BLOCKCHAIN SECRETS

The Ultimate Guide To Blockchain, Cryptocurrency and The Future of The Internet

Disclaimer

This e-book has been written for information purposes only. Every effort has been made to make this ebook as complete and accurate as possible. However, there may be mistakes in typography or content. Also, this e-book provides information only up to the publishing date. Therefore, this ebook should be used as a guide - not as the ultimate source.

The purpose of this ebook is to educate. The author and the publisher do not warrant that the information contained in this e-book is fully complete and shall not be responsible for any errors or omissions. The author and publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by this ebook.

Table of Contents

Introduction

Countless discoveries and inventions have been made throughout our history. Some of the developments have been minor, some of them have been major, some have been short-lived, and other events have been more critical and longer-lasting. There have been certain developments throughout our history that have been so vitally important to humanity that they are considered the sole factor behind all of humankind, collectively making progress and taking a critical and everlasting step forward.

For example, consider how the creation of farming equipment and fertilizers allowed for the exponential growth of food outputs from fixed pieces of land. Without these inventions and discoveries, the world would not have been able to support the explosive population growth that we have witnessed across the globe. It

was only a few hundred years ago that scientists and economists indicated the end of population growth, due to the fact that food production just grew at numerical rates, doubling or tripling every certain number of years, while populations grew at exponential rates, expanding to the power of two or more during that same period.

At the time, this meant that sooner or later there wouldn't be enough food to feed everyone unless more food could be obtained from fixed pieces of land every year. Fortunately, this is precisely what happened. Science was able to deliver heavy farm equipment, fertilizers such as ammonia, and other improvements so that that food harvests could keep up with the population growth rates. This allowed for more people to be sustained in the same area of land as before. Without these developments, the world would be a very different place today.

Similarly, the creation of antibiotics, penicillin, the introduction of air travel, ocean freight, and the steam engine, and more recently, the sharing of information in the Information Age that was made possible by the invention of microchips and transistors, have all changed the world irreversibly. As a result of these innovations and discoveries, we are more connected, better off, healthier, and have more accessible and cheaper access to goods and services than ever before.

When it comes to the information age, things have progressed at breakneck speed, ever since the first dot-com wave in the early to mid-90s. Everything from the user interface tools and technologies that have defined how we interact and interface with technology. Everything from payment solutions to banking solutions has dramatically changed over the last 20 years.

The same can be said for social networks and primary email, along with the advancements that have been made in fields of artificial intelligence (AI) and big data analysis, both of which have an impact on everything from helping with governance to online search. Collectively, we've gone from necessary solutions for all of the above to have sophisticated software services that combine various aspects of technology to deliver effective, robust, value-added, and seamless services to billions of people around the world.

However, with all the progress comes new challenges. AI, big data, and the ability of governments to implement mass surveillance initiatives, and the ubiquity of technology all around have begun to pose serious ethical questions and technological challenges. This leads to the question, where do you draw the line between legal and illegal surveillance? How can we, as a society, trust the data usage collection and manipulation practices of companies and governments when they aren't transparent. When it comes to the role of government and big corporations and their relationships with private users, where is the world headed?

It is with this exciting and challenging background in mind that blockchain will be discussed. In recent years, blockchain has become a popular technology and so much more than the latest tech fad. It is, in the opinion of many subject area experts and tech gurus, the next giant leap for humanity and something that will have a significant impact on our children and us as the farming and healthcare developments of the past had an effect on our great-great-grandparents more than a century ago. We have now entered the new Information Age.

Chapter 1 – A History of Money, Cryptocurrency, and Blockchain

The concept behind establishing a permanent, decentralized ledger, like blockchain, was first discussed in 1991. However, the first actual blockchain implementation was designed in 2008, by Satoshi Nakamoto. It was his initial design that was used as the underpinning technology that runs the digital currency known as bitcoin.

The blockchain that was engineered by Mr. Satoshi serves as the public ledger for all bitcoin transactions. Bitcoin, if you don't already know, is a digital currency that is now worth roughly $16,000, that runs on blockchain technology. The most well-known blockchain on the market today is that for Bitcoin, with the Ethereum blockchain coming in a close second.

The technology that allows bitcoin to serve as a digital currency, as a store of value, and as a medium of exchange is blockchain because bitcoin transactions are recorded in a blockchain ledge. This means blockchains are not limited to running bitcoin; rather blockchain application can span the entire gamut of trade, finance, healthcare, legal operations, records management, gaming, online exchanges, probability, and more.

Before you can get started understanding blockchain technology, you have to know how it fits in with our current currency and digital currency.

Money

Money is nearly as old as humanity. Many books have been written on the subject. One that is worth checking out if you are interested in the matter is *The Ascent of Money: A Financial History of the World* by Niall Ferguson. Money, to work, has to be both a store of value as well as a means of exchange. In the past, we've used many different items for money, including gold, silver, cattle, beads, and salt. No matter the form it takes, money has to execute these two essential functions. Also, there has to be trust that these roles can be fulfilled by the money.

Cryptocurrency

A cryptocurrency is a form of currency that has become popular over the last several years. Cryptocurrency is created by using the encryption techniques of computing and mathematics. These techniques allow us to transfer funds and verify that the transfer did, in fact, occur. Another essential aspect of cryptocurrency is that it is independent of governments and central banks, making them decentralized.

These days, many important banks are becoming increasingly involved with the same kind of technology that underlies cryptocurrency. However, it is essential to understand that any currency that arises from their endeavors won't be true cryptocurrency because it will be controlled by the banks. The most reliable and most dedicated advocates of cryptocurrency are determined that it will not be centralized.

How Did Cryptocurrencies Develop?

