The current cryptocurrency environment

- The current state of cryptocurrencies has a Wild West feel to it. A high number of people and organizations are jumping in to get a piece of the action. It's chaotic, it's risky, it's exciting, and it's rapidly changing. In barely nine years since the original cryptocurrency, Bitcoin emerged, many hundreds of alternative digital currencies have surfaced. People are using these altcoins, or cryptos, as they're often known, to buy and sell all types of products and services. These cryptos are also being used simply as investment instruments, where people try to buy low and sell high. Cryptocurrency has also enabled a completely new form of raising capital, called an Initial Coin Offering, or ICO. It's giving startups, in particular, a way to raise enormous amounts of cash that would be typically more difficult via traditional fundraising. Cryptocurrencies are challenging financial institutions and governments all over the world. Cryptos are disruptive to the status quo. Financial institutions must figure out how to work with them as ignoring them is no longer possible. Big players like Barclays, Credit Suisse, and many more are exploring integrating and supporting cryptocurrencies and their underlying blockchain technology into operations, products, and services. Governments are struggling to figure out the right regulation without stifling innovation, but at the same time, protecting markets and individuals. The race is on and the outcome is uncertain. China and South Korea, for example, have gone as far as banning ICOs. China was rumored to be looking at outlawing mining or limiting cryptocurrency mining. Some countries are exploring creating their own national cryptocurrencies, such as Turkey, Israel, Sweden, and Ecuador. And while this seems counter to the decentralized model of crypto, the details are yet to be seen. The code that runs Bitcoin, which is free for anyone to copy and use, has given birth to hundreds of old coins. As we'll see in a later video, anyone of us can create our own digital currency with a modified copy of Bitcoin software. While Bitcoin continues to dominate as the most popular and respected of the global cryptocurrencies, there is a massive long tail. Several others dominate and hundreds more wait patiently to merge or die in a noisy and unpredictable marketplace. Among the most popular today include Ethereum, Ripple, Bitcoin Cash, which is different to Bitcoin, Litecoin, Stellar, IOTA, Dash, Monero and Zcash. We can anticipate that this list will

change a lot in the months ahead. The underlying technology called blockchain that enables most cryptocurrencies to function, is being used in a massive number of other uses, spanning almost every domain in our economies. Blockchain technology is being used for supply management, identity management, in government for records management, in mature pilot experiments using the Internet of Things. And with Ethereum, for example, to power a whole new category of applications called distributed apps or DApps. As we'll discuss later, cryptocurrencies have engaged a large new community of hobbyists and professionals. It's also inspired a significant criminal element which use cryptos in all manner of activity, both across the public internet and in the more sinister, hard-to-reach corners of the dark web. Law enforcement is on it, but the evolving nature of the technology combined with the anonymity of crypto is creating significant challenges. Additionally, the cryptocurrency world is not without its share of hacking and fraud to add to the security concerns. The current state of cryptocurrencies and the rapid rate of change make it a compelling space to explore. Sure, the risks are significant, but so is the upside. Knowledge is essential, particularly if you're thinking of using cryptocurrency, investing in it, or creating a business with it. And it will be really important to keep up with it, as I anticipate it's gonna change rapidly in the months and years ahead.

The birth of bitcoin

- If you're relatively new to the subject of cryptocurrency and have read and heard about it through different media channels, you may be curious about the differences between the terms blockchain, Bitcoin, and cryptocurrency. I think it can be easy to believe that they are just the same way of saying the same thing but with different terms. I'd like to clear that up right now. Blockchain technology is the technology that enables most cryptocurrencies to work. It's the really techie stuff that functions behind the scenes. It's a unique form of database that stores and facilitates transaction information made with digital money. Most cryptocurrencies have their own blockchain database with their own set of rules. As you can probably now guess, Bitcoin runs on top of its own blockchain. In this course, we are focusing on cryptocurrencies like Bitcoin and others, called old coins, and not on the underlying blockchain technology. However, I'll provide a light

description of blockchain in this video because I think it's useful to put cryptocurrency concepts in perspective. Okay, so what is blockchain technology? A blockchain is a database. It's used to store certain types of data. It's unlike most databases that have come before it in that it has specific qualities. Two of those are at the core of what makes it unique and powerful. It's a distributed database and its entries are immutable. In other words, it doesn't sit on one all-powerful server and the data stored in it, once it's written, can not be deleted. But before I go too deep into this, let's quickly recap traditional databases. In a traditional structured database, data is stored in columns and rows in multiple tables, usually a table stores related data. For example, a table might contain a person's name and address. It will also contain a unique key, called a primary key, for each row that can be used to connect one table to another. In a billing system, for example, another table might contain invoice information for a purchase, the address of the buyer will likely be referenced via a primary key. Databases have become very sophisticated and can have complex logic built into them. In a client-server architecture, the database lives on a single logical server. Data is queried from the client, presented as a request to the server, which then runs the query and produces a result for the client. In web-based architectures, there are often at least three tiers, the web client, the web server, and the database. Much like client-server, both the web server and database server are centralized, often workload is distributed among many physical servers. In this way they could be said to be distributed, but logically they're governed by central rules. As a result of phenomena such as social media and massive disparate data sources, databases are increasingly unstructured in design. While techniques such as natural language processing and text analytics help to manage the data, the overall physical database architecture is largely the same. This type of setup is hierarchical and relies on central management. Somewhere in the environment is a set of rules in which on who can use the database and what rights each user has. It's served the world well and continues to be the dominant model for data management. What makes this database architecture useful and powerful also makes it vulnerable. Anyone with the right credentials can access and there are too many ways to hack the system as many high-profile cases have demonstrated over the past few years. Massive credit card thefts

