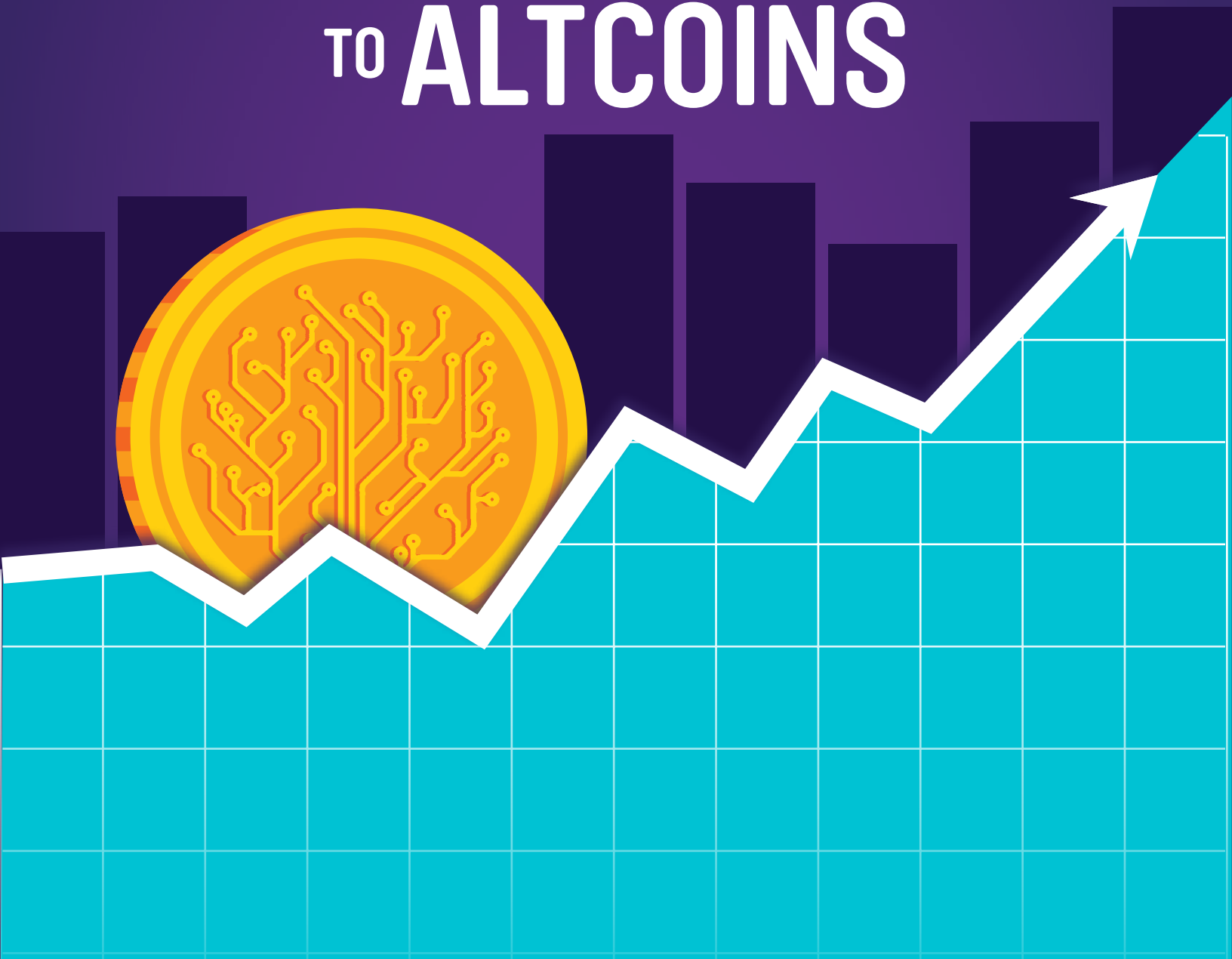
ABRA

THE ULTIMATE GUIDE TO ALTCOINS



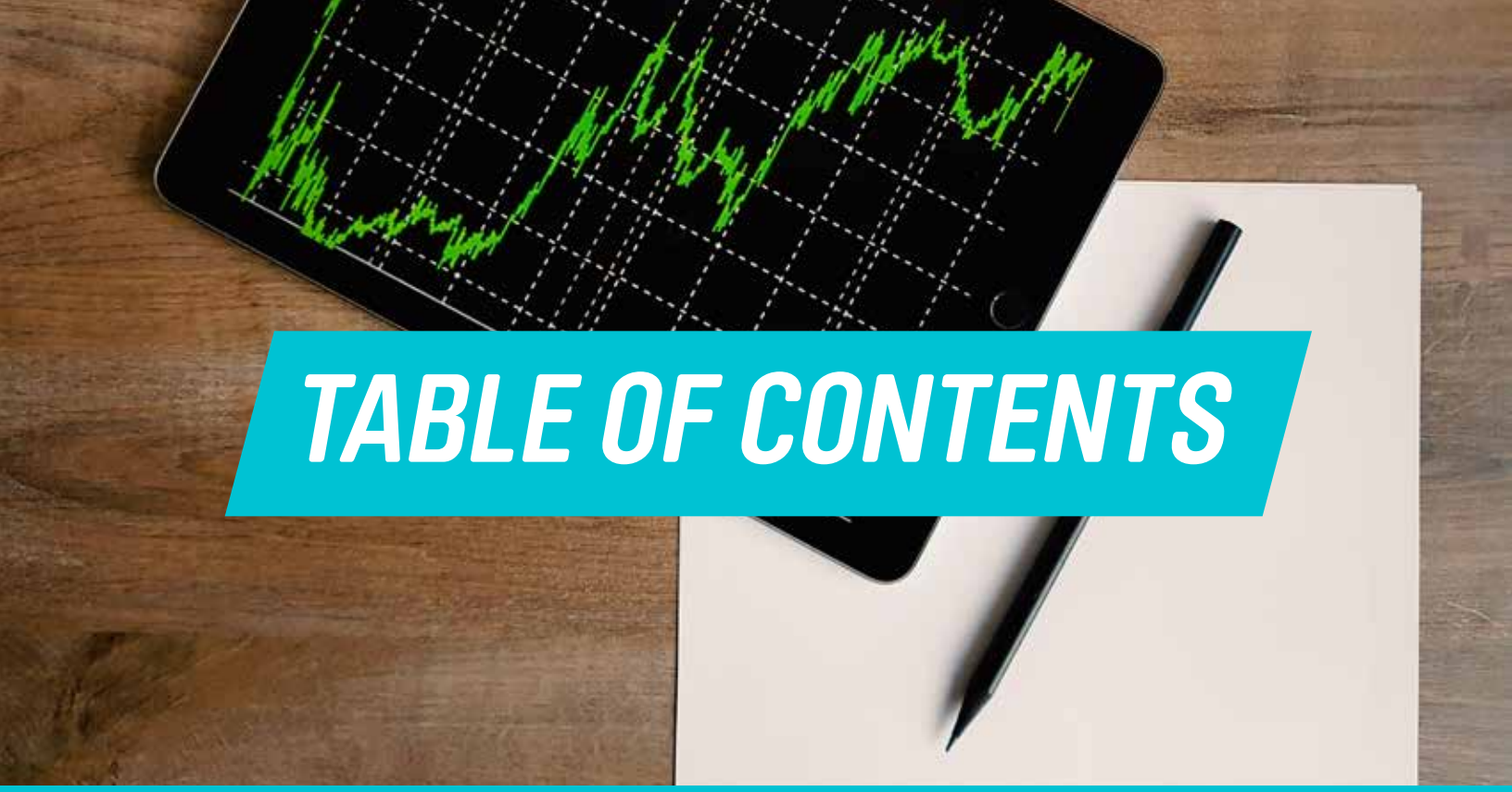


TABLE OF CONTENTS

Introducing altcoins

By now, you've surely heard of Bitcoin and cryptocurrency. During the past few years, these words have become household names, making headlines as the new global cryptocurrency market swells into the hundreds of billions of dollars.

For the good or the bad, Bitcoin generally gets all of the attention from the mainstream media. But there is a lot of experimentation and innovation happening with other forms of cryptocurrency. These other projects are generally lumped into a single massive category and called altcoins, as in alternative to Bitcoin.

While they are lumped together for the sake of definition, there are actually a lot of distinctions among altcoins. So much so that it's worth taking the time to try and understand how some of these projects work and what kinds of problems they are trying to solve.

The birth of Bitcoin and rise of altcoins

Bitcoin began as a white paper sent to a cryptography email list on October 31, 2008, by the mysterious Satoshi Nakamoto. While the identity of Nakamoto remains a mystery, the paper called *Bitcoin: A peer-to-peer electronic cash system* changed the world.

By January 2009, Nakamoto released the Bitcoin distributed ledger that acts as the network's foundation. Soon after, the genesis block, or the very first series of Bitcoin transactions, was recorded. As of mid-2018, more than 500,000 blocks full of verified transactions have been added to the distributed ledger.

Bitcoin is a major innovation for several reasons. In the computer science realm, the launch of Bitcoin brought with it a new way of organizing and interacting with data, which can have implications on all kinds of digital activities ranging from finance and money transfers to personal privacy and identity.

While the internet has changed the way people interact, do business, find friends, etc., there is still one big problem. It's hard to trust information on the internet, and it's even harder to interact in a secure way with people or businesses without the need for a third-party.

The problem that Bitcoin and altcoins solve

Bitcoin and altcoins are trying to create the infrastructure needed to conduct safe and secure transactions in a digitally-native way.

At their core, most of these new altcoin technologies are working toward replacing third-parties (such as banks, credit card companies, or any other centralized service that people currently need to interact on the internet) with tools that will allow people to act in more of a peer-to-peer matter, but to be able to do it in a way that protects against theft and fraud.

The main issue with third-parties, or intermediaries, is that they often turn into rent-seekers. Payment services charge high rates, for example. If digital services are not charging up-front fees, they are making money off of users in some other way, such as collecting and selling personal data, or from advertising.

Token economics is another major innovation enabled by the creation of Bitcoin and that is being explored in greater depth by many altcoins. These token economies enable groups of people to create systems of value that align goals or work with economic incentives.

Like the idea of creating trusted and secure data without the need for a third-party, creating technologies like Bitcoin and altcoins that allow for people to create sustainable economies will open up new opportunities for secure collaboration that will lead to innovation across sectors such as finance, social networking, communication, and many other fields.

Key cryptocurrency attributes