Bitcoin is the most well-known cryptocurrency on the market. It has been the recipient of hype, fame, and publicity. The general public has been fascinated by its extraordinary increase in value over the last several years. They have been awe-struck by the tales of significant wealth that has been generated with bitcoin, for those who acquired it in its infancy, when it was cheap.

Despite its novelty, people quickly realize that bitcoin is genuine money. In addition to bitcoin, there are many other cryptocurrencies, who like bitcoin, have had massive increases in their dollar value. Legitimate government and businesses are pursuing an increasing involvement in cryptocurrency. Despite critics, the market for these currencies is thriving.

Cryptocurrencies, Fiat Currencies, and Stocks

Fiat currencies are the currencies we use daily, like the dollar, yen, euro, and renminbi. Despite having the word currency in the word cryptocurrency, they are more similar to stocks and shares of the stock market than between fiat currencies and cryptocurrency. When you purchase cryptocurrency, you get some of the coins for that cryptocurrency, which acts like a technology stock and a digital entry into a ledger, known as a blockchain.

Blockchains

Blockchains are digital ledgers and can be formally defined as a continuously-growing list of records that are linked tougher and secured using advanced cryptography. In more simple terms, a blockchain is literally a chain of blocks. Each record in the list of a blockchain’s chain is called a block that contains specific types and pieces of information. Each block will usually include some sort of pointer as a link to the previous bock, transaction data, and a timestamp, which can take a variety of forms.

Another way to look at is that a blockchain is much like a database where each entry is linked to the previous and next entry. This means that the information contained within the blockchain can't be changed, once a block with specific data is added to the chain. Depending on the chain that you are looking

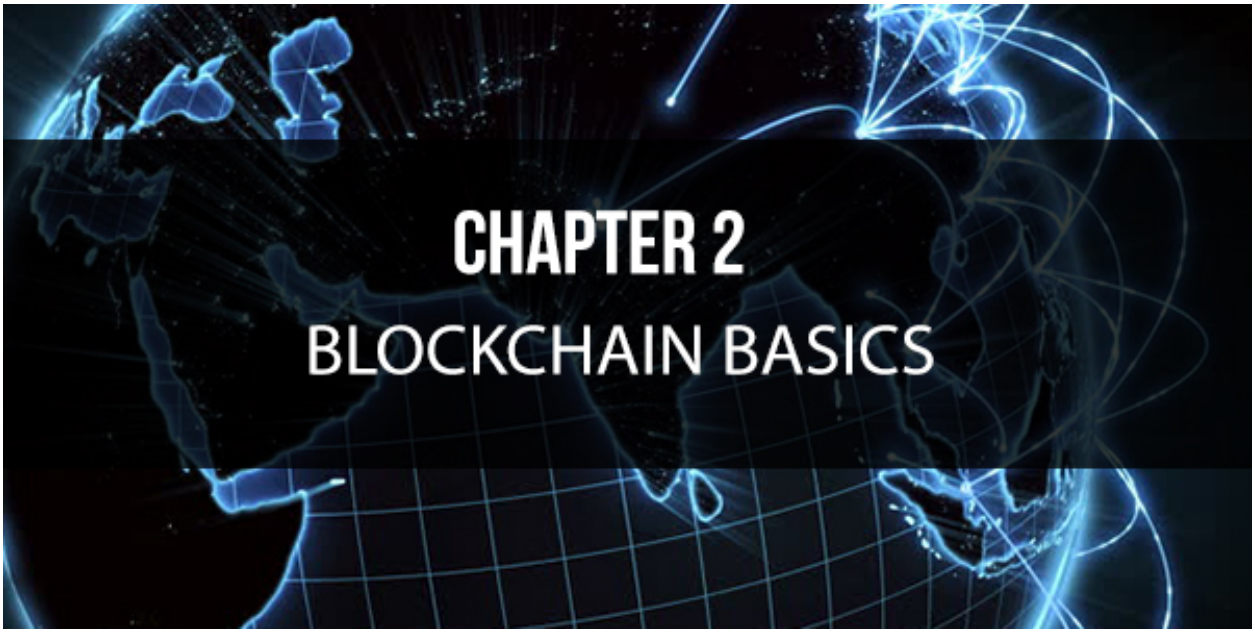
at, there are often useful tools for exploring that will allow you to scan the transaction data.

Blockchains are resistant to being modified because of their inherent design. This allows blockchains to record transactions between different parties efficiently. These transactions are not only verifiable but permanent as well. Once information is recorded in a blockchain, the data cannot be altered after-the-fact without altering the subsequent blocks by having the majority of nodes on the network agreeing to the change.

This inability to change the data within a blockchain make illegal or unfair actions almost impossible to carry out. If a hacker wished to alter information within a blockchain, they would have to gain control of every node. This security is one of the most useful characteristics of the blockchain.

Since blockchains are designed to be verifiable and permanent, they are especially suitable for recording events, maintaining medical records, drawing up agreements, fundraising, and keeping track of other documents.

Chapter 2 – Blockchain Basics



Whether you are aware of it or not, you conduct business every day, even if you don't work. At some point, everyone gets online and initiates some kind of transaction. Whether it is purchasing something from Amazon or buying something from iTunes, you are engaging in the business of blockchain technology.

Even though the term “blockchain” is relatively new, the technology has been around for about a decade. The digitized ledger that Satoshi Nakamoto created in 2008 was the basis for the spreadsheets that manage cryptocurrencies and other online trading transactions. The technology is used in cryptography, which is how text is coded on the Internet.

Cryptography is used in blockchain technology to create distributed trust networks. This, in turn, allows any contributor to

the system to operate the transactions securely without having to obtain authorization from someone else in the digital ledger. These transactions are then verified, approved, and then recorded in an encrypted block. This block is saved intermittently and then connected to the previous block, which in turn creates a chain.

