PayPal. "Bitcoin's basic idea is to create digital cash that can be spent as anonymously as the cash in your wallet, rather than as traceable as money in an electronic bank account. There's a tired metaphor that Bitcoin is "digital gold," letting you wander around shelling out gold coins for goods or watching them amass into a fortune -- at least in theory. Compare that to a service like PayPal, which can (and will) intervene in transactions at its whim, and you can see why people would desire more fiscal autonomy," Cooper explained.

He added, "Of course, PayPal and major banks expend huge amounts of time and resources to ensure that your money is safe, but with Bitcoin, the security of the system is trusted to your fellow users. Each transaction is publicly verified by the community of Bitcoin users, so as long as there are more honest users than dishonest ones (who would try and steal the cash for themselves) then your money is theoretically safe."

Cooper also makes use of the gold mining comparison to make it easier to understand how cryptocurrency works, and its safety features. "Let's labor that gold metaphor a little further, shall we? The coins are created in a process that's called "mining," but it's really a computer validating data called the blockchain. What's a blockchain? Well, imagine the data for every bank transaction in the world was printed out in one long line. Mining is the process whereby a computer goes through and checks every single Bitcoin transaction ever made, making sure that the books are balanced at the end. The machine (or "node") that successfully validates the blockchain (of the hundreds, if not thousands of machines that are competing) is then awarded a small fee of Bitcoins as a prize."

As far as security patterns, Cooper ventures, "Bitcoin is artificially self-limiting, and to ensure that there is a steady and constant flow of money coming into the economy, validating the blockchain is constantly made harder, keeping the successes to a regular pattern. In order to prevent people from circumventing these algorithms and inventing more money, the whole blockchain needs to be agreed upon by a majority -- so as long as the honest nodes control more CPU power than the dishonest ones, the system is safe. In practice, this means that as long as no more than 49 percent of Bitcoin users are trying to defraud the system, it'll work."

Perhaps you have used your financial institution’s online banking system to pay for purchases or send or receive money. Maybe you also have a PayPal account which you use for ordering online or sending money to your family or friends. The main difference between these services and that of
cryptocurrency is the decentralized nature of Bitcoin and other similar providers. When you are using your online banking account, you are accessing cash that still exists in physical form somewhere in the banking system, and as such can be subject to scrutiny, oversight, and processing fees that are set by governing authorities and banking institutions. Similarly, PayPal is also an electronic payment system linked to your actual bank account.

But with the use of cryptocurrency, you can bypass traditional banking procedures and institutional regulations completely, relying instead on the open-source and peer-to-peer network of cryptocurrency to process your financial transaction. In fact, while all transactions go through the public ledger and are stored there, there is no central authority or database that will keep track of how much wealth you currently have in your Bitcoin account. On the other hand, this also means that you are responsible for keeping your digital cash safe and secure from potential hackers and online thieves.

Before Bitcoin, there were already other similar attempts to popularize decentralized electronic currency systems, such as b-money and Bit Gold. In fact, going back to 1992, an independent digital currency was already being planned by a physicist named Timothy May, as written about by Morgen Peck in his article Bitcoin: The Cryptoanarchists’ Answer to Cash, which appeared on the IEEE.org Spectrum in 2012. "The pursuit of an independent digital currency really got started in 1992, when Timothy May, a retired Intel physicist, invited a group of friends over to his house outside Santa Cruz, Calif., to discuss privacy and the nascent Internet. In the prior decade, cryptographic tools, like Whitfield Diffie’s public-key encryption and Phil Zimmermann’s Pretty Good Privacy, had proven useful for controlling who could access digital messages. Fearing a sudden shift in power and information control, governments around the world had begun threatening to restrict access to such cryptographic protocols."

Peck wrote further, "May and his guests looked forward to everything those governments feared. ‘Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions,’ he said. By the end of the meeting, the group had given themselves a name—‘cypherpunks’—and the superhero-like task of defending privacy across the digital world. In just a week, co-founder Eric Hughes wrote a program that could receive encrypted e-mails, scrub away all identifying marks, and send them back out to a list of subscribers."

b-money, a predecessor of Bitcoin, was created in 1998 by Wei Dai, who had just graduated from the University of Washington at the time. The computer science degree-holder said, “My motivation for b-money was to enable online economies that are purely voluntary, ones that couldn’t be taxed or regulated through the threat of force.” b-money was a personal project of Wei and more of a concept, but it did lay important groundwork for the movement.

Another computer scientist, Nick Szabo, was the brain behind Bit Gold, widely considered to be another main predecessor of BitCoin. "I started thinking about the analogy between difficult-to-solve problems and the difficulty of mining gold," Szabo said. "Anything that works well as a proof-of-work function, producing a specific binary string such that it can be proved that generating that string was computationally costly, will work … I was trying to mimic as closely as possible in
cyberspace the security and trust characteristics of gold, and chief among those is that it doesn’t depend on a trusted central authority."

Then, BitCoin appeared, quietly at first. Peck wrote, “After b-money and bit gold failed to garner widespread support, the e-money scene got pretty quiet. And then, in 2008, along came a mysterious figure who wrote under the name “Satoshi Nakamoto,” with a proposal for something called Bitcoin. As is fitting for the creator of a private digital currency, Nakamoto’s true identity remains a secret. “I’ve never heard of anybody who knew about that name earlier,” says Szabo.”

The financial anonymity proved to be a hit among many Bitcoin users. "The system turns traditional banking privacy on its head: All transactions are made in public, but they’re difficult to link up with a human identity," Peck wrote. "Maintaining the dissociation takes vigilance on the part of the Bitcoin user and careful decisions about which outside applications and exchange methods to use, but it can be done. “Anonymity is typically compromised by means outside of Bitcoin’s control, in other words,” says Jeff Garzik, who is on the team of programmers now responsible for developing the Bitcoin software. Bitcoin is often described as providing pseudoanonymity, by creating enough obfuscation to provide users with plausible deniability."