Before launching into altcoin specifics, it's important to think about the attributes that define cryptocurrencies. If nothing else, understanding the basics will be helpful when pondering the potential of different altcoin projects.

Not all cryptocurrencies are created the same, but there are enough similarities between most of the key cryptocurrency systems that it is possible to create a list of common crypto characteristics:

Open source: One of the key characteristics of Bitcoin is that it is an open source network. This means that anyone can copy or clone the underlying computer code and build on top of it. This has happened several times already, most notably resulting in the creation of Litecoin and Bitcoin Cash. Most altcoin systems are built using open source principles and many altcoins are iterations of one another (like Ethereum and Ethereum Classic) or they might be a more specific application built on an existing blockchain. Like the altcoin Auger, which will create tokens that are part of a prediction market that is based on top of the Ethereum, which is a protocol-level blockchain.

Decentralized: This often refers to the governance of cryptocurrencies. Rather than being run by single entities or corporations, cryptocurrency networks are often operated in a public and permissionless manner, which means anyone with the right kind of computer equipment can download the network and run a node. Decisions about network updates and other important changes are made by the consensus of the network, which can sometimes be challenging. The tradeoff is that the network is distributed and more secure than systems that have single points of failure.

Peer-to-peer: As mentioned above, cryptocurrencies are designed to operate as peer-to-peer systems, rather than centralized systems. This kind of technology is designed to eliminate all kinds of middle-men and inefficiencies and inequities created by large organizations and institutions.

Blockchain-based: This almost goes without saying, but it's important distinction when thinking about how cryptocurrencies differ from other forms of "digital money." A blockchain, or a distributed ledger, is the base-layer infrastructure that enables all of the things on this list.

Not all cryptocurrencies follow the outline above. Some have deviated from these waypoints to try and create other kinds of tools and models. It's really important to do research and understand how each coin works and how it compares to other cryptocurrencies.

What are altcoins?

Besides Bitcoin, more than 1,500 altcoins exist. Together they comprise a global cryptocurrency market that as of mid-2018 was valued at over $300 billion.

As mentioned earlier, altcoins can exist in several formats. Some altcoin projects are trying to develop completely new kinds of blockchain protocols. These new protocols are often designed for specific traits. Monero and Zcash, are both new altcoins that were created with greater user privacy and security in mind, but each protocol is built upon different cryptographic principles.

A few altcoins, like Bitcoin Cash and Ethereum, are variants (or what are called forks) of other cryptocurrencies. Bitcoin was forked to create Bitcoin Cash, which enables faster transactions, and Ethereum Classic was forked to create Ethereum after a controversial decision to rewrite some of transactions recorded on the original Ethereum blockchain.

Other altcoins function more like utility tokens (which in this case means they are not necessarily building their own blockchain, but instead they will operate on top of an existing protocol).

In addition to offering digital alternatives to traditional currency, development teams around the world are using distributed and decentralized blockchain technologies to address challenges in computing power, file storage, and other digital bottlenecks with new blockchain-based solutions.