Components of a Blockchain

Two main parts make up a blockchain. The first component is the decentralized network. The decentralized network is what facilitates and verifies the transactions that are made. Having blockchains on a decentralized network means that the software isn't limited to one computer system. Instead, it can be controlled on multiple computer systems, and more importantly, it isn't controlled by the government.

The second component is the indisputable ledger where the transactions are processed and recorded in a location that is secure. This security makes it almost impossible for someone who is not connected to the chain to make changes or steal information.

Since there can be numerous contributors involved in any blockchain, any of the contributors can control the information that is entered into the ledger. Since every transaction is processed securely, and given a permanent time-stamp, it can become challenging for another contributor to alter the ledger in any way.

Blockchain technology can be used for various computerized and internet-based application. One of these applications is smart-contracts. Smart contracts allow businesses to automatically verify and execute agreements that function independently in a secure environment. Blockchain technology acts as a middleman for implementing all business deals, protocols, and programmed exchanges of information in smart contracts. As more and more transactions are completed online, to not only run our personal lives but professional lives as well, more and more deals are being signed and created online.

Blockchain applications have begun to become increasingly popular in the medical field in recent years. Researchers are now investigating these applications dealing with digital identity, insurance records, and medical records. There are many medical offices today that use some kind of digital machine to verify that the information they have on file is, in fact, your information.

Security Concerns

One of the most significant issues people are faced with today is the thought that all their information could be compromised by hackers because most of our personal information is digitized. It also seems that it has become too easy for complete strangers to access, copy and tamper with our data. However, it is still a risk that we all take despite the increasing probability of being hacked. Blockchain technology was created to help ensure that doesn't happen or in the very least make it more challenging to try.

For someone to hack the blockchain system, they would need to go back and change every single block. That would require a ton of effort and patience because blockchains could have upwards of billions of chains linked that a person would have to go through and change. Changing just one or two blocks would automatically send an alert that the system is being hacked. This is only one of the many reasons why blockchain technology has become so popular.

Blockchain technology can be used for a variety of other things as well. It can also be used for global payments, sharing music, or tracking diamond sales.

Types of Blockchain

There are three major types of blockchain. There are private blockchains, public blockchains, and consortium blockchains.

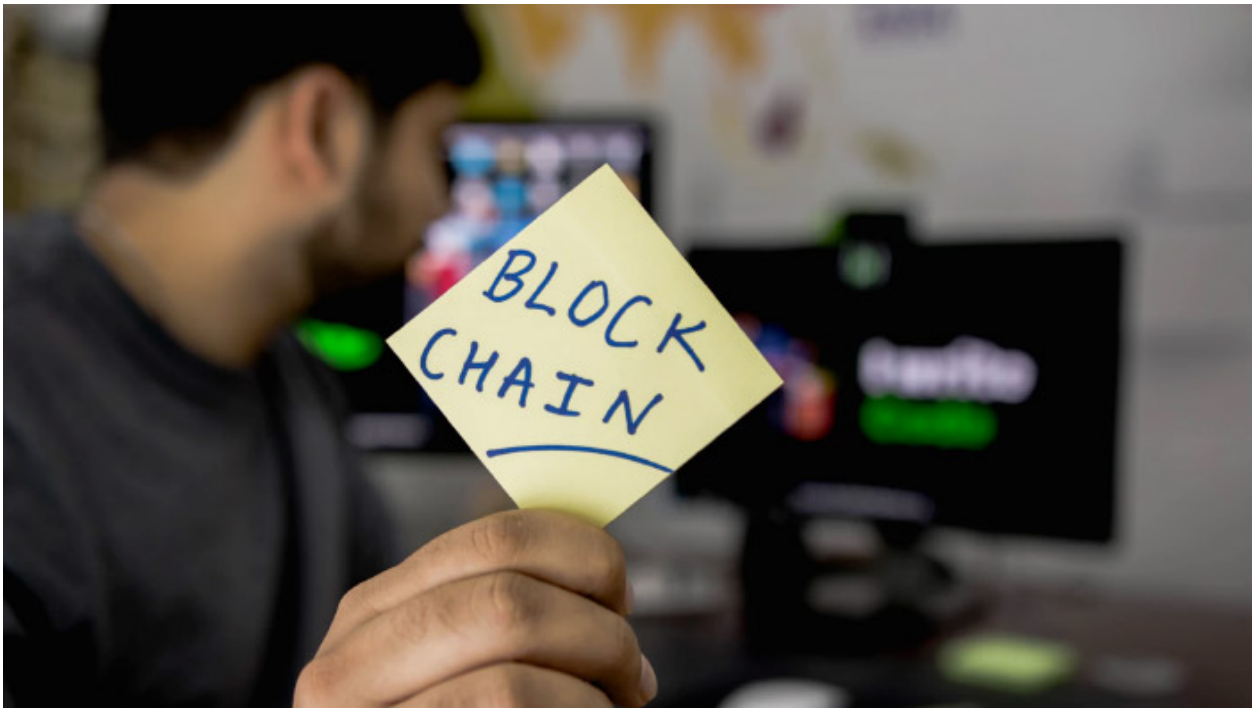
Public blockchains are created by the public. Anyone can participate in the creation, confirmation, and recordation of the content that is put into the blockchain. There isn't just one person in charge of overseeing the transactions that happen in this kind of blockchain.

Because there isn't a single person in charge of these blockchains, decisions are made by many decentralized agreement tools such as proof of work, which a computer algorithm that is used by cryptocurrencies like bitcoin. Public blockchains are open and crystal clear in content, making it easy for anyone who looks at them to understand what they are and what they can do.

Public blockchains, on the other hand, are privately owned by an individual or organization. With public blockchains, there is a single, designated person in charge. While there can be several contributors to this type of blockchain, the final transactions are either approved or disapproved by the person in charge and then recorded.