from the likes of Home Depot, Target, and Nieman Marcus are all too common. A blockchain database is structured in the sense that it contains specific blocks of data, organized in a particular way. However, there is a big difference in how the database is hosted. Unlike in a traditional database environment, a copy of the blockchain database resides in every computer that participates in a given blockchain. For example, all Bitcoin users will have a full copy of the Bitcoin blockchain database on their computing device. There is not central server. It is not hierarchical. In fact, we call it peer to peer, since the architecture is flat. In a simplified description, when a person first joins a blockchain-based environment, the full database is downloaded to their device. Next, as each transaction takes place in the blockchain, say Bitcoin currency is sent from one person to another, each transaction is recorded in every instance of the blockchain database. In this way it is said to be a distributed database. In fact, there is an industry preference to refer to the database as a distributed ledger. Unlike a traditional database, for a transaction to be processed and inserted into the blockchain ledger, consensus must be reached by all the participating devices. We'll discuss this idea in detail in a later video. Despite some recent well-known security failures, it's anticipated that blockchain technology will eventually be extremely well secured. One of the reasons is because it uses a type of security that requires special paired digital keys. A user of a blockchain has two keys, a private key and a public key. The private is only ever known to the user. Its paired public key, however, can be known by everyone and can be considered the address of the user for sending money within a blockchain. To protect the transaction, only the user with the private key can be associated with and unlock any transaction sent to their public key address. This works using a technology called cryptography. This explains why we refer to digital currency as cryptocurrency, or crypto.

How blockchain technology powers cryptocurrency

- Now that you have a basic understanding of blockchain technology, it's time to talk about its origin. Remarkably, the actual programmer or programmers behind Bitcoin are still unknown. We do know that Bitcoin first appeared in January 2009 as open source software. This is a type of software license which allows anyone to inspect, modify, and enhance the

software. The Bitcoin software enabled currency in a digital format to be used without any intermediaries or governing authority. This means that currency could pass from person to person without the need for a bank or any other financial intermediary. In this way, it's the opposite of all other forms of typical currency we know and use. Some say Bitcoin was developed as a response to the Great Recession of the late 2000s. Its inventors wanted to conceive of a new monetary system that did not rely on the whims of a few large banks. As a currency, it does not exist in physical form. There are no coins or notes. It lives natively on the internet. When a transaction takes place, participants who use Bitcoin, their computer specifically, validate the transaction, and it is recorded in a distributed ledger that is powered by blockchain technology. Now you're probably wondering, how can a digital currency possibly have value? Let's discuss this. To have value, typically something must be relatively scarce and it must be accepted by others for payment. Gold, silver, diamonds, and oil, for example, all derive their value from being both scarce and expensive to mine. How might this translate to a digital currency? The first characteristic is that there is only a limited amount of Bitcoins available. The original creators stipulated that there would only be ever 21 million Bitcoins. The second characteristic is how a person or organization can acquire a Bitcoin. Like gold, acquiring a completely new Bitcoin requires a unique type of mining. New Bitcoins are periodically released to the Bitcoin participant network and can be acquired by solving extremely complex mathematical puzzles. These puzzles take considerable computing power, so access to participate is limited. The computing power requires a lot of computers and a lot of power. This incurs a cost to miners. Much like those mining oil in the wild ocean, only those with exceptional resources can participate to have a positive cash flow. The value thereafter is calculated similar to any currency, by supply and demand. In simple terms, if demand for Bitcoin is high, its value increases. Less demand, price drops. Can Bitcoin be used to buy anything? Certainly, all manner of organizations, including many big and small retailers, accept Bitcoin. Wide acceptance has been foundational to its success. Bitcoin is certainly not perfect, and it's largely considered a work in progress. The software is still developing and maturing. Issues and risks are still being addressed, including, for example, the recent discovery of web links being

written to its blockchain that link to illegal web pages. That said, Bitcoin has inspired a massive industry of competitor cryptocurrencies, called Altcoins. You may already be familiar with some of them, such as Ether, Peercoin, Litecoin, and Ripple. There are hundreds more. The success of Bitcoin, powered by blockchain technology, has given birth to a whole new way of creating and using money. The cryptocurrency industry, still largely in its infancy, seems well-suited for the needs and expectations of the 21st century. But it's early, there still remain a lot of challenges and risks ahead. If you'd like to learn more about Bitcoin specifically and get much deeper into its details, I recommend watching Tom Geller's Learning Bitcoin course.