Now that you have a basic understanding of cryptocurrency, let us take a closer look at the much-touted benefits of this platform and how these advantages could potentially work for your needs.
Chapter Two: Benefits Of Cryptocurrency

Those who are considering using cryptocurrency options such as Bitcoin would do well to learn everything they can first about this and what advantages it offers. Below are some of the popular benefits of cryptocurrency that have made it quite the attractive option for so many users:

**Minimal or no processing fees.** You are already aware of the many processing fees that traditional banks charge users for their services. There are fees for opening or maintaining accounts, transaction fees (often both for sender and receiver), returned check fees, and many other miscellaneous charges. With cryptocurrency transactions, there are generally no processing fees to worry about, but for third party services that do charge fees, costs are still very minimal compared to what you would expect to shell out for similar transactions done through banks or electronic payment systems such as PayPal.

**Greater security versus identity theft.** Identity theft is a major problem in the world today. The 2017 Identity Theft Study commissioned by Javelin Strategy and Research reports that in 2016, identity thieves stole more than US$16 billion from 15.4 million consumers in the United States alone, up from $15.3 billion stolen in 2015 from about 13.1 million consumers. If you use your credit or debit card for purchases, particularly online, the risk of identity theft increases especially because credit cards work via a “pull” basis, deducting the amount from your credit line. With cryptocurrency, the opposite or “push” basis is used, where the user will send the exact amount without the need to provide any additional or unnecessary information.

**Fraud protection.** This is particularly useful for merchants who accept digital transactions, such as e-commerce websites. With credit or debit cards, senders can counterfeit or suddenly reverse a transaction, causing credit card charge-backs. With cryptocurrency transactions, all financial actions made are non-reversible, and there is an increased security system in place to prevent fraudulent activity.

**Fast transaction settlements.** For big purchases such as real estate and other property purchases, there are typically many third party processes involved, and additional payments. Notary filings, lawyer deliberations, permits, applications, and other documents have to be submitted and reviewed, typically causing delays and longer hold times. With the use of cryptocurrency, these processes are no longer required, with the transaction only having to go through the mining process which generally takes much shorter (in many cases, only a few minutes for verification in the public ledger). Bitcoin contracts are an efficient means to securely transact big purchases between users who no longer require the oversight of additional third parties and would like the settlement achieved in the soonest possible timeframe.

**Decentralized network.** As already mentioned in the previous chapter, Bitcoin and other cryptocurrencies do not rely on central banks and other traditional financial institutions for oversight. Rather, this is a peer-to-peer network that frees up control and transfers much of the control and responsibilities to users. The blockchain technology utilized by cryptocurrency providers for verifying transactions is not controlled by just one governing authority, rather it relies on a global computer network with mass collaboration happening in real time.
**Greater access.** A large number of the global population do not have access to traditional financial services provided by banks and other institutions. This could be attributed to a number of reasons, including geographic restrictions, infrastructure deficiencies, or the restrictive costs usually associated with banking services especially in developing markets. Cryptocurrency opens up the global currency to these billions of individuals (estimates range from anywhere between 1.5 billion to 2 billion worldwide) by allowing them to access peer-to-peer financial transactions without the need for an established bank account or line of credit.

**Ease of transaction and worldwide acceptance.** Cryptocurrency is not hindered by exchange rates, state restrictions, interest rates, and other limitations set by central banks and governing authorities, making it more universally acceptable and providing for faster, easier transactions especially for users who need to transact with other users in different worldwide locations.

Do you like the idea of financial independence and not having to worry about someone else, i.e. a governing authority being able to scrutinize your transactions or even restrict your financial activities? If so, then cryptocurrency may be a viable option for you to consider. In the next chapter, we will take a look at various types of cryptocurrency currently available, as well as some options on how you can obtain cryptocurrency and start using it in your daily transactions.
Chapter Three: Types Of Cryptocurrency

A quick search on the Internet will give you a list of a number of different cryptocurrencies that are available to users. As of last 2016 there are about 740 different cryptocurrencies available, but you really do not need to worry about knowing and understanding all of these types. There are several dozen cryptocurrencies that have reached a level of market capitalization (at least $10 million) to be considered major players, but in the next few pages we will look at only a few of the most widely-used of these digital currencies.

Over time, as your needs change, you may find it essential to know more about the other types, but to start off you just need to focus on the market leaders.

Bitcoin: No discussion of cryptocurrency would be complete without delving into the biggest of them all, which is Bitcoin. This cryptocurrency and online payment network started in 2009 as an open-source software, the brainchild of Satoshi Nakamoto who may be one programmer or a group of programmers. Bitcoin uses a peer-to-peer system with transactions verified in a public ledger known as the blockchain.

The very first bitcoin transaction was performed by programmer Hal Finney, who received 10 bitcoins from Nakamoto. In his description of the transaction, Finney said, "When Satoshi announced the first release of the software, I grabbed it right away. I think I was the first person besides Satoshi to run bitcoin. I mined block 70-something, and I was the recipient of the first bitcoin transaction, when Satoshi sent ten coins to me as a test. I carried on an email conversation with Satoshi over the next few days, mostly me reporting bugs and him fixing them."

He continued, "Today, Satoshi's true identity has become a mystery. But at the time, I thought I was dealing with a young man of Japanese ancestry who was very smart and sincere. I've had the good fortune to know many brilliant people over the course of my life, so I recognize the signs. After a few days, bitcoin was running pretty stably, so I left it running. Those were the days when difficulty was 1, and you could find blocks with a CPU, not even a GPU. I mined several blocks over the next days. But I turned it off because it made my computer run hot, and the fan noise bothered me. In retrospect, I wish I had kept it up longer, but on the other hand I was extraordinarily lucky to be there at the beginning. It's one of those glass half full half empty things."

Finney was tragically diagnosed with ALS in 2009, but was still able to follow Bitcoin's emergence in the mainstream discussion. "The next I heard of Bitcoin was late 2010, when I was surprised to find that it was not only still going, bitcoins actually had monetary value. I dusted off my old wallet, and was relieved to discover that my bitcoins were still there. As the price climbed up to real money, I transferred the coins into an offline wallet, where hopefully they'll be worth something to my heirs."