The purpose of consortium blockchains, also known as federated blockchains, is to remove the only autonomy given to just one contributor by the use of private blockchains. This type of blockchain allows for more than one contributor to be in charge. Instead, there is a group of companies or individuals that gather and make decisions that benefit the entire network.

Blockchain Technology Breakdown



Blockchain technology is an irreversible, encrypted, decentralized ledger that has the potential to make all centralized activities, processes, and organizations entirely autonomous. This means that a person will have the ability to eliminate the middleman and specialists, effectively reforming every single business in the world.

Blockchain technology is merely a way to keep track of any money or trading exchanges you engage in online. You can think of it like an accountant who keeps track of all the money that you spend. Currently, blockchain technology is mostly used to handle

any type of situation that deals with cryptocurrency, like bitcoin. Let’s consider the following example.

When you complete a transaction using bitcoin, that specific transaction is processed through the blockchain. Before the transaction can be achieved, you or someone connected to your bitcoin account has to verify that the transaction is legitimate. Once the transaction can be confirmed as being valid, it is recorded and saved to a ledger that is controlled by the blockchain. At this point, nobody can change or alter the transaction in any way. Only you or those with access to your account can verify transactions.

Blockchain technology is controlled by a decentralized network, which means that it isn't controlled by any government. By running on a decentralized system, it is much easier to conduct business transactions. It is also more private because you don't have a federal bank holding your money or other assets. Everything is strictly handled by you and your company. To understand the importance of decentralization, you need to consider the following examples of centralization and decentralization.

Centralization Example

When you use your debit card at the bookstore, you swipe your card to pay for your purchases. At this point, the

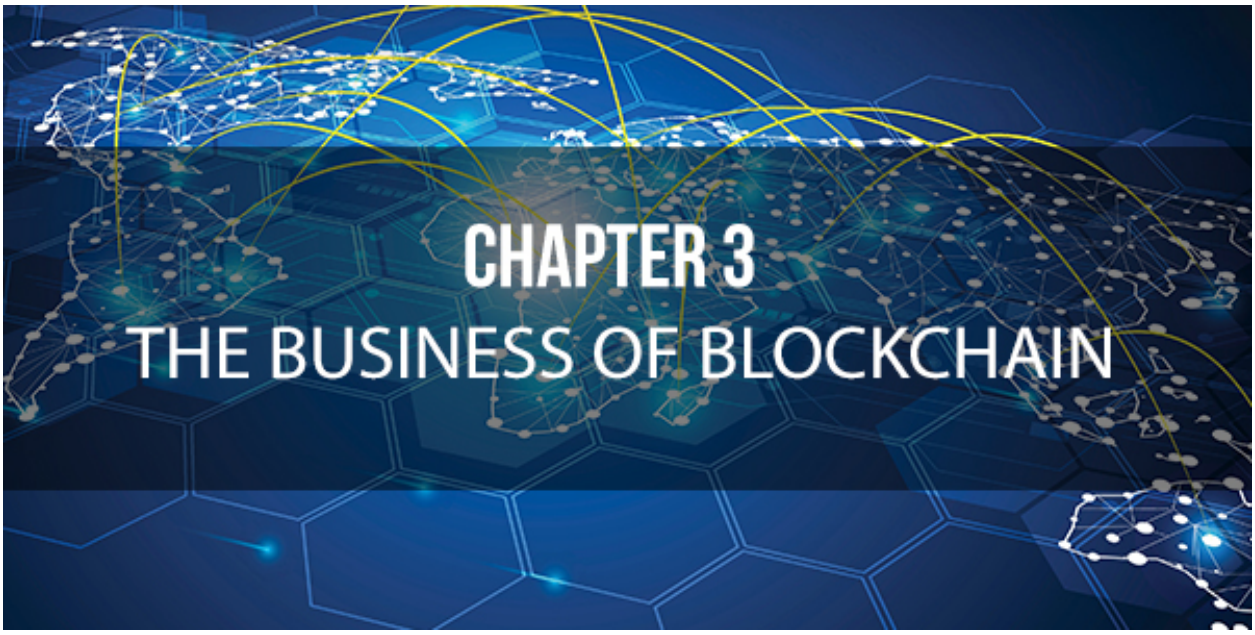
company then sends a bill to your bank for the amount agreed to when you paid for your goods. The bank then must verify that it was you who made the purchase. The bank, once the transaction is confirmed, releases the money to the company and records the transaction in their ledger. The ledger the bank recorded the transaction in, includes all the operations the bank made on behalf of the card you used. The bank has complete control over what happens with the ledger. Other than having the ability to look at your banking statements, you have no authority to change anything or do anything with the ledger. Centralized ledgers are much easier to hack because they are controlled by multiple entities.

Decentralized Example

Imagine that you want to transfer 1.00 bitcoin to someone. All you have to do is tell whoever is in charge of the network, whether it's one person or a group of people, that you are transferring 1.00 bitcoin. Once this is done, the transaction is approved and then it is recorded.

Decentralized blockchains are much better than centralized transactions because it takes less time to complete a single transaction. Other reasons decentralized blockchains are better is that a person or company can send secure information to another person or company, such as encrypted messages and medical records.

Chapter 3 – The Business of Blockchain



Everybody has trust issues with something in their lives. Many people today, don't trust inputting their information into the internet. However, even with this mistrust, it hasn't stopped many people from continuing to do it.

One purpose of blockchain technology is to help ease the distrust that people have with inputting their information on the internet and is one of the main reasons why companies are increasingly investing their money in the use of this technology. In fact, between 2013 and 2016, a study showed that blockchain-managed funds reached a total of $1.6 billion, which equates to a 1,600 percent increase.

Different Industries that Use Blockchain Technology

The financial industry is one of the sectors that have greatly benefitted from the use of blockchain technology. This is because of the vast sums of money and transactions that are in play in the industry. Here are a couple of examples of the different companies that are utilizing blockchain technology today.