Methods of cryptocurrency creation

- When you hear or read about crypto I'll bet it takes the form of bitcoin or Ether from the popular Ethereum blockchain. Perhaps Ripple, Litecoin, Peercoin, Dogecoin, and a few others. Each of these have enjoyed considerable success in different ways as viable forms of digital money. Each of them have seen their value rise significantly, and sure, sometimes drop. But still they are largely retaining value, at least for now. Although these are among the most popular and thus most frequently cited, there is currently a long tail of well over 1000 other cryptocurrencies. The term alt coin is used to describe all these cryptos as a way to note them as alternatives to bitcoin. What's the reason for so many cryptocurrencies? Right now we're in a period of significant crypto chaos. It's the wild west. There is little law and order and everyone is vying for a piece of the action. There are good guys and bad guys. It's equal measures scary and exciting. Every action carries enormous risk. In this wild west anyone who wants to can spin up their own currency with their own set of rules. This includes you and me. Why wouldn't you want your own youcoin. Imagine the bragging rights. Imagine the power. Your coin could emerge as a favorite, bringing you fame and fortune. You could become part of a historical shift from government-backed currencies. Fiat currencies like the dollar and Euro to a dominant digital money economy. First you'd call it anything you want. For me, perhaps, rickentelcoin. Then you would define the rules and monetary policy for the currency. For example, you might have a cap on the total number of coins that could be issued. Next you may want your coins to be used for a specific

use. For example, GENERcoin is used in support of the renewable energy sector. Perhaps you might want to have your coin use an alternative proof of work and consensus mechanism. After all, it's your cryptocurrency. You get to make the rules at the beginning. You could use your crypto to raise money for a new business idea. That's called an Initial Coin Offering, or ICO, and it's something we'll discuss in detail later. I'm guessing you'll use your coin with good intentions. But not everyone will. There are plenty of scammers out there. In this crypto wild west there are a lot of bad people in town. In the absence of any regulatory oversight and in a climate of irrational exuberance over crypto, people are hastily throwing money at unsubstantiated cryptos. If you buy a scam crypto, there's no recourse. You've lost your money. The crypto wild west is an unpredictable and risky place, but it won't always be that way. In time the market will likely stabilize. Let's look at a few examples of alt coins and their use. The ripple blockchain uses an alt coin called XRP that powers its cross-border payment system. This is an innovative solution for moving money more quickly between countries. If you've ever done this the traditional way, you'll know that it can take a few days, unless you're prepared to pay a substantial service fee. Another example is Ether. This is the cryptocurrency generated on the Ethereum blockchain. A really successful platform for writing smart contracts, software programs that run on blockchain technology without any need for a centralized software development platform. Others include Zcash, similar to bitcoin, but with a focus on transaction privacy. Litecoin, almost identical to bitcoin but with a faster transactional confirmation process. Every two and a half minutes versus 10 minutes with bitcoin. And our last example, IOTA, a cryptocurrency developed specifically to help enable innovation in the internet of things. If you want to learn a lot more about other alt coins and their specialty, check out coinmarketcap.com. Let's return to the topic of how you might now create your own cryptocurrency. There is the harder way but one that provides you with maximum control. And then there are out-of-box options that make it easier but provide you less flexibility. The harder way, which I guess is subjective, is to copy the existing code that powers bitcoin. Yes, you heard me right, copy the existing bitcoin code. It's called forking, or specifically a software fork. It's perfectly legal and supported. Bitcoin is open source. It's free for anyone to copy and

modify. Hundreds of today's cryptocurrencies were created this way. If you'd like to get your hands on a copy, it's available from several sources. As an example, you can get it from the software repository GitHub right here. Once you spin off your own copy of the bitcoin source code, to make any modifications will require you to have programming skills. Changes to the source code requires knowledge in C++. This requirement will certainly limit the number of people who can go this route. However, as you can imagine, there is an ecosystem of providers who can do the specific work for you for a price. Let's look at the easy way but less flexible way of creating your own crypto. For this you'll use one of the many out-of-box, often Wizard driven, solutions available online. As an example you can take a look at Wallet Builders. This service provides a free version that lets you create a cryptocoin as a test service. To get some experience, you might consider giving that a try. However, in order to go live with your crypto, they do have a fee structure. Other services include CryptoLife and Coin Creator. You can also check out the Waves Platform. These services tend to be less flexible because you are limited to the capabilities they offer. If you want to find a happy medium between the best but more complex option of programming in the bitcoin code and the commercial Wizard driven solutions, another option is to use the Ethereum blockchain to create your crypto. You'll need some deeper technical skills, but there are some great support tools available. You could learn more here. Realizing that creating your own cryptocurrency is a real possibility can be eye opening. But the technical work of creating crypto is by far the easiest part. Maintaining and sustaining a tradable digital currency is exceptionally difficult and most will fail.