Ethereum: Ethereum is actually an open-source computing platform with a cryptocurrency token called the ether. It was launched in 2015 as a decentralized platform where users can build, transact and perform distributed applications and Smart Contracts. With a market capitalization of $4.46 billion, Ethereum is second to Bitcoin in the cryptocurrency industry. But what makes Ethereum different from Bitcoin primarily?
In his article for Forbes.com, contributor Roger Aitken notes that Ethereum is designed primarily as a smart contracts platform rather than a marketplace. "It's possible to build an exchange on it. However, it wasn’t designed with that in mind. Take the issue of block times - essentially how fast transactions are processed. Bitcoin, which some might say is the ‘granddaddy’ of cryptocurrency, has 10-minute blocks. And, it’s also argued that transactions are not generally considered truly secure until they have had three confirmations."

Aitken continues, "Newer systems are much faster - or at least have lower latency. Ethereum, for example, currently has block times of around 14 seconds. But even that’s nowhere near the super or ultra-low-latency systems required by professional traders and institutions that pack a punch to beat the competition. Whilst the blockchain isn’t ever going to be suitable for the sub-microsecond rates required by high-frequency trading (HFT) algorithms, seconds do count in some quarters. And, if you can go faster well why not."

Litecoin: Litecoin was released on October 7, 2011 on GitHub using an open source client. It was started by a former Google employee named Charlie Lee and based on an open source global payment system using scrypt as its proof of work. Litecoin has a faster transaction confirmation or turnaround time than Bitcoin because of its faster block generation rate.

How does Litecoin achieve this faster transaction rate? In his explainer for arstechnica.com, Ian Steadman notes that the people behind Litecoin saw a possible “forking into two” of the Bitcoin blockchain as it became popular. "Roughly every 10 minutes, a new blockchain is generated and disseminated throughout the Bitcoin network by each node, and the version that becomes the accepted, canonical version is the one that is disseminated by the greatest number of nodes. It is, in a way, democratic. However, something very worrying happened on March 11, 2011 when the blockchain forked into two. For roughly six hours, there were effectively two versions of Bitcoin in operation. This shouldn't happen. It was only resolved when one chain eventually "pulled ahead" of the other, becoming established as the legitimate blockchain again."

Steadman continues, "Litecoin was founded in October 2011 in recognition that this kind of problem was probably going to happen if Bitcoin became popular. Merchants require large numbers of small value transactions happening quickly, something that Bitcoin isn't really well-suited for. Larger transactions, happening more slowly (remember, new blockchains generate every 10 minutes) are more suited to it. That's why Litecoin has a faster transaction time (roughly two and a half minutes) than Bitcoin. With four times as many coins in circulation, it theoretically offers smaller divisions of coins to make smaller transaction values more feasible."

Zcash: Zcash is relatively newer, having only burst into the scene in 2016 as another open source and decentralized cryptocurrency. Zcash prides itself in providing more privacy and security particularly for transactions and user details such as sender name, recipient name, and the amount transacted. The founder of Zcash, Zooko Wilcox, said to Investopedia, "Zcash is a new blockchain and cryptocurrency which allows private transactions (and generally private data) in a public blockchain. This allows businesses, consumers, and new apps to control who gets to see the details of their transactions, even while using a global, permission-less blockchain."

Investopedia also explains the “shielded transactions” feature of Zcash: "Zcash offers its users the choice of ‘shielded’ transactions, which allow for content to be encrypted using advanced
cryptographic technique or zero-knowledge proof construction called a zk-SNARK developed by its team. These constructions ensure validity of transactions as well as secure ledger of balances without giving out any other information (such as parties or amount involved). Thus Zcash offers an added feature over bitcoin, while ensuring that nobody is cheating or stealing."

**Ripple:** If you are considering cryptocurrency for overseas transactions, whether personal or business-related, Ripple may be of interest to you. This is an open source payment system protocol that specializes in real-time, low-cost and secure international payment settlements. Since its release in 2012, it has reached a market capitalization of $1.26 billion, and is currently the third largest behind Bitcoin and Ethereum.

According to Nathaniel Popper of *Dealbook*, Ripple could just be the cryptocurrency with the most chance of beating Bitcoin. "Founded in San Francisco by former bitcoin developers, Ripple holds out the promise not just of a new currency, but also of a novel method to send money around the world. With that potential, it is winning something that has proved elusive for virtual currencies: involvement from more mainstream players in the financial system," he wrote.

How is Ripple different from Bitcoin and the others? Popper explains, "Ripple is being heralded in some quarters as a more significant innovation than its competitors. Ripple maintains not only a currency, but also a system on which any currency, even bitcoin, can be moved around or traded — akin to a cross between Western Union and a currency exchange, without the hefty fees. A person using the system can deposit any sort of money into a personal Ripple wallet through a business that is signed up as a Ripple gateway. That money can then be moved to the wallet of another Ripple user, without going through a bank or a credit card system."

Popper writes on, "People moving the same type of currency, say dollars or pounds, to another account on the Ripple system will not have to use its currency, known as ripple or xrp, pronounced letter by letter. But ripple is meant to provide the fastest and cheapest conversions, of one nation’s currency to another or among various types of digital money. The hope is that once people begin using ripple they will keep some of their money in the currency and eventually use it directly to make purchases."

Ripple uses distributed ledgers, a feature that is popular particularly with banks and other traditional financial institutions. Houman Shadab, professor at New York Law School, says this is a particular advantage for Ripple. "Distributed ledgers, at least for now, are more attractive because of the control they afford over the system. They're not subject to the vagaries of price volatility of the underlying currencies. And also they have a more secure, distributed authentication process that doesn't rely on the incentives of miners who authenticate transactions based on the value of the currency."