- ***Crowdlending***
  Crowdlending campaigns have started to take over the act of having to go to the bank to get a loan. Crowdlending is a person to person lending company. Today, there are, on average, more than 50 billion person to person loans being made worldwide. This industry will likely feel an enormous boost with the use of blockchain technology.

- ***IBM Global Financing Unit***
  IBM has become one of the major players in blockchain technology use, with a proven track record of being a great asset for tracing transactions. IBM's Global Financing Unit processes $2.9 million in payables for the company every year. It is also responsible for granting credit to more than four thousand suppliers. IBM has been successful in lowering dispute settlements by 25 percent, thanks in part to

blockchain technology. This decrease in percentage has resulted in the group being able to free up $100 million in pre-confirmed capital for other purposes.

- ***Bookkeeping***
  The bookkeeping industry has greatly benefited from blockchain technology. Every transaction that takes place in the economy today is registered internally in the private records of individual market participants. Blockchain technology takes place when accounting expands past the borders of the network.

Adding Value to Your Business

There are numerous ways that blockchain technology can add value to a business. One way is by building a network for your business. Dr. Michael Yuan, the Chief Scientist of CyberMiles notes how blockchain can provide value to startups and companies. His theory is that the key benefit of blockchains will deliver the ability to construct a network for all kinds of businesses. What his theory states are that rather than competing against each other, companies can collaborate and build a system with each business industry having its own chain.

Another way that blockchain technology can add value to a business is by banking the unbanked. It might be hard to believe,

but there are a lot of people in the world who don't have bank accounts. Blockchain technology will provide the opportunity for these people to create a bank account. Someone could just open a bitcoin account and in return have a digital wallet.

A third way in which blockchain technology can add value to a business is by lowering the time for transactions to be complete. Again, time is playing a significant role in the blockchain world. Christopher Brown, CEO of Modular, create Blossom, a digital wallet for Ethereum. The program is a multi-featured desktop wallet application that gives businesses and users a more straightforward way to handle their funds. It takes less time than if you were to head to the bank to get cash.

Next, blockchain technology can add value to businesses through legal contracts. This can be done by linking the Internet of Things (IoT) data and blockchain technology. Utilizing the data from IoT devices allows individuals and businesses to connect to legal contracts that have been saved on the blockchain. For example, when you are buying a house, all the documents that you sign, must also be signed by the seller. This means that all the documents must be in one place for both parties to have access. Outside information from IoT connected devices is linked to the blockchain, making the legal contracts immediately usable without anyone being able to interfere in the process.

The final way that blockchain technology can add value to a business is by helping with monetization. The ways companies are making money are changing. People no longer pay attention to ads because you can now fast-forward through the commercials and online they can be ignored. Plus, the money generally goes to the site where the ad is placed, which has a tremendous impact on business.

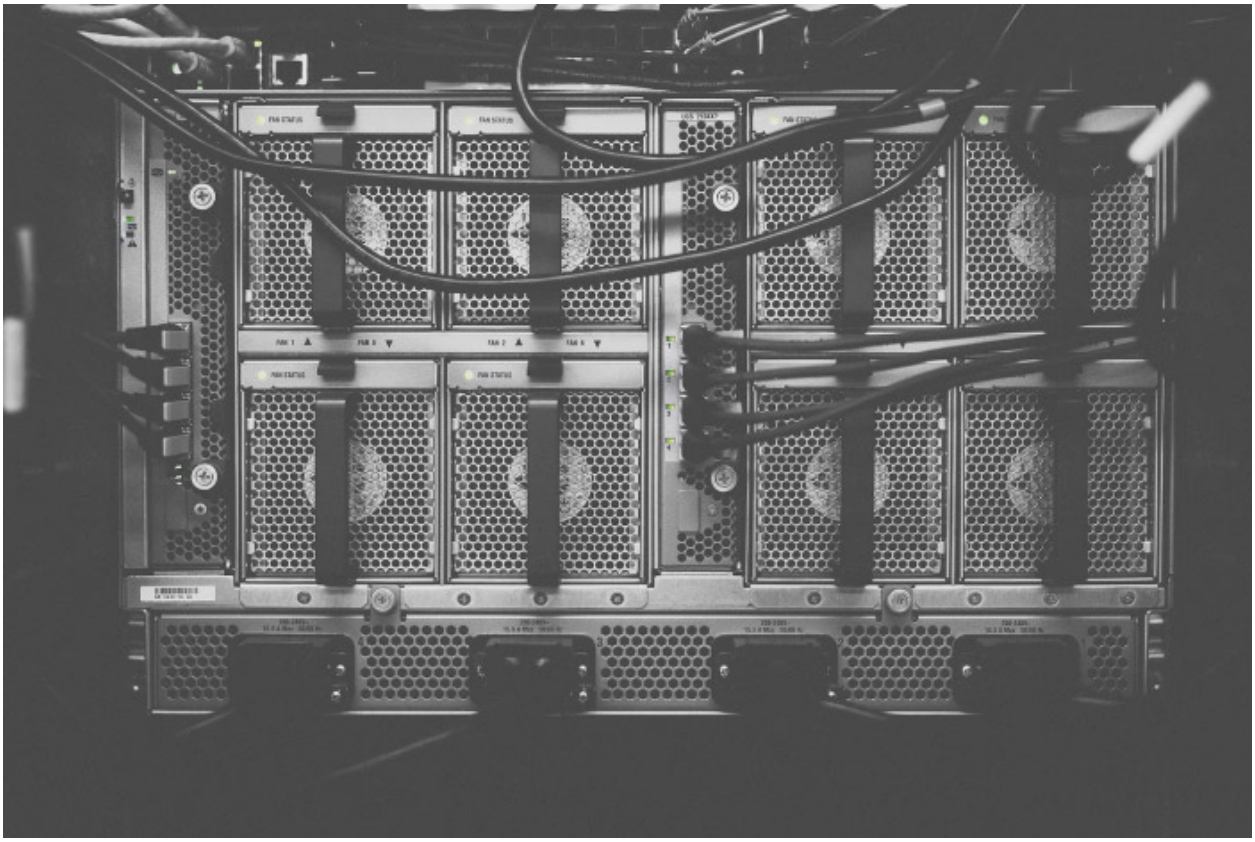
Blockchain technology solves this problem. This is because every part of the content that is created for ads is recorded on the blockchain, which is how content creators are rewarded through cryptocurrency or fiat currency.