The challenges of succeeding with cryptocurrency

- It's worth noting the remarkable fact that today, anyone with an internet connection can create a bonafide digital currency. It speaks to the low entry barriers that the digital revolution is enabling for all manner of capabilities. From spinning up an e-commerce store over a weekend, to easily coordinating global events online. There are many reasons why a person or organization may want to create a cryptocurrency, and we discussed several in the last video. What will become clear quickly is that

creating a cryptocurrency is the easiest part of having a successful cryptocoin. Most will fail. So the question becomes, what are some of the things we must do, and things that must go right to have a chance of success? The first thing to recognize is that creating and nurturing a cryptocurrency is a longterm endeavor. For some the first pass at creating the code might just take a day. However, we'll assume that we want to create our own parameters. For example, how much currency will be available? Will it be capped or unlimited? Will we use proof of work or some other consensus mechanism? Do we want more or less privacy around transactions? Is it a public cryptocurrency, or do we want to define it for certain usage, say within an organization or industry? These are some high level business decisions, but there are also a whole host of technical parameters we may want to define too, such as the hashing algorithm, or block size. In addition, despite promoting the security benefits of the underlying blockchain technology, security remains an issue with cryptocurrencies. Constant effort is required to fend off hackers and shore up vulnerabilities. All of these choices mean that coding is required, and ongoing maintenance of the code will be needed. And of course modifications of the code won't stop there. There will be a need to add or remove features as time passes, in response to community needs, security issues, and other challenges, such as scalability. Understanding the longterm commitment and attendant expenses, the need to foster a community of developers, and the challenges of meeting all requirements, must not be understated. The next hurdle, and not a trivial one at all, is to make both miners and users aware of your cryptocurrency. We're talking marketing here. How do you bring attention to your money, when there's so much competition and crypto marketplace noise? Cryptocurrencies like Ether, Litecoin, and Zcash have done a great job of creating and fostering a variety of communities. These include communities of interest, meetups, significant social media footprints, events, blogger pickups, and online forum participation. This creates enthusiasts who further champion and promote a new coin, particularly when it is observed that the founders are motivated, deliberate, and committed to the longterm. There is strategy here, and sure, an element of luck. If you have to sequence this, put effort into getting your mining community established first. Miners create energy and momentum and will help build crypto coin

credibility. Users, effectively the buyers of the currency, will build as volume of currency increases and price follows. Additional communities that will be essential within a short period, will include merchants and exchanges. Depending on the strategy, you might decide to work on having a particular merchant accept your currency. Unless you have a good friend who owns a business and is prepared to make a bet on you, or you have an incredible network that gets you the same result, this won't be easy at all. Litecoin, for example, has been successful in getting considerable retailer support as you can see here. A good strategy, good timing, and some good luck really helps. The same can be said for exchanges. That's really the holy grail. If your cryptocurrency can be bought, sold, and exchanged for other cryptocurrency, or fiat currency, you've hit the jackpot. Many of the most reputable crypto exchanges only support a small number of cryptocurrencies, but this is changing too, as the market matures and public participation greatly increases. Finally, success with a cryptocurrency may lie with intent. If we return to basics for a moment, we have to remind ourselves that the fundamental purpose of money is to acquire products and services. A compelling cryptocurrency offers people an alternative form of money for the digital age. Something that enables them to, for example, spend with anonymity, or avoid financial fees, or to complete international transactions quickly, or maybe all of these and more. However, if we only view our cryptocurrency as a tradable asset class, where the intent is to simply make money from changes in its value, this can undermine its credibility and quickly limit its potential. A cryptocurrency with tight integration, with exchanges and merchants, where brokers and other stakeholders view it as a credible mechanism for the exchange of value, will have a greater chance of success. Making money in speculation has a place, but it's becoming the domain of dubious get-rich schemes and scammers in cryptocurrency. The evidence is getting clearer that these cryptocurrencies have little chance of longterm success.

What is an initial coin offering (ICO)?