No one can be sure which of these coins will succeed, but this guide was created to introduce a few other cryptocurrencies that might be worth keeping an eye on.

Altcoin opportunities

This guide is not intended as investment advice, but it is a brief overview created to provide some information about how altcoin markets work.

Today, Bitcoin accounts for less than half of the total cryptocurrency market capitalization because of the dramatic growth in altcoins during 2017. Ethereum occupies second place in terms of market cap. As of mid-2018, the price of one unit of Ethereum (known as ether, or ETH) is hovering around $500.

Back on January 1, 2017, the price of one ETH was $8.24. Put another way, if you invested $10,000 on January 1, 2017, that investment would be worth approximately $600,000 today. In about a year and a half, the value of ETH has increased in a way that represents unprecedented gains when compared to any other conventional investment or financial market.

It's important to remember that not all altcoins are created equal. Some, like Ethereum, have global development teams working on a shared vision and have a strong community supporting those goals. Other altcoins exist as little more than a website and a white paper and they have somehow raised millions of dollars.

It's really important to do your own research and to understand the technology behind each of these systems. With that said, the majority of the cryptocurrency market is contained within the altcoins that follow Bitcoin.

Abra has made it easy to buy, sell, and hold both Bitcoin as well as 25 altcoins and counting. The rest of this guide will provide some background and context on some of altcoins listed in the app.

This guide is for informational purposes only. It is not intended as investment or financial advice.

Ethereum (ETH)

At a glance

Network launched: July 30, 2015
Origins: Whitepaper and crowdsale
Maximum supply: There is no maximum supply, but the current circulating supply is 100,242,669
All-time high: $1,377.72 on January 13, 2018

What is Ethereum?

"Ethereum is a decentralized platform that runs smart contracts: Applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference."
—ethereum.org

Ethereum is a blockchain system where thousands of computers around the globe are networked together to create a distributed, decentralized computer. This computer runs an operating system called the Ethereum Virtual Machine (EVM).

The EVM understands and executes the software written in Solidity, or other Ethereum-specific programming languages. The applications executed by the EVM are called smart contracts. A smart contract is just a program that controls the transfer of ether between accounts if certain conditions are met. For example, a smart contract for landlords could exist on Ethereum and the locks in the rented apartment only continue to open if the renter pays their monthly bill.

It is not free to access and run computations on the Ethereum blockchain. Like in Bitcoin, a native cryptocurrency is necessary for the blockchain to function. Ether (ETH) is the native token that enables users to pay to execute smart contracts on the Ethereum world computer.

Why is Ethereum important?

A growing number of entrepreneurs and developers view Ethereum as a valuable tool and have started to use it to build decentralized businesses that couldn't have existed before. Ethereum smart contracts can be used to eliminate third parties from many industries, which would lower costs and creates more secure products. Ethereum use cases are many, including decentralized identity registration, supply chain management, and democratized crowdfunding.

Due to the demand for ether, the value has increased rapidly over the past year. The Ethereum network now processes more transactions per day than Bitcoin. The number of applications and businesses have also been increasing at an exponential rate. Ethereum is only three years old, but it is showing tremendous potential to create trustless, decentralized applications that will be used by millions of people across the world.

Litecoin (LTC)

At a glance

Network launched: October 13, 2011
Origins: Bitcoin fork
Maximum supply: 84,000,000
All-time high price: $375.29 on December 18, 2017

What is Litecoin?

"Litecoin is a peer-to-peer internet currency that enables instant, near-zero cost payments to anyone in the world."
— litecoin.org

Litecoin was designed in 2011 to enable faster and cheaper blockchain-based transactions by Charlie Lee, a former employee at Google. The Litecoin protocol experienced massive adoption and growth in 2013, reaching a $1 billion market capitalization shortly thereafter.

As of June 2018, Litecoin ranks number six in terms of total market capitalization. Litecoin transactions take significantly less time to transfer than Bitcoin, with a fraction of the transaction fees, opening up usage possibilities for everyday purchases where Bitcoin may be prohibitively slow or expensive. In short, Litecoin is similar in functionality to Bitcoin, and it is faster and cheaper, which enables the possibilities of everyday transactions.

In May 2018, Abra announced native functionality for Litecoin, meaning Abra users can now directly deposit litecoin into the Abra app, make trades for other altcoins and then make withdrawals again in Litecoin.

Why is Litecoin important?

The main advantage of Litecoin is that it made day-to-day purchases possible. When the price of Bitcoin was low, purchasing something quickly and cheaply may have been possible, but at its all-time high in December 2017, buying a single cup of coffee with Bitcoin would have cost $30+ in fees. On top of that, the transaction would take at least an hour to process, if not much longer — not exactly ideal for everyday purchases. The cryptocurrency community is actively trying to solve this problem with technologies such as Lightning Network for Bitcoin, but as of today, these protocols have not yet been fully implemented.

Litecoin on the other hand, was designed to make payments instant, by enabling transaction verifications that take minutes rather than hours, which lowers transaction fees.

While the value of Litecoin continued to surge year-over-year, it was still somewhat complicated to purchase until recently when it was added to the exchange Coinbase in May 2017. Once more widely accessible, Litecoin experienced a meteoric rise, and wound up increasing in price by 6,000 percent in 2017 alone.

Another key distinction between Litecoin and Bitcoin is the size of the market. As of mid-2018, Bitcoin had 17,079,137 bitcoin in circulation. Litecoin, on the other hand, had 56,865,548 LTC in circulation.

How does Litecoin work?

Many cryptocurrencies are created through a process called mining, which means that many computers on the network are solving computationally difficult puzzles to validate transactions. Miners are rewarded for their work, or for dedicating computing power to the network, by receiving newly issued units of the cryptocurrency being mined.

This model of dedicating computer time and energy toward maintaining a blockchain and creating new cryptocurrency is called proof-of-work, or PoW.

Once the network reaches consensus (which is what the mining process is all about) and records a transaction to the blockchain, it's very difficult to change or invalidate this work because it would require going back and redoing all the work that had already been done. While this would be technically possible it is very costly in terms of the energy and computing power required, making it practically and economically difficult to defraud the blockchain.

Bitcoin and Litecoin both rely on proof-of-work, but they go about the process using different methods, which ultimately results in differences in transaction speed and cost. Bitcoin uses the SHA-256 hashing algorithm, requiring costly and sometimes hard-to-find ASIC (Application-Specific Integrated Circuit) equipment, whereas Litecoin can be mined on the less expensive and more common GPU (Graphics Processing Unit) found in computer video cards.

Litecoin runs on what is called the Scrypt algorithm, which didn't allow the jump to mining on ASIC setups, keeping the barriers to entry lower, at least at first. Today, Litecoin mining (as well as mining other cryptocurrencies) is getting more complicated and expensive.