**Peercoin:** This cryptocurrency uses proof-of-stake and proof-of-work systems, and is also marketed as a more environmentally-sustainable option and using less energy than its counterparts. How? A *Heavy.com* post explains, "Right now, Peercoins use “proof of work” but it will be phased out as mining difficulty increases and rewards decrease. Then, most new Peercoin will be generated as interest, 1% per year, on existing Peercoin using the less resource-demanding “proof of stake” mining.”
Another difference of Peercoin compared to Bitcoin is the transaction fee charged (the average is about $0.06). According to Peercoin creator Sunny King, "From my point of view, I think the cryptocurrency movement needs at least one ‘backbone’ currency, or more, that maintains high degree of decentralization, maintains high level of security, but not necessarily providing high volume of transactions. Thinking of savings accounts and gold coins, you don’t transact them at high velocity but they form the backbone of the monetary systems."

**Monero:** Launched in 2014, this cryptocurrency is characterized by its security features, untraceability, and privacy for users. Monero is funded by donors and community-generated resources. While also relatively new to the scene, Monero has grown exponentially in both market capitalization and transaction volume, with a market cap of well over $600 million.

Transactions on the Monero network are kept private with the use of ring signatures to conceal sending addresses, mandatory RingCT protection for transaction amounts, and stealth addresses concealing the receiving addresses. As Investopedia explains, "Monero has been launched with a strong focus on decentralization and scalability, and enables complete privacy by using a special technique called ‘ring signatures.’ With this technique, there appears a group of cryptographic signatures including at least one real participant – but since they all appear valid, the real one cannot be isolated."

**Dash:** Dash was originally called DarkCoin, and this cryptocurrency network also specializes in anonymity using a decentralized mastercode network keeping transactions close to untraceable. It was launched in January 2014 by creator and developer Evan Duffield, and rebranded to Dash the following year. This open source, peer-to-peer cryptocurrency makes use of a decentralized system for governance and budgeting, and is the sixth largest cryptocurrency in terms of market capitalization.

As the first decentralized and autonomous organization, Dash seeks to solve some innate problems with human error in the Bitcoin network. Juan S. Galt writes in cointelegraph.com, "Dash is comprised of three types of 'nodes' - three different ways in which the DASH software clients can be used, with specific roles and responsibilities on the network. The first are miners, who provide proof-of-work security to the cryptocurrency in a similar fashion to Bitcoin, though instead using X11, an algorithm designed and believed to be ASIC resistant. Miners provide computing power in exchange for a regular payment from the network to the tune of 45% of the block rewards."

"The second are full node wallets, which host the accounting ledger (blockchain) allowing users to access the network, use the currency and further decentralize it. And the third and most innovative element of DASH are its “Masternodes.” These are regular full nodes that anyone can run, but with the difference that they host a 1,000 DASH collateral, equivalent to roughly US$2,500 at current rates (works with cold storage). The collateral earns hosts the right to provide services to DASH users at a profit – 45% of block rewards. Services such as DarkSend — the feature that brought DASH to fame — as well as Instant Transactions, the controversial 4 second transaction locking feature," he continues.

Dash's Decentralized Governance by Blockchain or DGB is constructed on top of this Masternodes network, allowing changes or upgrades to the currency from the community itself.
**Namecoin:** Namecoin is based on the bitcoin code and also utilizes the same algorithm of proof-of-work. It is known primarily as a decentralized domain name system for dot-bit domains. Other potential uses for Namecoin that have been proposed include messaging and identity systems, personal namespace, shares and stocks, alias systems, etc.

You will likely be utilizing Namecoin if you will be purchasing a dot-bit domain, with your transaction being logged in the public ledger or blockchain. The top level .bit domain is free from censorship unlike other domains such as .com or .net. Also, .bit is independent of the Internet Corporation for Assigned Names and Numbers or ICANN.

Much discussion has revolved around whether Namecoin can render ICANN obsolete soon enough as .bit domains have now become more accessible. Eli Dourado, the head of global policy and communications for Boom, wrote in theumlaut.com, "Namecoin is a fascinating substitute for the domain name system because, like Bitcoin, it is completely decentralized and censorship-resistant. Proposed censorship measures like SOPA and PIPA simply could not apply to Namecoin because it is virtually impossible to reverse or interfere with name registrations, which are enforced with strong cryptography. New top-level-domains are added by the consensus of the miners, just as Bitcoin miners must agree on the rate of growth of Bitcoin’s money supply."

It is expanding also to other uses, as Dourado explains, "Namecoin has uses beyond DNS. Namecoin is at base a decentralized key-value store. We can use it to store information about ourselves in an easily accessible form. Using the non-domain namespaces of Namecoin, we could store information that it would otherwise be hard to securely or conveniently exchange. For example, public key encryption relies on one being able to verify that one’s correspondent’s public key is actually theirs. If we’ve never communicated before, signing something with my private key only proves that I’m me if you have some good reason to believe that the corresponding public key is mine."

**Omni:** Omni used to be called Mastercoin, and it was designed mainly to enable more complicated financial functions in cryptocurrency. The protocol for Omni is also built on the bitcoin blockchain, and the Mastercoin project was officially launched in July of 2013. So how does Omni differentiate itself from Bitcoin?

In his article for BitcoinMagazine.com, Vitalik Buterin notes that Mastercoin/Omni attempts to build on top of existing infrastructure. "The key difference in Mastercoin is this: rather than trying to bootstrap an entirely new blockchain, as every other cryptocurrency does, Mastercoin seeks to create an entirely new network of currencies, commodities and securities on top of Bitcoin itself ... Rather than simply using the Bitcoin blockchain as a secure timestamping system to store its own blocks, Mastercoin uses the Bitcoin blockchain to store every transaction."

He adds, "Philosophically, the best way to think of Mastercoin is as an alternative way of making sense of Bitcoin transactions; just like the Bitcoin protocol takes a series of transactions and parses them to determine how many bitcoins are in every address at any particular moment, the Mastercoin protocol also takes the available Bitcoin transactions and parses them to extract data relevant to the Mastercoin network."
The developer of Mastercoin/Omni, J.R. Willett, explained in his paper *The Second Bitcoin Whitepaper* why he designed this to be a protocol layer on top of Bitcoin rather than creating a new cryptocurrency from scratch: "Alternate blockchains compete with bitcoins financially, confuse our message to the world, and dilute our efforts. These barriers interfere with the adoption momentum of bitcoin and the adoption momentum of alternate currencies as well, regardless of how well-conceived their rules may be. New protocol layers on top of the bitcoin protocol will increase bitcoin values, consolidate our message to the world, and concentrate our efforts, while still allowing individuals and groups to issue new currencies with experimental new rules. The success of any experimental currency protocol layer will enhance the value and success of the foundational bitcoin protocol."