An organization has several ways to raise money. Startups are particularly constrained because traditional financial institutions are typically reluctant to invest in new companies that are unproven and with little collateral. Instead,

startups can raise money through their own savings, through family and friends, and, if they are lucky, from investors. Established organizations can raise capital through traditional financial services and by having an initial public offering, where they sell shares of the enterprise to investors. With the emergence of blockchain technology and cryptocurrencies, a new form of raising capital has emerged. Called an Initial Coin Offering, or ICO, this process enables a startup to sell a predetermined number of tokens or a new cryptocurrency, if the startup is offering that, to investors. The investor typically purchases with cryptocurrency, such as Bitcoin or Ethereum. In some instance, cash is used, too. The investor isn't buying a share of the startup, but instead is relying on the value of the token or cryptocurrency to increase as it is traded through specific exchanges indefinitely after the sale ends. The first ICO was held in 2013 and, as of late 2017, there were as many as 50 new ICOs being issued per month. These ICOs have been generating enormous amounts of money in record time. An ICO called Filecoin raised $200 million within its first hour. How do we know what ICOs are available? There are many websites now supporting the initial offerings, as well as the subsequent trading, once the ICO is closed and the business has been launched. These include Coinschedule, ICO Alert, and TokenLot. Token exchanges include NEXT.exchange and TokenDesk. There are few restrictions on who can buy into an ICO. Since the startup is taking money from a global audience of investors, the amount raised can be large. A risk with ICOs is that they are raising money pre-product. It makes the investment highly speculative. There is significant debate on whether and how ICOs should be regulated. As of early 2018, both China and South Korea have banned ICOs. All countries are evaluating this sudden new model, and the future of ICOs remain fluid. The U.S. Securities and Exchange Commission, the SEC, which is tasked with protecting the country's investors, do not offer any oversight for ICOs at this time. They have issued alerts and consider ICOs exceptionally risky investments. The question on the SEC's role depends on whether the token being offered represents an actual security. A security is broadly defined as an instrument of investment in the form of a document, such as a stock certificate or bond, providing evidence of ownership. If so, then the rules of the SEC kick in. Without getting too deep into this, to determine whether cryptocurrency or token can be considered

security requires something called the Howey Test. The basic concept of the test is whether the answer to these two questions is yes or no. Is there an expectation that the purchased token will make money for the investor? And second, do the management of the enterprise providing the token work to make its value increase? While certainly not comprehensive, this is the basic concept. If the answer is yes to both, then it's a security. The conclusion is that a cryptocurrency and a token issued in an ICO could be a security, but it's not definite. If it's deemed to be a security, there are a lot of obligations from the seller that must be met, otherwise the legal consequences are significant. It's my opinion that this area will heat up in the months ahead, as cryptocurrencies, tokens, and ICOs mature and more of the population begins to participate. Another trigger will be when traditional investment brokers begin to make these new digital products and services mainstream offerings. Finally, the SEC has indicated that it is supportive of ICOs, so they plan to see how they can play the right role. In other words, unlike many other countries, U.S. doesn't want to seek a way to ban them. Moreover, it wants to find a way to appropriately regulate them to protect investors. So where does that leave us with ICOs? On the one hand, they represent an incredible way for startups, in particular, to quickly raise a lot of money. That's important, because great ideas need funding. It's giving entrepreneurs more options and confidence, and generally that's a good thing for an economy. There are legitimate ICO successes, both for the startup and investor. Some examples include NXT, IOTA, Ethereum, NEO, and Stratis. On the other hand, making it too easy attracts bad ideas with good marketing and scammers. Both will make your money disappear quickly. In addition, without any protection from the SEC or any other governing or enforcement authority, the risks of an ICO, particularly to the investor, are exceptionally high. I'm a pessimistic about ICOs, as I think the model has an opportunity to mature in the months and years ahead. But right now, there's certainly a fair amount of unpredictability.

The mining process

- Cryptocurrencies exist at a fairly high level of obstruction. For example, there's no underlying supporting role material such as silver or gold. There's no centralized management. And as of now, no federal government backing and limited regulation. And yet it works as a currency. Fundamental

to any currency is the confidence of the user in its use. For example, we have confidence in fiat currency, that is government-backed currency because it carries the full faith and credit of a national government. In cryptocurrencies, for the most part, it is miners and the mining process that provides confidence in their legitimacy. Probably the most important question in cryptocurrency transaction is, does the payer, the person giving money, have a cryptocurrency available to make the payment. In a traditional centralized system, the bank will manage this. If someone tries to write a check for an amount they don't have, eventually the transaction will fail. How can this be achieved in cryptocurrency? We've seen in an earlier video that cryptocurrencies run on a blockchain. This blockchain technology basically a type of database, is stored in its entirety on each participant's computer. When one use in this blockchain wants to pay another user, a process of consensus must be met by all participants to allow the transaction. This is at the heart of the magic that blockchain creates. If consensus is not reached, that is participant computers don't agree that the transaction is legitimate, then it can't take place. Consensus is the governance in the decentralized model that replaces the bank in the centralized model. We can say then that mining is the process that enable consensus. I'll keep the description of the mining process here relatively simple. Alice wants to pay Bob with cryptocurrency. Bob's address is known to Alice. It's his public key. In this example, we'll say Alice wants to send five bitcoins. Her transaction is first broadcast to the bitcoin blockchain signed with her private key. Her private key associates Alice with the bitcoins that she owns. Now when she broadcasts her transaction, special users called miners are waiting to receive the transaction request. Miners act to validate transactions and pass this information on to more users of the bitcoin blockchain, so they can also confirm the transaction. This is the consensus process. Miners are incentivized to do this work because they receive compensation, a tiny amount of bitcoin in this case. But is the work that they are doing? First, miners validate Alice has the five bitcoins. They do this by checking her sign transaction with the bitcoins associated with her. Then using information in the transaction request, a miner's computer's processing power is used to solve a complex mathematical problem. This problem will take some input data from the transaction and must transpose