Growing Money

Many experts believe that blockchain technology will become the way of the future. Cryptocurrency is rapidly increasing because people want to put their money in a place that is not only safe and secure, but that will also gain value like a savings account. However, savings accounts aren't as secure as they would like. By the end of 2017, future markets had already been created for bitcoin. That was also the year the finance industry saw a dramatic increase in Initial Coin Offerings, (ICO). In the last year, ICOs have gained more money than venture capital investments.

While cryptocurrencies continue to improve in their abilities to quickly process transactions, eventually they will compete against credit card companies processing of transactions.

The Cloud and Blockchain



At some point, everyone has used the cloud to back up data that they don't want to lose. If you didn't know, the cloud actually runs on a blockchain. Experts say that we have started to take luxury for granted. In the past, you couldn't merely click a button and automatically save data to a backup site like iCloud or OneDrive. Instead, you were required to transfer the information on a

compact disk or flash drive. Then, you would have to take the disk or flash drive to another computer to download the data.

While you can still do this today, there isn't a guarantee that this type of technology will last. Like the floppy disks of the past, compact discs and flash drives may become obsolete, but internet saving applications will always be updated because we now live in a tech-savvy world.

Blockchain and Gaming

eSports and online fantasy sports have grown significantly over the last decade with more and more people creating online fantasy sports teams. Online games, like Fantasy Football, were some of the first sites to adopt the earliest versions of bitcoin and other cryptocurrencies. They also use blockchain technology to run and keep up with the gaming technology.

The uses of blockchain technology don't just stop with fantasy sports. The most popular smartphone applications to download today are games. This is why, as the technology grows, more developers will likely make use of blockchains, as well as cryptocurrencies.

Supply Chain Management and Blockchain

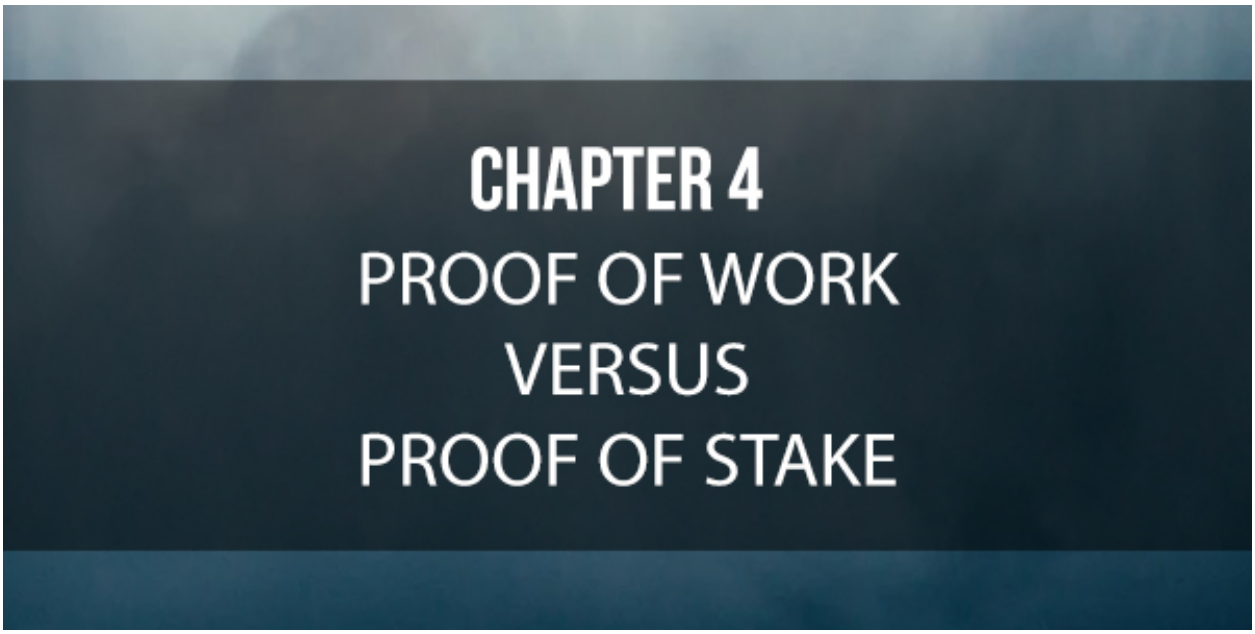
Blockchain technology will also benefit supply chain management by providing a way to trace goods while at the same time being cost effective. For example, sending packages through the United Parcel Services from one business to another. In the past, someone had to call to find out where their box was if it hadn't arrived when it was supposed to. Today, you are provided with a tracking number that allows you to see where the package you sent or are waiting for is in transit, which creates a blockchain.

Blockchain technology has made it easier for businesses to do business together because it has dramatically simplified the production process, and transfer process, as well as the verification and payment methods, used.

Blockchain Technology and Quality Assurance

In business, mistakes happen, no matter how careful you are and how closely you follow processes and procedures, and it can be challenging to pin down how the mistake occurred. With blockchain technology, mistakes and errors can be traced back to the point of origin. Not only does this make it easier to investigate mistakes, but it also saves companies time and money.