But according to Buterin, perhaps the most promising feature of Mastercoin/Omni is its concept of self-stabilization: "With Mastercoin as it is, it is certainly possible to use bets to hedge one’s position so as to have one’s net worth in the Mastercoin network effectively track the value of a traditional stable currency or asset, such as the USD, commodities or silver ... A self-stabilizing currency works as follows. First, the currency’s creator (who has no further involvement once the currency is up and running) picks a currency or commodity that the currency would follow, and finds a price feed for that currency. They then take this information, along with some other metadata such as an “agression factor” to indicate how closely the currency should track the underlying index, and publish it as a Mastercoin transaction. From that point on, the Mastercoin protocol itself simulates a sort of central bank for this currency, creating units out of thin air and selling them to anyone who is willing to pay slightly above the market price."

**Nxt:** Just like Ripple, Nxt veers away from the Bitcoin code completely and uses its own Java software code. This open-source payment network and cryptocurrency was launched by software developer BCNext in November of 2013. With its own integrated Asset Exchange, marketplace, and messaging features, Nxt was designed to be a flexible platform with financial service providers and application developers in mind.

In a report for *CoinTelegraph.com* on the launch of Nxt, Amanda B. Johnson remarked, "Joining the ranks of Ethereum and MaidSafe as hopefuls to decentralize the software part of the Internet, Nxt has at least one leg-up over either of those protocols: it’s already been launched ... Using the brand NxInside, the team hopes that software developers will choose to build future product and service offerings on top of the Nxt protocol."

**Dogecoin:** What started out as a “joke currency” in 2013 has reached a capitalization, as of May 2017, of $130 million. The Dogecoin cryptocurrency was a project of Portland, Oregon-based programmer Billy Markus. Initially, Markus had set out to create Dogecoin as a more fun alternative to Bitcoin, hoping it would attract a broader demographic who at the time was wary of Bitcoin’s associations with online drug proliferation. Markus reached out to Adobe marketer Jackson Palmer, who had created the joke website, when he came across Dogecoin online.

"I was tinkering with a coin that I had already made called ‘Bells,’ based off of Nintendo’s Animal Crossing, that wasn’t particularly successful," Markus said. "I was mucking with it and I figured out how to change all the fonts to Comic Sans MS, then thought, ‘oh ok, this could be funny.’ So I had a mockup of the client with the Dogecoin picture Palmer made, and I just wanted
“to show that I wasn’t a n00b and I could actually make coins... This wasn’t some weird master plan that we had.”

Palmer added, “A lot of cryptocurrency—namely Bitcoin, with its history with Silk Road—has been sitting in the shadows. It’s associated with the dark web. So I think by combining a coin with a meme, which is something that people see spammed to hell on their Twitter and Facebook feeds every day, I think it adds a face, the Doge face, and makes it more accessible. It’s something people can get behind. It’s no longer this shady thing that geeks in basements use. It’s important to note that this wasn’t some master plan, it was just the two of us throwing a few emails back and forth before we pushed it out there."

The fun, meme-based approach of Dogecoin and its mass appeal proved to be ingredients to its quick rise. “In hindsight, it was obvious that cryptocurrency was ready for something that was more accessible, and a meme is obviously really accessible,” Markus related. "Everyone recognizes the doge meme. It’s based on a dog, and everyone loves dogs. It was a perfect storm.”

Palmer agrees, emphasizing that the appeal of Dogecoin contributed a lot to its rapid adoption even by those who are beginners in the world of cryptocurrency. “Cryptocurrency has a lot of growing to do, and it also has a lot of stabilizing to do. If all we’ve done with Dogecoin at the end of the day is grow awareness in a decentralized currency such as Bitcoin, then I think we’ve done a good job, because for a lot of the people who are using Doge now, it’s their first cryptocurrency that they’ve ever used, and they’ve started mining. They’re learning, and I think it’s great that people actually want to learn about it because it’s associated with this doge meme.”
Chapter Four: What Is Blockchain Technology?

Blockchain is a term that you have already noticed quite often not only in this book, but undoubtedly in discussions about Bitcoin and cryptocurrencies in general. Blockchain technology is used in Bitcoin as a public ledger or storage space for transactions that have been conducted in the network. Because transactions are being done every day, this public ledger continues to grow as the recordings increase, and these records are added as blocks of information in an organized, linear pattern.

You can think of blockchain technology as the official record that a certain transaction was processed on the Bitcoin network. Once a block of information has been added to the database, it is there permanently. Instead of a random order of adding the blocks of information (which would undoubtedly cause confusion), blockchain technology adds the data chronologically and with a hash or portion of the previous block included for continuity.

Investopedia uses a banking analogy to further explain the basic setup of blockchain technology: “To use conventional banking as an analogy, the blockchain is like a full history of banking transactions. Bitcoin transactions are entered chronologically in a blockchain just the way bank transactions are. Blocks, meanwhile, are like individual bank statements. Based on the Bitcoin protocol, the blockchain database is shared by all nodes participating in a system. The full copy of the blockchain has records of every Bitcoin transaction ever executed. It can thus provide insight about facts like how much value belonged a particular address at any point in the past.”