Ripple (XRP)

At a glance

Launched: 2012
Origins: Ripple is based on an earlier payment network called OpenCoin
Maximum supply: 100,000,000,000
All-time high: $3.84 on 1/4/2018

What is Ripple (XRP)?

"Ripple provides one frictionless experience to send money globally using the power of blockchain. By joining Ripple's growing, global network, financial institutions can process their customers' payments anywhere in the world instantly, reliably, and cost-effectively. Banks and payment providers can use the digital asset XRP to further reduce their costs and access new markets."
— ripple.com

Ripple is the name of the company that created what is known as the Ripple Protocol, as well as the XRP token. Both of these are more commonly referred to as Ripple. Ripple offers near-instant transactions at low cost, but does so in a way that some consider controversial or even contrary to truly decentralized cryptocurrency systems. There's no mining, there exist some elements of centralization, and the network validation is built upon private nodes.

Ripple's goal is to create a global, enterprise-scale blockchain solution for handling payments across borders with no chargebacks. This type of service is designed primarily for banks, payment providers, and other financial institutions.

Ripple's market potential consists of the hundreds of trillions of dollars that move across borders each year. Ripple experienced 36,000+ percent growth in 2017, making it the year's best performing cryptocurrency. As of mid-2018,

it ranks third in total market capitalization. At one point in late 2017, Ripple reached a total market capitalization of over $130 billion, rising to an all-time high of $3.84 per XRP token.

Why is Ripple (XRP) important?

Having raised over $93 million through traditional investment methods from some of the biggest names in venture capital, Ripple is much more than just a small team with a white paper or successful ICO (initial coin offering). The company itself is well-funded and counts the likes of UBS, Santander, Standard Chartered, UniCredit and American Express as customers.

Ripple primarily seeks to modernize cross-border payments on a global scale. Transferring money across borders using traditional methods, such as third-party services, is painfully slow, and almost always expensive. The fastest way to get money from San Francisco to Berlin is to literally hop on a plane with cash and fly it there. A standard wire transfer or SWIFT payment can take days, and incur hefty fees. So, in an era of technological progress and rapid delivery of just about everything else on a global scale, why is it so difficult to move money from one country to another? Antiquated systems have created a need for new, less restrictive methods for transferring funds, and Ripple has developed a solution in an attempt to address this and modernize the global financial system.

Ripple and the XRP token run on the Ripple Protocol, which is built with private, centralized nodes. A node is a computer on the Ripple network that is authorized to verify transactions and keep the entire process running smoothly. In this fashion, the XRP ledger is not truly decentralized (like Bitcoin's permissionless, distributed ledger which allows anyone with a computer and internet connection to download and run a node) but rather functions through the collaboration and agreement of 55 validator nodes, held by private institutions such as Microsoft and Massachusetts Institute of Technology. This gives the nodes authority over the network as opposed to a more decentralized system.

XRP does not use proof-of-work to maintain the network and create new

coins. Instead, the Ripple supply is pre-mined. Some are held by Ripple and some have been distributed. Banks love this system because of the familiarity that centralization offers, but its lack of decentralization has been the source of some controversy among the cryptocurrency community.

How does Ripple (XRP) work?

Think of Ripple as a gateway — banks don't necessarily need to use the XRP token to adopt the Ripple Protocol; they can elect to use native fiat currency, other cryptocurrencies, or any other unit of value such as commodities, or even frequent flyer miles.

Transactions can enter the Ripple gateway as US dollars, for example, exchange into XRP, transfer to where it needs to go, then exchange back out into native fiat currency, such as Indian rupees, once it's reached its final destination. This method brings international wire transfer times down from days to just seconds. Confirmations are near instant, with no chargebacks, and transaction fees are minimal, with just .00001 XRP charged per transaction.

Payments settle in four seconds with Ripple, compared to hours with Bitcoin. Ripple can also handle 1,500 transactions per second versus an average of only three to four transactions per second with Bitcoin. The rapid transaction speed, and the ability to handle a high volume of transactions, means that Ripple offers a viable alternative to current payment processing models, and has been proven to be able to scale to handle the same throughput as VISA.

Stellar lumens (XLM)

At a glance

Launched: July 31, 2014
Origins: One of Stellar's founders was also involved with Ripple and the early Bitcoin exchange, Mt. Gox.
Maximum supply: 104,025,824,192
All-time high: $0.93 on January 4, 2018

What are Stellar lumens (XLM)?

"With a team of top technology and finance professionals, the nonprofit Stellar.org expands access to low-cost financial services to fight poverty and maximize individual potential."
— stellar.org

Stellar lumens (XLM) are the tokens released as native assets by the Stellar Development Foundation, a nonprofit launched by Ripple co-founder Jed McCaleb in 2014. While some may think that Stellar is a fork of Ripple, upon closer inspection, the two actually have much more in the way of differences than they do in common. They are, in McCaleb's words, two "*completely different codes.*" While the codes do differ — and Stellar would argue they made significant improvements to problems with Ripple — the key difference between them lies in their vision for the future of cryptocurrency.

Why are Stellar lumens (XLM) important?

Stellar considers itself "*finance with a mission.*" Large portions of the world's population remain unbanked, and Stellar seeks to make access and participation in the global economy universal. This philosophy is fundamentally inclusionary, and the entire codebase is open-source, meaning anyone can change or modify the code, and everyone can participate. Whereas Ripple is

for-profit, Stellar plans to cover operational costs by setting aside 5 percent of the total available lumens for their own use, along with accepting donations. If Ripple is going after the banking industry, Stellar is going after the individual.

One of the strengths of Stellar is the team they have created to guide the network they are building. They offer grants of up to USD $2 million in lumens to developer partners on behalf of the Stellar Build Project. Stellar recently partnered with IBM as part of their Hyperledger project, where they will attempt to solve the problem of global cross-border payments together.

Furthermore, Stellar contains one critical component that is not found with Ripple — the ability to conduct ICOs on the Stellar network. In other words, new cryptocurrency projects can use the Stellar blockchain to release their own token. So far, most new projects in the cryptocurrency space have launched ICOs using Ethereum using ERC20 tokens. But, due to Ethereum's popularity coupled with current scaling mechanisms, the past year saw massive backlogs of transactions with slow transaction speeds and volatile, hefty fees. Stellar promises faster transactions and lower costs than Ethereum, which is why some crypto startups have started to use Stellar as a platform to launch initial coin offerings.

These features, combined with the decentralized and altruistic mission of Stellar, have attracted favorable attention in contrast to the criticism facing Ripple. The two are pursuing very different things, and many feel there is room for both in the big picture of the global financial ecosystem.

How do Stellar lumens (XLM) work?