Chapter 4 – Proof of Work vs. Proof of Stake



A majority of the public blockchains that are currently available are based on a proof of work system. However, in 2018, the second biggest cryptocurrency, Ethereum, began testing a new system that would change its blockchain from a proof of work to a proof of state system. Before we can get into what exactly this means, it is essential to understand what exactly is occurring when a transaction is verified.

Proof of Work

The mining of bitcoin is accomplished by using a high-powered machine that will utilize a SHA256 double round has a verification process with the purpose of validating bitcoin transactions as they

happen. This is done to provide security for the sanctity of the bitcoin blockchain. The speed that your machine can mine bitcoins is measured regarding hashes per second.

Bitcoin, in exchange for this service, compensates those that are doing the mining by offering them a fraction of a bitcoin for every validation. They do this to offset time and energy costs. Additionally, those who initiate the transaction will typically provide some amount of a transaction fee to help offset costs as well. The higher the computer processing power of your bitcoin mining machine, the more you can make through the process.

To be accepted into the blockchain, each block must have a valid proof of work. A proof of work is a type of data that is both difficult to produce as well as time-consuming. Creating proof of work is essentially a random process with a low probability of success. This means that a bitcoin mining machine that is trying to complete the process requires a significant degree of trial and error to be successful. Bitcoin uses what is known as the hashcash proof of work.

The hashcash proof of work is a type of cryptographic algorithm that makes use of a hash function as a core building block of the mining process. The most common hashcash function that is used today is the haschash-Sha256. This particular proof of work function was created by Dr. Adam Back in the 1990s. It was initially used as a way to prevent email spam abuse because

successfully generating the hashcash for a single email was simple. However, creating one for a vast number of emails at the same time proved to be much more difficult.

You can tweak hashcash proofs of work for the difficulty to ensure that new blocks aren't being generated faster than the network can handle. This means that a new block can't be generated more than once every ten minutes at this time. As the probability of each successive generation is low, this makes it challenging to determine which bitcoin machine is going to generate the next block.

For a new block to be considered valid, its hash value must end up being less than that of the current target. This means that each block will have to naturally indicate that work has been completed to generate it. Each block also contains the hash of the preceding block, which is how the chain understands where each block falls within the overall blockchain. To change a block, the work must be redone on all the previous blocks, and new and connected hashes must be generated for all of them. The blockchain is then essentially protected from tampering, because of the enormous computational power that is needed.

Proof of Stake

Most of the significant cryptocurrencies today work off of some variation of the proof of work model, either through the SHA256 hash or through another, similar hash. However, Ethereum, bitcoin's largest competitor, has been working on an alternative that could significantly change the way blockchain transactions are verified.

In early 2017, Ethereum released the implementation guide for a hybrid proof of work/proof of stake system. They are rolling out this new system in phases before they make it the platform's primary verification system. The plan currently states that the blockchain platform will alternate between the two systems. With the new system, about one out of every 100 blocks will use the new system while the rest will continue to use the old system.

There hope is that the new system will improve the rate at which they can produce new blocks. This will mark the first step in the plans for Ethereum's evolution. This will be the first time a proof of stake system will be used to secure a blockchain, which will be a significant step forward. This new system will serve as the proof of concept test for an alternative to the proof of work model that dominates the cryptocurrency today and provide proponents the ability to test their claim of its superiority. When the new proof of stake model is rolled out on a larger scale, it will significantly reduce the amount of electricity that is required to verify a single block.

It's important to understand just how the proof of stake system differs from the proof of work model. With proof of stake verification, rather than having the miner solve the equation to verify the block, a validator, who is confirmed reliable by the stake they have in the system, will commit to its accuracy. They know that if they lie, they will lose their own ether as well.

During the first stage of deployment, all of the blocks that are verified through the new system will also be checked through the old system to help double verify that the blocks contain the information that they should, while also testing the accuracy of the new system. Validators will then look at the various chains that are available and make a decision based on how much ether is currently in the chain. If they make a poor choice, they will lose their money. This process will help form a consensus that leads to a single more massive chain from the many smaller ones.

Benefits of the Proof of Stake Model

While the process of implementing the proof of stake model isn't smooth sailing, it doesn't mean that the proof of stake system is going to lose out. It contains many clear benefits over the more traditional process. This first clear benefit that this new model will have is that it will drop the more than one million dollars Ethereum miners spend on electricity each day to around $100,000 or just ten percent.