William Mougaya, a venture specialist, entrepreneur, strategist, and marketer, compares blockchain technology to popular Google Docs collaboration features. "The traditional way of sharing documents with collaboration is to send a Microsoft Word document to another recipient, and ask them to make revisions to it. The problem with that scenario is that you need to wait until receiving a return copy before you can see or make other changes because you are locked out of editing it until the other person is done with it. That’s how databases work today. Two owners can’t be messing with the same record at once. That’s how banks maintain money balances and transfers; they briefly lock access (or decrease the balance) while they make a transfer, then update the other side, then re-open access (or update again). With Google Docs (or Google Sheets), both parties have access to the same document at the same time, and the single version of that document is always visible to both of them. It is like a shared ledger, but it is a shared document. The distributed part comes into play when sharing involves a number of people."

Mougayar adds, "Imagine the number of legal documents that should be used that way. Instead of passing them to each other, losing track of versions, and not being in sync with the other version, why can’t *all* business documents become shared instead of transferred back and forth? So many types of legal contracts would be ideal for that kind of workflow. You don’t need a blockchain to share documents, but the shared documents analogy is a powerful one."

Blockchain technology is well touted for its very durable and reliable qualities as a database of information. The Bitcoin blockchain technology has been operating since 2008 and so far has not experienced any major disruptions or failures, although there have been some incidents brought about by hacking attempts or human error. The technology itself has proven to be as reliable as it is
robust, which makes it even more attractive to users apart from the independence from controlling entities.

Author and TEDx speaker Ian Khan from Technology Futurist sings the praises of blockchain technology. "As revolutionary as it sounds, Blockchain truly is a mechanism to bring everyone to the highest degree of accountability. No more missed transactions, human or machine errors, or even an exchange that was not done with the consent of the parties involved. Above anything else, the most critical area where Blockchain helps is to guarantee the validity of a transaction by recording it not only on a main register but a connected distributed system of registers, all of which are connected through a secure validation mechanism," he said.

Aside from reliability, blockchain technology is also quite transparent, and is designed to do self-checks every ten minutes, going through transactions and reconciling or fixing overlaps. This self-checking, self-correcting feature not only makes it publicly transparent but also almost impossible to corrupt, as any attempts to corrupt the data in blockchain would require overriding the network as a whole, with the use of massive computer processing.

Ethereum inventor Vitalik Buterin says, "Blockchain solves the problem of manipulation. When I speak about it in the West, people say they trust Google, Facebook, or their banks. But the rest of the world doesn’t trust organizations and corporations that much — I mean Africa, India, the Eastern Europe, or Russia. It’s not about the places where people are really rich. Blockchain’s opportunities are the highest in the countries that haven’t reached that level yet."

How do data get transmitted to the blockchain? The blockchain is made up of a group or network of computer nodes. Each computer obtains a copy of the blockchain when the user joins the blockchain network. *BlockGeeks.com* describes this as a very powerful second-level network with each node as an administrator and the opportunity to win Bitcoins.

"Nodes are said to be “mining” Bitcoin, but the term is something of a misnomer. In fact, each one is competing to win Bitcoins by solving computational puzzles. Bitcoin was the raison d’etre of the blockchain as it was originally conceived. It’s now recognized to be only the first of many potential applications of the technology ... As well, a range of other potential adaptations of the original blockchain concept are currently active, or in development,” the site says.

Peer-to-peer information and database management is the central aspect of the decentralized technology behind Bitcoin’s blockchain technology. The network of computers that are interconnected to Bitcoin’s blockchain manage the transactions and records, making it unnecessary for any large, centralized, governing authority to have to pull together the records and open up the possibility of external control or influence.

Former United States Secretary of the Treasury Larry Summers says, "Bitcoin has the same character a fax machine had. A single fax machine is a doorstop. The world where everyone has a fax machine is an immensely valuable thing."

Meanwhile, Melanie Swan, the author of Blockchain: Blueprint for a New Economy, boldly predicts, "I think decentralized networks will be the next huge wave in technology."
And Mougayar adds, "Online identity and reputation will be decentralized. We will own the data that belongs to us."

How does security on the Bitcoin blockchain technology work? Overall security on the network uses encryption technology, and every user has a set of public and private keys. The public key refers to the user’s address on the network; this set of numeric characters is randomly generated and every Bitcoin can be traced back to its originating public key or address. The private key, on the other hand, is like a password. The user needs the private key to be able to access the information he or she has stored in the blockchain.

This technology provides users with the ability to transact with each other without the need to go through any other channels or authorities. If you are closing a deal with someone, for instance, a vehicle purchase, if you have their Bitcoin information you can then directly complete the settlement there. No need for any third-party to process the sale and go through additional paperwork or verification.

George Howard, an associate professor at Brown University and Berklee College of Music, and also the founder of his company, George Howard Strategic, says 2017 in particular will be a year of massive use of blockchain technology among business startups. "2017 will be a pivotal year for blockchain tech. Many of the startups in the space will either begin generating revenue – via providing products the market demands/values – or vaporize due to running out of cash. In other words, 2017 should be the year where there is more implementation of products utilizing blockchain tech, and less talk about blockchain tech being the magical pixie dust that can just be sprinkled atop everything. Of course, from a customer’s viewpoint, this will not be obvious as blockchain tech should dominantly be invisible – even as its features and functionality improve peoples’/business’ lives ... This implementation stage, which 2017 should represent, is a crucial step in the larger adoption of blockchain tech, as it will allow skeptics to see the functionality, rather than just hear of its promise."

How is blockchain technology continually changing Internet-based transactions and processes? One aspect is smart contracts, or simple contracts coded in the system that are executed when basic requirements are satisfied. Smart contracts can be used for various functions such as payouts automatically released when certain thresholds or benchmarks are met.

Another area, although still in mostly developing stages, is crowdfunding and the sharing economy. As Bitcoin and other cryptocurrency options become more available to the mainstream users, crowdfunding for initiatives becomes easier to achieve in the peer-to-peer setting. An example of this would be Ethereum’s Decentralized Autonomous Organization (DAO) experiment in 2016, which was crowd funded using DAO tokens and raising over $200 million in two months. Meanwhile, the sharing economy can also greatly benefit over the next few years as peer-to-peer payments with no additional transaction fees become feasible.