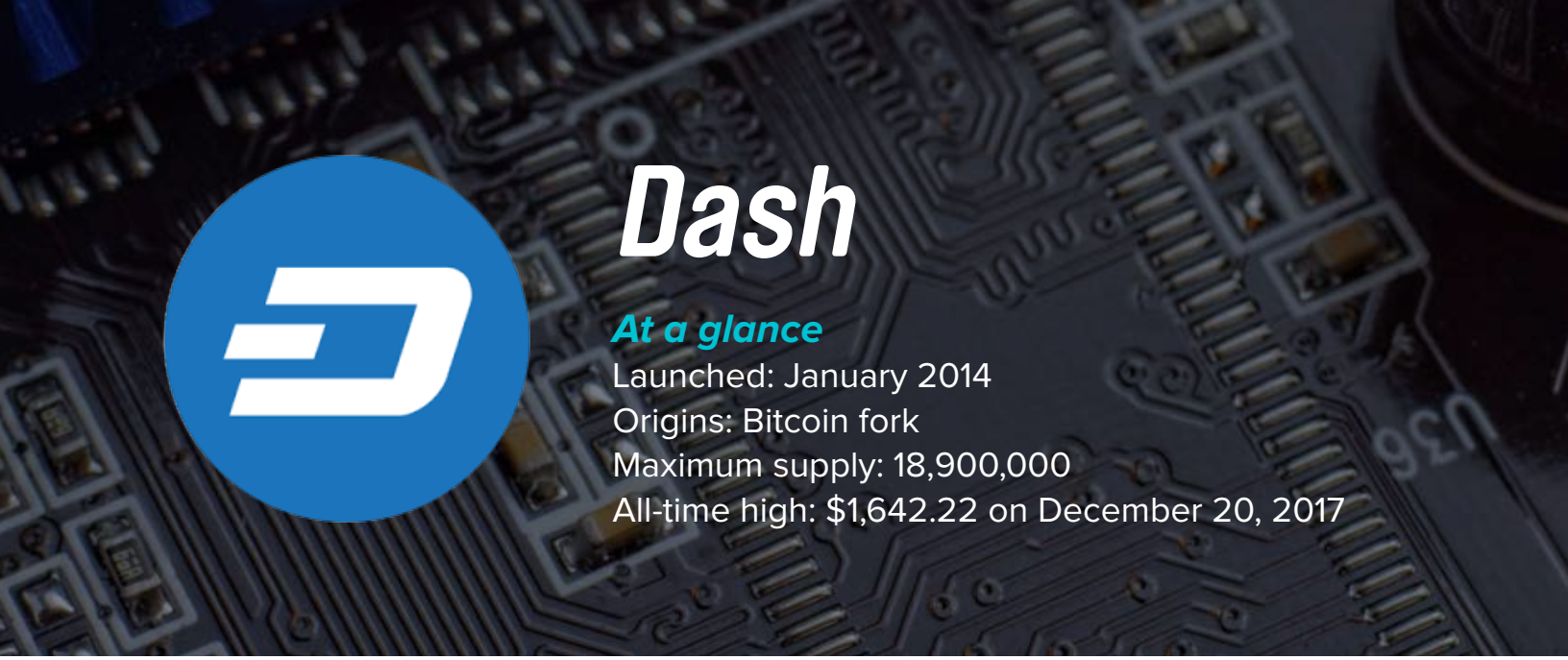
Stellar operates on what is called the Stellar Consensus Protocol, a decentralized network of peers capable of running independently of one another. This decentralized network of servers syncs and reaches consensus, creating the Stellar network and allowing the ledger to be distributed as widely as possible. Stellar isn't as decentralized as something based on a proof-of-work mechanism such as Bitcoin, but it achieves better speed and efficiency as a result of this trade-off. While the original code base was similar to Ripple, the latest version, Stellar-core, is quite different, using a separate consensus

algorithm entirely.

Stellar also differs from Ripple in terms of how the exchanges take place. Banks collaborate directly with Ripple to provide the intermediary services necessary to exchange one currency for another and send it on its way. With Stellar, this occurs in a more decentralized fashion. Stellar uses what are called "anchors," which in their words do the following:

"Anchors are simply entities that people trust to hold their deposits and issue credits into the Stellar network for those deposits. They act as a bridge between different currencies and the Stellar network. All money transactions in the Stellar network (except the native digital currency of lumens) occur in the form of credit issued by anchors."

So, the anchors help with currency transfer, but how does the exchange take place? An official Stellar exchange supports transactions in a few ways. First, by facilitating peer-to-peer exchanges, such as when someone wants to exchange US dollars with someone else who has Indian rupees. Second, lumens can be exchanged for Indian rupees to bridge the gap: Someone can buy lumens with US dollars, exchange those lumens for Indian rupees on the Stellar exchange, and then send them to the final recipient. Lastly, a chain of conversions can be created to link them along. For example, the US dollar could be exchanged for euros, and then those euros could be exchanged for Indian rupees. This is all possible with the Stellar exchange, with the help of lumens to fill the gaps when necessary.



Dash

At a glance

Launched: January 2014
Origins: Bitcoin fork
Maximum supply: 18,900,000
All-time high: $1,642.22 on December 20, 2017

What is Dash?

"Dash is digital cash. Money exchanged on a highly secure, open source, peer-to-peer network, much like Bitcoin. But, unlike Bitcoin, it's really the first form of digital cash that works just like physical cash."
— dash.org

Dash first burst onto the scene in 2014 and has been tearing its way through the charts and the press ever since. As of mid-2018, it sits at number 13 by market capitalization, with the total circulating supply of roughly 8 million dash valued around $86 million. The total possible future supply is limited to close to 19 million. Dash prides itself on being private, (nearly) instant, and secure. With transaction confirmations taking four seconds, they're available even faster (1.3 seconds) for those who choose to pay a small fee using something called InstantSend. This makes it possible to actually buy a cup of coffee with cryptocurrency, just like cash.

Why is Dash important?

Dash is fungible. What this means is that one dash can be substituted for another dash, much like how one dollar can be traded for another dollar, regardless of where that dollar has been. As part of a transaction, once dash is mixed through a native-feature called PrivateSend, all previous history is cleared,

making it impossible to distinguish one dash from another.

Since the digital cash is not held by a bank, purchase histories are private and they can never be tracked or intercepted. Transactions occur near instantaneously, with low or even zero fees because there's no bank in the middle. What's more, many businesses accept dash already — web hosts, VPN providers, web stores, marketing services, online games, and online casinos.

How does Dash work?

Dash was created as a hard fork of Bitcoin in order to emphasize privacy, which the Dash development team found lacking in Bitcoin's system. It features a protocol-level, trustless mixing service called PrivateSend. In essence, this means that units of Dash are moved around and mixed up on the way from point A to point B in order to make transactions truly anonymous. Because Dash started with the Bitcoin codebase, it was immediately compatible with all existing merchant, exchange, and wallet software written for Bitcoin. It takes two-and-a-half minutes for a transaction to appear on the Dash blockchain.