it to a predetermined output or target using a special algorithm. It's the stuff that computers are really good at. Computers can cycle through enormous volumes of guesses at rapid speed until a target is reached. The first miner to solve the problem is awarded the bitcoins. That miner then broadcasts a solution to the bitcoin blockchain. That's what's called proof of work, which is further validated to be correct, then finally to all participants of the blockchain where consensus is reached and the new transaction is approved and added as a block to the blockchain. It all sounds terribly complex, but it solves a few important challenges. First it solves what's called the double spend problem. We don't want Alice exploiting a time window in the transaction to spend money that she has already committed. As a basic example, if Alice only has five bitcoins, we don't want her to give five to Bob and at the same time give five to Stephanie. Proof of work creates rigor to every request and a fake second spend would be caught and rejected during or just after the first request. The second important reason for the proof of work process is to create the immutability of the blockchain. You'll recall that the mathematical problem that the miner solves uses input from the proposed transaction to create a new output. Each subsequent transaction uses parts of this new output as an input to the next output. In other words, every new transaction is dependent on every single previous transaction in the blockchain. Since proof of work is required for a new transaction, and this is a rigorous process of both mathematics, time and computing processing power, to change a previous transaction, say to falsify a record such as faking a bitcoin amount associated with a user, would require all subsequent transactions to be recreated too. The energy and cost to do this is effectively restrictive. Without leaps in processing capability, which could happen in some distant future, it becomes impossible to change prior records. This is how immutability is achieved. While all this seems complicated and convoluted, let's return to some basics. Mining is valuable because it enables cryptocurrency to function. But it's also lucrative for the miner. If your computer can solve lots of the mathematical problems you'll be awarded cryptocurrency. You're creating money using the processing capabilities of your computer. Returning to bitcoin, in its early days beginning in 2009, there weren't many bitcoin miners. So lots of them accumulated bitcoin rewards. At the time, they were not worth much at

all. Over time though bitcoin began to rise in value and more miners participated. Responding to the higher volume of miners, the bitcoin software increased the complexity of the mathematical problems. In fact, the software is designed to adjust based on miner participation. More complexity meant that miners needed more computing power. Instead of just one personal computer, they would need better hardware. Now the entry barriers were increasing. Anyone could still participate, but only those with a lot of computing power were likely to quickly solve an increasingly difficult new mathematical problem. And thus earn new bitcoin rewards.

Choosing the right hardware and software

- Technically anyone with a computer connected to the internet can engage in cryptocurrency mining. Particularly in the first years of Bitcoin, very few could have predicted the significant increase of value. That said, the value of Bitcoin is a rather fickle proposition. Ultimately its value it's determined by the confidence that after you buy Bitcoin, you're able to sell it to someone else at a higher price than what you bought it for. Any number of factors can impact its rise or fall. For example, a major retailer or economic sector showing support can raise value whereas the imposition of a government regulation could lead to a significant fall in value. Over the past few years, the price of popular cryptocurrencies such as Bitcoin, Ether, Litecoin, and Peercoin have all generally trended upward. For this reason, buying these currencies with the intend to simply sell later, to realize a profit, is popular. It is also an area of debate and contention since far too many are using cryptos for this purpose. And not as many to buy products and services. One argument says that if the preponderance of the use is for buying and selling for profit, then sustainability as a currency may not be maintained. As a cryptocurrency gets more popular and more miners participate, the computer processor and power requirements increase. This is because the complexity of the mathematical problem to solve increases relative to the number of miners engaged. With the significant popularity of Bitcoin, the computing power now required to have a chance to be a winning miner has grown. It's now close to impossible to succeed by simply using a regular home computer. The basic calculation that is required is that the money that can be earned from mining must be higher than the combined cost of purchasing