Yet another advantageous position blockchain technology finds itself in is the ease and security of file storage. Because information can be decentralized or stored throughout the network, they become more difficult to lose or get hacked. Decentralized web sites help to reduce the amount of information going through already overloaded online content systems, increasing average file transfer times and streaming requirements.
Blockchain technology makes land title registration and purchases much faster and more efficient. As BlockGeeks.com explains, "As publicly-accessible ledgers, blockchains can make all kinds of record-keeping more efficient. Property titles are a case in point. They tend to be susceptible to fraud, as well as costly and labour intensive to administer. A number of countries are undertaking blockchain-based land registry projects. Honduras was the first government to announce such an initiative in 2015, although the current status of that project is unclear. This year, the Republic of Georgia cemented a deal with the Bitfury Group to develop a blockchain system for property titles ... Most recently, Sweden announced it was experimenting with a blockchain application for property titles."

With blockchain technology, stock trading and share settlements become more efficient as confirmations happen almost immediately or in short time periods, compared to normal clearing times of up to three days. As blockchain becomes more commonplace in stock trading, common third parties such as auditors, clearing agencies, and consultants become less essential. In fact, as BlockGeeks.com points out, many stocks and commodities exchanges are now testing their blockchain applications for their services, such as "the ASX (Australian Securities Exchange), the Deutsche Börse (Frankfurt’s stock exchange) and the JPX (Japan Exchange Group)."

Furthermore, the site says, "Most high profile because the acknowledged first mover in the area, is the Nasdaq’s Linq, a platform for private market trading (typically between pre-IPO startups and investors). A partnership with the blockchain tech company Chain, Linq announced the completion of its first share trade in 2015. More recently, Nasdaq announced the development of a trial blockchain project for proxy voting on the Estonian Stock Market."

“There are so many people involved in the healthcare process for a single patient – hospitals, doctors, insurance companies and, in some cases, the government – so how do you make sure those records remain secure, encrypted, and that they’re not lost or corrupted? Blockchain can act as an encryption process so that documents can be shared securely, and also ensure that documents are not altered,” Mann told The Guardian.

"Bitcoin is the one solid, mostly-undisputed success story of blockchain, but there are lots of obstacles to come and we still don’t know if it can stand the test of time," Mann continued. "We’re still in the exploratory, Wild West phase of blockchain development but I am hopeful that it can serve a purpose."
Chapter Five: How To Obtain Or Accept Cryptocurrency Coins

Because of the number of options out there for cryptocurrency, this can be both exciting and confusing for the beginner. Which one should you go for? Where do you start? How do you compare which is the best for your needs? Keep in mind that you don’t have to know everything and each type of cryptocurrency available on the market to be able to start enjoying its advantages. With more than 700 different kinds of cryptocurrency out there, it will be near impossible to familiarize yourself well with each one anyway.

Before you dive in, understand first that cryptocurrency is not a typical investment, and is a world of difference away from the usual shares or investments. Cryptocurrency is purely digital coins or tokens, so don’t expect any paper certificates to hold on to. Also, as you are purchasing your cryptocurrencies, remember that you are also contributing to the development of these decentralized networks.

Brian D. Evans, the founder of BDE Ventures, gave these tips for buying digital currencies for beginners: "For most people in the U.S., Coinbase would be the easiest option to buy Ethereum, Bitcoin, or Litecoin (it doesn't support any others yet). After verifying your account, you can add a number of payment methods including credit or debit cards, U.S. bank accounts, or even wire transfers of funds. Other options for exchanges that will take U.S. dollars for coins are Kraken, and Gemini in the U.S. Typically you will need to verify your account with a driver's license and add other details to expand your buy limits. Since cryptocurrencies are "hard currencies," the exchanges don't want to risk getting ripped off, since you can't reverse a cryptocurrency transaction once it's done."

Evans also notes that there are up-and-coming cryptocurrencies you would want to check out also. "If you are looking for some of the newer coins that are making big movement but haven't made their way to the aforementioned exchange sites, you can look into Poloniex or Livecoin. You can transfer Bitcoin or Ethereum to these platforms from Coinbase and then exchange it for any other digital currency that you want."

Why should you start buying cryptocurrencies? One reason would be speculator, as there is a chance that the cryptocurrency you purchase may soon grow exponentially in value, increasing your wealth. If you are looking to diversify your wealth, cryptocurrency would be one of the options you can look into for future growth.

Financial stability would be another reason for buying cryptocurrencies. Many people today are skeptical of governments and central governing authorities over banks and other financial institutions, so they are purchasing cryptocurrencies as these are free from central banks and oversight. When financial markets experience recession or even crashes, digital currencies such as Bitcoin may prove to be great investments.

Once you are ready to start, you will need a wallet or private key as already mentioned in previous chapters, or you can purchase directly from any number of cryptocurrency exchanges. TechFruit.com's Joaquim Miro relates, "After finding out which cryptocurrency you want to buy, you will place a bid to buy at a certain price, or at the market price. You will also indicate which
public key you want your currency to go into. Think of public keys as a holding account. The public key tells people which holding account to send the currency to. Then you also have a private key, which is encrypted and protects your currency that is held in that specific holding account in your wallet. This key is decrypted only at the moment where the transaction goes through, which happens behind the scenes so you don’t know to worry about it."

Perhaps you have a business or entrepreneur and you are considering accepting Bitcoin or other cryptocurrency in your purchases and orders. Nasdaq.com says yes, “In years past U.S. merchants have had to pay over $78 billion in credit and debit card processing fees. Since cryptocurrencies are decentralized, meaning that they don’t require a bank to verify each transaction, you can eliminate those transaction fee which normally cost 2 percent up to 5 percent for each transaction. In other words, it costs almost nothing for your customers to transfer funds to you. As for you — as a business owner — don’t have to share your hard-earned revenue with that third party financial institutions.”