Dash doesn't need to reach unanimous community consensus to make significant changes to the codebase, so it's not at risk of hard-forking due to changes in the core code. (One example of a hard fork happened in late 2017, when Bitcoin was forked over a scaling debate. The result of the fork was the creation of Bitcoin Cash.) Instead of the forking model, Dash developers set up a system for voting democratically on major changes, with a system of master nodes.

A master node is an individual who holds enough Dash to have a "stake" in the ecosystem and enables Dash-specific functions like InstantSend and PrivateSend. Think of these master nodes as something like voting shareholders. They vote on things such as what should happen with new projects, who should get funding from the treasury, and which direction development should go.

Ethereum Classic (ETC)

At a glance

Launched: July 30, 2015
Origins: the original Ethereum blockchain
Maximum supply: there is no maximum supply, but the circulating supply is 102,239,847
All-time high: $47.77 on December 20, 2017

What is Ethereum Classic (ETC)?

"The single most important moment in cryptocurrency history since the birth of Bitcoin."
— Gavin Wood, Co-Founder of Ethereum

In the early days of Ethereum, a hacker successfully stashed away $50 million worth of ether overnight, and almost got away with it. The fallout caused an ideological battle that divided the Ethereum community, and shook the cryptocurrency community. Would the community stick to the principle that "code is law," in the case of the hardened smart contracts that ran the ecosystem, or would they make an exception and return the stolen ether to its rightful owners?

The debate ended in a hard fork (or a spit in the underlying blockchain, similar to the Bitcoin/Bitcoin Cash fork mentioned earlier). The result created Ethereum blockchain splintering off, taking almost the entire community along with it, and leaving behind the original core code. The fork also reversed the transactions, and returned the stolen funds to the original accounts. But those that stuck true to their "code is law" ethos remained with the original core code, known today as Ethereum Classic (ETC).

Ethereum's evolution

The Ethereum ecosystem is built on smart contracts — that is, contracts written in computer code, that execute themselves according to the programmed parameters. When Ethereum was created, an organization that was called the DAO (decentralized autonomous organization) was built on the Ethereum blockchain. The idea was to create the DAO to operate like a company (but without the corporate structure) and provide some infrastructure so that other decentralized applications (dApps) could be built and launched. Projects would be added, voted on by DAO token holders, then funded. Within a month of the formation of the DAO, over $150 million had been added, which amounted to 14 percent of all ether at the time.

If DAO participants didn't like what was going on they were welcome to split off and create their own child DAO. Unfortunately, this created a massive loophole whereby a hacker was able to run an attack designed to exchange $50 million worth of DAO tokens and send it to an Ethereum address under his or her control.

The hack was immediately discovered, and the price of ether plummeted. But since DAO transactions required a 28-day waiting period before the transaction cleared, the community had time to debate the possible options about whether to hard for and reverse the transaction, or the let the transaction stand.

How does Ethereum Classic (ETC) work?

Ethereum Classic works just like Ethereum — it's built on proof-of-work mining and smart contracts, but it doesn't share compatibility or updates with the Ethereum (ETH) codebase.

This means that as Ethereum (ETH) transitions away from proof-of-work and into proof-of-stake, for example, these updates will not necessarily take place with ETC, unless the community develops them concurrently and independently.

ETC devotees claim there's nothing to stop Ethereum (ETH) from implementing another hard fork if some other hack or corruption happens in the future.

Monero (XMR)

At a glance

Launched: April 18, 2014
Origins: a fork of the CryptoNote protocol
Maximum supply: there is no maximum supply, but the current circulating supply is 16,124,276
All-time high: $467.50 on April 18, 2014

What is Monero (XMR)?

“Monero is cash for a connected world. It’s fast, private, and secure. With Monero, you are your own bank. You can spend safely, knowing that others cannot see your balances or track your activity.”
— getmonero.org

While ideological debates rage within communities like Ethereum, the Monero team is working on ways to “let the market decide” in a more decentralized manner. In order to do this, Monero is deploying some serious forward-thinking technology with the goal of creating a more robust, truly private cryptocurrency.

The private nature of Monero, means that it is more fungible than some other cryptocurrencies. By default, Monero is untraceable because the sending addresses, receiving address, and transaction amounts are all unreadable.

Besides privacy, Monero also has other features that are innovative for the crypto space. One interesting feature is dynamic scalability or the ability to change the block size as necessary to improve the network.

Monero is also supported by a grassroots community, and has seen its value rise steadily since it was launched in 2014.

Why is Monero (XMR) important?

Privacy-centric coins are important for many reasons beyond criminal activity, which is the use case that often dominates media coverage about privacy and cryptocurrencies.

Privacy coins provide benefits and peace of mind for ordinary, law-abiding citizens, that are simply lacking with other more publicly traceable cryptocurrencies, not to mention more traditional transactions. In recent years, banks, large corporations, and even governments themselves have had their records compromised.

While a few other cryptocurrencies such as Dash and Zcash come close, with options or privacy or features known as "selective transparency," Monero is inherently untraceable. With Dash, for example, the receiver can see some level of detail on who has sent them the payment. With Monero, the receiver has no access to or record of who sent them the transaction, only that they have received it.

Monero is also censorship-resistant, and truly decentralized. What this means is that if a news organization like WikiLeaks is viewed as dangerous or controversial by governments or financial institutions, a company like MasterCard can step in to stop facilitating the transaction of funds on their behalf because they disagree ideologically or politically with how the funds will be spent.

With censorship-resistant cryptocurrency, no central organization controls or monitors the flow of currency, and Monero is specifically designed to resist any form of control like this, even if the pressure was put upon the community to try.

How does Monero (XMR) work?

Monero is grassroots: open source, decentralized, and freely accessible to all. It's built on the contributions of the community, with a current team of 30 core developers, and 240 developers contributing to the project in total. The community features active forums and chat.

Like other cryptocurrencies, Monero uses a distributed peer-to-peer consensus network to record transactions on a blockchain. Participants who validate the transactions on the network work together to reach consensus and create the blockchain in an irreversible way once they have reached an agreement.

Unlike Bitcoin, Monero is dynamically scalable, which means that the block size is able to be adjusted over the course of time by the miners working on it, letting the market decide how many transactions should be contained in one block. As block size debates and lagging network speeds have plagued the Bitcoin community, it's valuable to understand what a block is, and what block size means.

In short, a block is a batch of transactions posted to the public ledger. To work efficiently, a certain block size was implemented into early on in Bitcoin to prevent malicious miners from spamming the network with huge blocks. The block spamming issue is accounted for in Monero by implementing a penalty for big blocks by reducing the reward for miners creating them.