hardware, maintenance and paying for ongoing electricity needs. That said, with so many old coins, even people with a regular home computer can still mine and get old coin rewards. Let's look at a variety of hardware and software scenarios. First, a big disclaimer here. All my dollar assumptions here are examples and may not reflect reality anymore. You mine and trade at your own risk. We'll start with a basic setup. We'll say that a regular home computer can be purchased for a $1,000. You'll need the mining software that is free to download from the respective cryptocurrency website. It will run on most operating systems. You might also choose a local wallet to store your private key. Sometimes a special software is required which the specific old coin will identify. For example, Geth is the program that communicates with the Ethereum network. And acts as the relay between your computer, its hardware and the rest of the Ethereum network. Okay, so let's say you can earn $5 per day mining with this computer. That's not unreasonable. For some of the newer popular coins such as Peercoin and Feathercoin. Earning $5 per day and with electricity costs of $1 to power your PC for 24 hours, the payback period will be just a little less than nine months. Not bad, however, you're not going to get rich. Here we also assume you have an existing internet connection and that the computer will not be available for any other use. You might also need a fan to keep the machine cool. Not as likely with a home computer, but air conditioning and the attending costs become essential with more processing power. To increase your earnings require a bigger investment in computing power. High performance home computers for say, computer aided design or gaming can be anywhere from $5,000 to $10,000 and more. Computers with additional graphical processing units or GPU's are great for fast processing and subsequently are perfect for mining. They also consume much more power which increases your electrical bill. If you're just wanting to experiment or create a small passive income, you'll need to do the math to figure out what makes sense to you. These examples are all for the entry level miner. So what might be hardware and software requirements look like to make some real money? For this, you're going to need what's called a mining rig. The smaller rigs are made up of the usual home computer parts like hard drives and central processing units, CPU's. But with more emphasis on graphical processing units, GPU's. A good starting configuration might be six GPU's. The rig can't

be configured in the typical computer case so a special housing unit is now required. They come with their own fans but you'll need additional cooling. It's also gonna get really noisy. All this processing require more power wattage too. A standard computer uses around 500 watts. This new rig is going to need at least 1,200 watts. There are no special RAM or hard drive requirements. Four gigabytes of RAM and 120 gigabyte SSD hard drive will suffice. To increase processing, more rigs can be built and they can be tethered together. These mining rigs can fill a car garage and at an industrial level, the scale of current Bitcoin mining for example, entire warehouse floors and large data centers are being used. Searching online for mining rigs will provide you lots of options for you from DIY to pre-built. It's an exciting and growing space. To increase your own processing capabilities, you can join a mining pool. This is when multiple people combine their mining rigs over the internet to jointly mine the same cryptos. Check out Miner Gate as an example. There's also mining software that enables you to dynamically change mining to different old coins that are more profitable. In addition, in order to avoid hardware costs, it's possible to participate in cloud mining. In this setup, you simply pay for the use of mining rigs that are run by a provider. To learn more, check out Genesis Mining as an example. Cryptocurrency mining can be a fun hobby. And for many, it can be a real money earner. It's certainly not for everyone and the risks remain high. We'll discuss those next.

The challenges of being a miner

- It's common to look back at the early days of a successful and lucrative trend and wish to have invested early. Those that get in early often have enormous luck or have incredible, unique foresight. For those that mined Bitcoins in its early days and held on to them and their private keys, they were able to realize exceptional gains. In July 2010, a single bitcoin was worth eight cents. In December 2017, a single bitcoin reached a staggering $17,900. That kind of value appreciation is rare. Even the most prescient could not have anticipated such growth. This kind of return on investment attracted significant interest. More miners jumped in as the price appreciated and as a result, the processing requirements increased. Most small-time miners with their home computers or mini rigs were effectively shut

out as big players threw millions of dollars in building warehouses full of mining rigs. Today, mining Bitcoin with one's own rig is largely fruitless. Any Bitcoin that could be mined would cost many more times to mine than what it's worth. That said, cloud mining and joining a mining pool does offer alternatives worth exploring for enthusiasts and professionals. Of course, this is a story of Bitcoin. Today, there are thousands of old coins that are ripe for mining for all types of users. However, as long as an old coin requires proof-of-work, it has the same risk of Bitcoin. As value appreciates, it becomes harder for the little guy to play. The challenge then becomes to pick some winners early and mine old coin when their value is low. The truth, though, is that most old coins will fail. Cost to mine will be expended, but the winning coins may ultimately have no value. There will be many winners though. And those that get lucky and can use business savvy to anticipate winning old coins could reap big rewards. Betting on the right old coins at the right time isn't the only risk, however. Mining presents some other challenges too. The process and components of proof-of-work is part of the genius of the cryptocurrency phenomenon. However, as more people and organizations participate, power demands to support all the processing needs is growing quickly. For those who lose each new block opportunity and thus the attendant winning crypto, they have effectively expended energy with no return. If we extend this to a global scale and that's exactly what we're dealing with here, miners are burning through enormous amounts of energy. It's massively energy-inefficient. Without a viable alternative to proof-of-work, the energy needs of miners could both impact our other more essential electrical needs and they could inadvertently contribute towards making our climate crisis worse. Alternatives to proof-of-work called proof-of-importance, which uses roles for validating transactions, and proof-of-stake, which uses the type of participant financial stake, are emerging and show promise, but are still rare in public blockchains. Bitcoin and old coins have largely enjoyed unhindered freedom for almost 10 years. Largely absent of regulation and constraints, the technology and opportunities have grown exponentially. Many have made a lot of money, many have lost. How long might this window of unregulated innovation continue? We can look to China and South Korea for answers. Both have made ICOs illegal. And China is rumored to be looking to limit and even ban cryptomining all together. A big