If you are looking to get a slice of the pie, now would be an excellent time to start in cryptocurrency. TechnologyReview.com "When it comes to the future of money, there is a growing consensus that cryptocurrencies are set to play a major role. One cryptocurrency, in particular, has entered the public lexicon as the go-to digital asset: Bitcoin. But the cryptocurrency market is significantly more complex than the public lexicon might suggest. And while there have been plenty of studies examining the role and future of Bitcoin, there have been few that explore the broader cryptocurrency market and how it is evolving."
**Conclusion: Where Is Cryptocurrency Headed?**

The prevailing attitude among so many in the world today is one of independence and taking more control over one’s various affairs and transactions in daily life. This is where cryptocurrency is conveniently positioned, as it offers a level of security and privacy that would be comparable to paper bills or coins. It is also riding the continued transition of many aspects of the human experience from the physical to the digital. With its easy access and continued growth in many sectors, it would be only a matter of time before many other cryptocurrencies also explode in growth, in much the same way as Bitcoin, Ripple, etc.

Simon Yu, the CEO of a company called CakeCodes, made this observation about the accelerated growth of the cryptocurrency segment: "The astronomic price growth of bitcoin signals the increasingly widespread acceptance of digital currency in general. The market has now recognized that bitcoin is a better store of value than gold, being particularly useful in facilitating and securitizing financial transactions. As regulators and countries catch up to the growing demand and legally acknowledge bitcoin as legal tender, we can only expect the price to follow."

Doug Miller, the Vice President of Business Development for a hardware wallet company called KeepKey, also has his eyes set on the rapid acceptance of cryptocurrency. "Bitcoin has momentum; more and more people and businesses are becoming aware of how important this form of payment and investment is becoming. With supply being low and demand being high, this is a great formula for bitcoin's rising value," he said.

Bitcoin, in particular, is currently setting record highs in its price. **CNBC.com** reports, It is close to hitting a price that could see a 47 percent correction, according to one analyst, following a huge rally for the cryptocurrency that has led it to record highs. On Thursday, bitcoin hit an all-time high of $2791.70, according to CoinDesk data, marking a 180 percent rally year-to-date. Meanwhile, the number of long positions – those betting on bitcoin to rise – has risen 18.2 percent, while short positions – those thinking the cryptocurrency will fall – have declined 10 percent since the start of the week, showing that traders are getting more bullish on the cryptocurrency, according to data from Bitfinex."

Bitcoin could also continue to be the gateway or starting point for customers who want to use not just Bitcoin but other cryptocurrencies as well, and as these cryptocurrencies gain a foothold on the mainstream, Bitcoin will continue to lead and become the benchmark. Daniel Masters, director of Global Advisors Bitcoin Investment Fund, said, "Some of these currencies are doing a lot better relatively, but the point here is we are moving into this really rich diverse cryptocurrency ecosystem side by side the fiat currency."

Perceptions regarding bitcoins and cryptocurrency in general are also changing. While the wariness still exists regarding its potential for being used in nefarious online activities, much of the attention has shifted towards what can be its positive effects on burgeoning enterprises, developing economies, and emerging sectors of the market that can use cryptocurrency’s peer-to-peer transactional ecosphere to speed up development at reduced costs.
Davide Menegaldo, Chief Operating Officer at HelperBit, has this view of the future of cryptocurrency: "I would imagine this scenario: in the future financial instruments linked to bitcoin will be finally approved. High finance will invest into the cryptocurrency (more than the 300M expected for the bitcoin ETF approval). I’m thinking about 5-10 times the current price. Bitcoin will not necessarily be used as a method of payment (it depends also on how the size block / Segregated witness / LN matter will proceed or will not), but primarily it will be used as a store of value. However, there will be much more competition as a payment method because some banks could issue their own crypto currency, while the current ones will remain a handful. Ethereum will consolidate as the second most important infrastructure, and 99% of ICO tokens will have any value."

Smart contracts, the main feature of the Ethereum network which uses ether tokens, could also become the wave of the future and improve the speed and efficiency of transactions on a global scale. Leonardo Pedretti of Etherevolution and Ethereum Italia tells Huffington Post that in the next five years, "users will use Ethereum even without knowing it. The same thing happens today when you download an app, without knowing deeply the technology used behind it."

Bitcoin looks poised to continue to lead at least over the next few years, but if you are looking for a viable alternative to Bitcoin, many experts lean towards newer cryptocurrencies such as Monero and Zcash. Ameer Rosic, contributor of the Huffington Post and Chief Executive Officer of Blockgeeks, said in his post What is the Future of Cryptocurrency?, “At present time, Dash and Zcash have respectively a value of $100 and $70. Of course their monetary values mean nothing in terms of what will happen in future, but we can say that they are showing a high interest. Also, Zcash provides a revolutionary cryptocurrency that is fully anonymous, so the data showed on the blockchain doesn’t provide any info about the amount or the people involved in the transaction. This feature may could be vital for Zcash future because no other digital currency - together with Monero (XMR) - allows this kind of complete anonymity and privacy.”

Scalability, in particular, is working in Monero's favor. "Today Monero ($123) reached the fourth place according to its market capitalization ($255,773,115), right after bitcoin, ether and dash. Created back in 2014, it soon doubled - and then quadrupled - its price. This renewed interested in the Monero currency might be caused by the low bitcoin scalability. In fact, it is faster and with lower fees than bitcoin," Rosic says. "This means that if the scalability-related issue of bitcoin won’t be solved soon (hard-fork scenario), altcoins will increase their value, popularity and market cap, so they will be more used as payment gateway, while bitcoin will be more and more exploited as a store of value. But this is only if the block size debate won’t be solved soon."

The next decade will undoubtedly lead to more innovations in the cryptocurrency, and as Bitcoin, Ethereum, LiteCoin, Monero, ZCash, and other cryptocurrencies firm up their niches in the market, mainstream acceptance will increase and established financial institutions will continue to find ways to integrate cryptocurrency into their platforms, better serving customers and leading to a more open and inclusive marketplace.

Whether you choose to deal with only one type of cryptocurrency, or perhaps a combination of different digital currencies depending on your needs and what they offer in terms of privacy and turnaround, it would also be wise to seek to work them into any established financial services from
traditional providers which you already subscribe to, as a co-existing atmosphere between the two looks poised to be the norm in the years to come.