There's a big debate in the Bitcoin community as to whether to increase the block size in order reduce the possibility for delayed confirmations because smaller blocks are filling up too quickly to handle the level of traffic coming in. The key thing to keep in mind here is that with Monero being "dynamically scalable," the market will be able to decide on things like block size, reducing the need for mass-consensus.

Monero is inherently private, with the wallet addresses themselves (the things that identify sender and receiver) never actually appearing on the blockchain. One way that Monero accomplishes this is by using stealth addresses to hide the receiver, ring signatures to hide the sender, and ring confidential transactions to hide transaction amounts.

In the case of stealth addresses, think of them as a "one-time public key" to unlock the transaction. It shows who can spend the funds later, and is only spendable by the proper recipient, but an outside observer cannot tell if funds are moving between people or be able to link the addresses together. The sender can verify if the payment was received by the receiver, but the payment cannot be traced back to the sender.

In the case of ring signatures, the source of the outputs is obfuscated, which means that the true sender is hidden. The transaction is signed by the true sender with the one-time public key, and is concurrently signed by a bunch of decoy senders.

Think of it as signing a check from a joint bank account with a number of your friends, where only one of the signers is the actual account holder, and the rest are decoys. If you take a look at the check, the true signer will be on there and the check will be valid if it needs to be verified with the right person, but to anyone who had intercepted the check, they wouldn't be able to tell who the actual account holder is.

Effectively, this hides the origin of the transaction. Ring confidential transactions are built out of this methodology, but function to hide the transaction amounts. Put together, Monero has built a solid way to hide the sender, the receiver, and the transaction amounts.

Qtum

At a glance

Launched: December 19, 2016
Origins: Qtum was developed as a proof-of-stake protocol that enables decentralized apps.
Maximum supply: 100,664,516
All-time high: $73.32 on December 18, 2017

What is Qtum?

Qtum ranks in the top 25 of cryptocurrencies and bills itself as the world's first blockchain made ready for business. A relatively new project with an initial coin offering (ICO) in March 2017, Qtum has made waves with meteoric growth in just over a year.

With a strong team, and strong backing, Qtum can be best thought of as a hybrid between Bitcoin and Ethereum, taking good parts from both, and creating a new and accessible place for businesses to launch distributed applications built on smart contracts.

Why is Qtum important?

Qtum features a strong team lead by Patrick Dai, who was recently acknowledged as one of China's "30 under 30" to watch, with other team members coming from prestigious and well-known Chinese tech companies such as Alibaba, Baidu, and Tencent. Beyond their ICO capital, they are backed by more traditional capital from established angel and private investors in China.

A rarity in the blockchain world, Qtum is also backward compatible with Ethereum contracts as well as Bitcoin gateways and will remain backward

compatible even after updates. This allows for easy platform adoption and a "plug and play" methodology that leans upon what other technologies in the space have done well.

Qtum is making a big push to create technology that is nimble and flexible enough to enable smart contracts on mobile devices and also plans to expand into IoT (internet of things) devices. Based in Singapore, Qtum is positioning itself to go address the Asian markets and even more specifically, the Chinese market.

How does Qtum work?

Qtum features a first-of-its-kind PoS (proof-of-stake) consensus protocol. This protocol achieves consensus through the agreement of computers on the network (nodes) to do the right thing, but Qtum promises something different, and more flexible.

In the future, Qtum promised to roll out iPoS (incentivized-proof-of-stake) mechanisms, which will reward participants. They claim to be the first cryptocurrency to bring together smart contracts from Ethereum, transaction models from Bitcoin, and proof-of-stake as means to maintain the blockchain.

Borrowing structural code from both Bitcoin's transaction model and Ethereum's virtual machines and smart contracts has served Qtum well thus far. Bitcoin's UTXO (unspent transaction output) model and SPV (simple payments verifications) protocol are rolled into the build, which means that transactions can occur in a simple, lightweight format. The setup also allows smart contracts on mobile devices through lite wallets, and features such as QR code-based transfers like Bitcoin, when moving funds from address to address.

The smart contracts aspect itself involves (from the Qtum website) a "*formally verifiable translation of human-readable agreements to machine smart contracts, and the error-resilient specifications of their elements, terms and conditions.*" What makes smart contracts so powerful is that they eliminate

human error, are unable to be changed, and they are self-executing.

These are contracts built in code and in the case of Qtum they can be translated into terms that both humans and machines can read. The greater the accessibility, the larger the potential market size, and the more powerful the network.

Qtum is innovating rapidly on what others have done well, and rolling these features out together in a new, polished, and powerful package.

NEO

At a glance

Launched: February 2014
Origins: a decentralized blockchain designed to support decentralized apps. Previously known as Antshares
Maximum supply: 100,000,000
All-time high: 196.85 on January 15, 2018

What is NEO?

"NEO is a nonprofit community-based blockchain project that utilizes blockchain technology and digital identity to digitize assets, to automate the management of digital assets using smart contracts, and to realize a "smart economy" with a distributed network."
— neo.org

Started by a blockchain research company called Onchain in 2014, the project originally called Antshares was rebranded as NEO in 2017. NEO has been labeled the "Chinese Ethereum," or at times the "Ethereum killer," and like it's competition, focuses on digital assets, the verification of digital identities, and smart contracts (contracts built from code that execute and run themselves with rules on how funds can be transferred). Calling itself a distributed smart economy network, NEO runs on GAS in the same way that Ethereum runs on ether. That is to say, a separate token known as gas is needed to run smart contracts, depending on the computing power used. Coded in common programming languages, there's no need to learn special coding skills such as those required to write Ethereum projects, which are developed using the Solidity language.

NEO consistently ranks near the top ten of cryptocurrencies by market cap.

Why is NEO important?

One of NEO's biggest design features is accessibility because NEO projects can be coded in common programming languages such as C#, Python, and Java. This opens many doors to new developments within the ecosystem, with lower barriers to entry, and a more inclusive approach to collaboration on the project platform. This is important to any cryptocurrency platform allowing ICO's, such as NEO, Ethereum, and Stellar, where other projects can release their own cryptocurrency on the underlying blockchain built by NEO.

With connections to both Chinese tech giant Alibaba, as well as potential good standing with a skeptical Chinese government, NEO is poised to address the Chinese market. It also features partnerships with Agrello, Bancor, and Coindash. The team behind NEO is also working with Fadada and Microsoft to collaborate on a project called Legal Chain, seeking to modernize and address the shortcomings of the legal system through digital applications.

NEO doesn't allow forks and instead makes use of a special consensus mechanism known as dBFT (Delegated Byzantine Fault Tolerance). Transaction volume is another key component of NEO — up to 10,000 transactions per second are possible.

NEO also has some future-proofing baked into its core components. More specifically, the blockchain is being developed to be "quantum resistant," which will become increasingly important as quantum computers are developed that may be fast enough to crack the encryption.