risk for miners is the uncertainty of federal policy in a given market. Add to this the rapid impact of regulatory decisions thousands of miles away can result in massive downward crypto fluctuations. While nations appear largely supportive of the potential for cryptocurrencies and generally don't want to curtail innovation, until there is some notion of where things are headed from a regulatory perspective, anxiety will continue. Finally, in this emergent space, there continues to be a lot of security risks, from simple private key theft, which is the equivalent of giving a criminal the login name and password to your bank account, except without any recourse, to unstable exchanges, hacking, and fraudulent ICOs. There is plenty to be concerned about. One of the more sinister and emerging hacking techniques is called cryptojacking. This is when criminals take over a computer for use as a mining machine. It's remarkably easy to do. Unlike other hacking techniques, cryptojacking does not necessarily require any software to be sneaked onto an unsuspecting computer. Simply by accessing a certain website, JavaScript is run, which leverages the processor for mining activities. Monero, a popular cryptocurrency, has been a particular target used by cryptojackers to mine. There are solutions to counter cryptojacking, including browser extensions such as MinerBlock and by domain blocking. Cryptocurrency mining is an exciting opportunity for enthusiasts and professionals alike. But as I've described here, it's full of risks too. Despite the nine years that have passed since Bitcoin first emerged, it still looks to me that we're at the beginning of the massive potential and impacts ahead.

Where do you go from here?

- The current state of cryptocurrency is one defined by significant opportunity. But in a context of high risk and uncertainty. Today we see all the characteristics of a marketplace and technology in flux. Each day brings new participants, more investment, more challenges and in many cases, many more questions. To understand what to do now, means that we have to have some ideas of what might happen in the future. Cryptocurrencies are certainly not without their detractors. There are several high profile government business and technology leaders who have said that cryptocurrencies will ultimately fail. They believe there is insufficient underlying substance for

momentum to continue. That the foundation is too brittle to appropriately mature. That the forces of the global marketplace and the weight of existing financial institutions and government regulations will be too much to bear. They might be right. There are also a lot of leaders who believe that cryptocurrencies are a threat to our economies. That if not managed appropriately could result in a worst, totally economic collapse, or at best, in economic chaos. They might be right too. We should listen to all of these views and we should make careful personal decisions relative to cryptocurrencies that are informed and appropriately risk evaluated. What is clear today though, is that there are few signs that crypto innovation is slowing down. Everyday it seems, brings a new idea, a new opportunity and a new direction. Who knew that in the early days of Bitcoin, that we would see the emergence of a whole new class of raising capital called ICO's? Who knew that the enabling technology of crypto, blockchain technology would be seen as one of the most disruptive and powerful new enablers of innovation across almost every sector of our economies? Digital currencies seem perfectly aligned with the opening act of the fourth industrial revolution. A new period of humanity defined by ubiquitous connectivity of people and things. By low barriers to the transfer of value across borders. By technologies such as augmented reality, artificial intelligence, and new approaches to work and city living. Cryptocurrencies have less friction than traditional forms of money. They can move quickly between entities including between machines that may negotiate their own terms of engagement without human intervention. It is possible cryptocurrencies could displace feed currency and dominate our global marketplace within just a few decades or even sooner. All of this is possible but uncertain. What is certain is that many threats and risks must be countered. A new technology and set of behaviors will never prosper if confidence cannot be attained. The hacking, fraud, disruptions and limitations of technology such as transaction settlement speed and growing blockchain size must be addressed. We'll never eliminate and defend against all the actions of bad actors but we can go a long way to make those issues a minor cost relative to the benefits. For individuals, this is a great time for learning and for doing a small amount of experimentation. As many have rightly said, it's probably a bad idea to invest in cryptocurrencies if you can't afford to lose your entire investment. For enthusiast, there is a lot to

play with from writing dapps on Ethereum to building a mining rig. For professionals, there are a lot more options from making investments to innovating and building completely new businesses and approaches to all ways of doing things. The cryptocurrency movement could die in a brief moment if a set of future regulations backfire. Or it could quickly blossom and mature if there's a national recognition by several state governments. Today this kind of sudden fork in the road is a reality. Anticipating the future requires us to think about solving problems that don't yet exist. This makes it specially difficult. The future of cryptocurrencies is particularly uncertain. Without a doubt, it is exceptionally compelling and exciting to both observe and experience as it unfolds.