How does NEO work?

As mentioned earlier, NEO runs on GAS, the companion cryptocurrency required to compensate participants for the computing power necessary to execute activities on the network. Eventually, 100 million GAS will exist, which unlike NEO, can be subdivided into smaller units. Consensus nodes known as "bookkeepers" validate transactions on the network in reward for GAS. Stakeholders — people who hold NEO — get GAS in return for holding on to NEO and their participation in the network. Each NEO holder gets a vote,

based on ownership amounts, on what happens in the NEO ecosystem — if stakeholders don't like what a consensus node is doing, for example, they can vote to remove the authority of that node, taking it off the network and out of the ecosystem. Using this method, NEO has built a thriving community based on participation.

Technically speaking, NEO developers are tackling several problems at once, while providing a number of features. Different types of digital assets can be registered, transferred, and traded on the NEO platform. Digital certificates offer full legal protection of assets and they can bet can be exchanged peer-to-peer, without needing an intermediary or third party exchange to facilitate trade. What are known as "Turing-complete" smart contracts enable the platform the possibility to solve just about any computational problem. Blockchain-based platforms like NEO and Ethereum have designed a way for the "world's computer" to function, distributing computing power to potentially solve the world's biggest problems.

Like Ethereum, NEO features virtual machines — a virtual computer composed of software instead of physical parts — in this case, known as NeoVM (NEO Virtual Machine). These virtual machines feature shorter startup times, efficient execution, and unlimited theoretical scalability, all made possible by the dBFT (Delegated Byzantine Fault Tolerance) which is basically just a mechanism through which the network is able to reach consensus and ensure finality of transactions.

Some of the other features that the NEO community are actively working on include: NeoFS for decentralized file storage, NeoX provides for transactions and smart contracts that can cross blockchains, and NeoQ offers the encryption we mentioned earlier that can't be solved by quantum computers.

Zcash (ZEC)

At a glance

Launched: October 28, 2016
Origins: a privacy-focused public blockchain that operates similarly to Bitcoin.
Maximum supply: 21 million
All-time high: $5,941.80 on October 29, 2016

What is Zcash (ZEC)?

"Bitcoin and most cryptocurrencies expose your entire payment history to the public. Zcash is the first open, permissionless cryptocurrency that can fully protect the privacy of transactions using zero-knowledge cryptography."
— z.cash

Zcash is building an open, permissionless cryptocurrency designed to tackle privacy in a slightly different way than some of the other cryptocurrencies mentioned.

Zcash can be thought of as a fork of Bitcoin, focusing on privacy, anonymity, and fungibility. With a circulating supply of just under 4 million, Zcash was founded in 2016 and will have a total supply of 21 million coins. Founded by Zooko Wilcox of ZECC (Zerocoin Electric Coin Company), Zcash is an open source project run by a private organization. With an initial investment of $1 million, its early investors will receive 10 percent of the total supply over the first four years, known as the "founders" reward.

Zcash has seen some absolutely wild price action in its short existence thus far, seeing a price of $3000 per coin in the first week, crashing to $50, and at one point hitting an all-time high of $5941.80.

Why is Zcash (ZEC) important?

Zcash is important because Bitcoin lacks some privacy controls. Consider the

following: With Bitcoin you have the sender's address, the receiver's address, and the amount transferred visible with every transaction. This is potentially problematic because let's say you purchase an everyday item at a cafe — the restaurant will see your sender address, be able to look up your wallet on the public ledger, then be able to find the amounts of all payments you've sent and received. All this information is publicly available on the Bitcoin ledger, permanently recorded in the blockchain in a way that can never be altered. Great for verification that these digital funds have not been spent twice, but not so great for privacy.

Zcash addresses this problem by making all aspects of the transaction completely anonymous, private, and built upon strong encryption. This is possible using a system of zero-knowledge proofs called zkSNARKs.

Zcash has caught the attention of huge players such as JP Morgan, even establishing a partnership with the firm in their development of the enterprise-scale blockchain known as Quorum. JP Morgan may find such a system appealing in the case of wanting to secure their trades from the eyes of competitors, or in diligence required to protect data. As far as partnerships within the cryptocurrency world go, this one is a big deal.

How does Zcash (ZEC) work?

Without having to understand the advanced cryptography involved with the magic of zero-knowledge proofs, one key takeaway is that Zcash functions in a very similar manner to Bitcoin, but adds a layer of privacy that is built on a layer of strong encryption. Payments are concealed because the sender, receiver, and amounts are obscured, ensuring that privacy and anonymity remain a top priority.

In short, this protocol means that someone is able to prove that certain information is in someone's possession, without actually revealing that information. It's able to prove that the encrypted data and transactions are legitimate, without revealing what this data is, who the actual owners are, or what amounts are being spent. Effectively it can verify that someone has funds, it has never been spent, and that it's been moved to someone else — exactly what we need to establish a more private version of Bitcoin.

Next steps: Abra and altcoins

Abra as an altcoin exchange, wallet, and investment platform

Specialized cryptocurrency exchanges provide the first entry point for people looking to get into Bitcoin and altcoin markets. There are a lot of different types of exchanges, and it seems like more are being added every week.

Abra is a unique exchange for a few different reasons. One of its biggest advantages is that users can find 25 different cryptocurrencies (including all of the ones mentioned in the guide above) and 50 fiat currencies on the platform. Rather than creating multiple wallets to support each altcoin, Abra users only really need to keep track of one wallet and still be able to access multiple assets.

The reason this is possible is that Abra leverages blockchain and cryptocurrency technology to create synthetic currencies. In other words, the values of altcoins or fiat currencies are pegged to Bitcoin, and as those values grow or shrink so does the corresponding value in a user's wallet. This allows users to move quickly and efficiently across multiple digital assets.

Many users also report that Abra's clean design and easy interface makes exchanging between traditional currencies and cryptocurrencies easy and straightforward. Abra can be funded by an American Express, wire transfers, or by bank accounts in the United States and the Philippines. Abra users can also use Bitcoin and Litecoin to transfer funds into the wallet (with more native support for other cryptocurrencies coming soon).

Besides the ease of use, security is another advantage of using Abra as a cryptocurrency exchange and wallet. One of the main security risks for most other exchanges is that they are custodial, or basically like traditional banks in terms of control. Abra, on the other hand, is a non-custodial system, or self-custodial, which means that users never give up access to their assets. The trade-off for this more secure arrangement is that users have to take more responsibility for maintaining their private key, which is what will give them access to their wallet on the blockchain.

Abra as an altcoin gateway

Cryptocurrencies and blockchain are revolutionary technologies that are growing in popularity and value. Abra takes the best of blockchain technology and combines it with straightforward design in order to enable a better cryptocurrency exchange and wallet experience.

This guide was created for informational purposes only. It is not intended as financial advice.