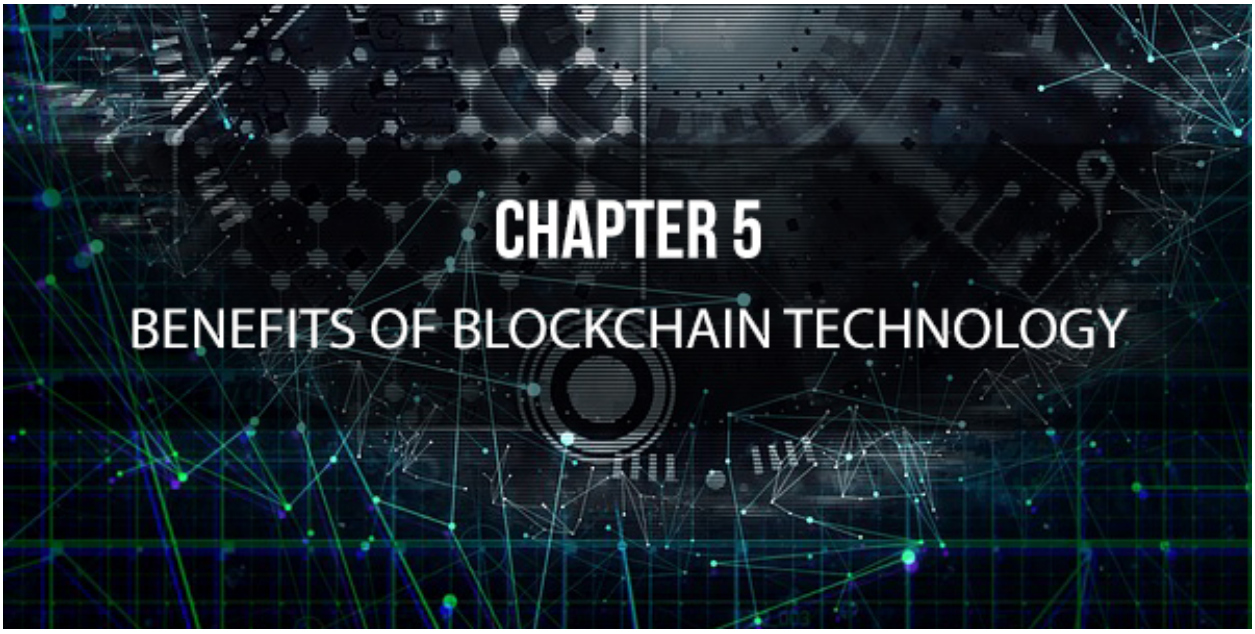
In addition to making it cheaper to mine cryptocurrency, the proof of stake model will also make it more unrestricted because it won't matter how fast the user's computer is because the calculations will be completed within the blockchain itself. As a bonus, this makes the 51 percent attack much more difficult to pull off successfully. A 51 percent attack happens when a group of miners comes together to control more than 51 percent of all nodes running a particular blockchain in an attempt to add completely false blocks to the system that the unaffected nodes will then accept as accurate because a majority of the nodes are already reporting it that way.

Proof of stake will also make it possible to ensure the validators stay honest by forcing them to be vested in the transactions that they verify because they know if they don’t play fair, they will lose their own money. Finally, the proof of stake model makes it easier to produce blocks faster than ever thanks to a process called sharding, which is the process of breaking a more extensive database down into more manageable pieces. When databases are broken down, it allows each piece to have its own set of validators who complete their own transactions within the shard. Once this occurs, it makes scalability more modular and even faster.

Proof of Stake Challenges

The new process won't be without its own share of issues. The first issue will be that the new system isn't guaranteed to work. This is because this type of model hasn't been put into play at a large scale before. This means that there is a chance that the original blockchain could be damaged if the transactions aren't processed as planned, or if a smart contract is miswritten. To combat this scenario, the Ethereum team is working on what is called the finality property. This will ensure that the current state of the blockchain will be secure before the new one can be implemented.

Chapter 5 – Benefits of Blockchain Technology



The promise of blockchain technology saw all of the world's contracts and agreements digitized into code and stored in public, transparent databases that are safe from being deleted, tampered with, or revised. The future will see every kind of agreement, business process, online task, funds payment, and transactions with a single digital record that can be identified and validated. As the technology continues to expand, we'll see middlemen, like lawyers, stock exchange brokers, and banks, saving billions, if not trillions of dollars every year.

Blockchain technology is ideally suited to revolutionizing the way many industries do business. Here are just some of the ways that blockchain technology will accomplish this.

Eliminating Third Parties

Blockchain technology will eradicate third parties and increase the number of exchanges that aren't subject to trust issues. Blockchain will allow two or more parties to conduct a transaction, of any type, without having to resort to official oversight or intermediation with an external party. This will significantly reduce, or even eliminate counterparty risks.

Counterparty risk is a risk that each party of a contract will face if the counterparty doesn't live up to their contractual obligations. It is a risk to both parties and is something that should always be considered when evaluating a contract.

Control Over Data

With blockchain, users are more empowered and have better control over their own data. With blockchain protocols in place, users own and are in control of all their information and transactions themselves. Uber is a perfect example of this. Uber is one of the world’s largest car services companies, but they don’t actually own any of the cars that run its business, but they rake in billions of dollars through car rides that are logged by drivers using the Uber app.

Better Data Quality and Integrity

With the blockchain technology, data is always complete because the next block can't be created or mined without being linked to a verified block being finished in the chain. It is also consistent because all the data has to conform to the protocol standards or else it won’t be recorded in the chain, as well as being widely available.

Durability and Reliability

Blockchain technology has been proven not to have a single point of failure and is capable of withstanding malicious exterior attacks more efficiently. This is compared to closed systems that contain possible weaknesses and point of failure that are scattered throughout the entire system from within.

The Integrity of Data Processing and Transfers

Due to the unchangeable nature of the blocks in a blockchain, every user on the network can trust that every transaction they make will take place on the network and that they will always be executed precisely as the system was designed. This removes the need for any third party to oversee the transactions,

maintaining the integrity of the data being processed and all transfers.

Transparency and Auditability

All transactions made to and on a blockchain are, by design, created on a public ledger that can be looked at by everyone. This creates a highly transparent system that can be searched by anyone. There are various services, such as etherscan.io, that allows users to search the vast databases and transactions in order to audit everything that is happening within and on a blockchain.

Faster Transactions

Transactions between banks, like ACH, (automated clearinghouse transactions) can take days to clear. This is especially true for transactions that are made outside of regular working hours. Just think about when you send a wire or make a purchase at the end of the business day on Friday. Without blockchains, you are unable to see any timely updates to the status of your funds. Often you aren't provided an update until the following Tuesday or Wednesday. Blockchain technology reduces the transaction times to minutes, and sometimes even seconds, and they are processed around the clock.

Lower Transaction Costs

With blockchains, no outside parties are overlooking the transactions. Because of this blockchains can potentially reduce the transaction fees significantly. With reduced transaction fees, it could possibly lead to billions of dollars being saved annually.

Chapter 6 – Risks and Challenges of Blockchain Technology

One of the major draws of blockchain technology is also one of its most significant challenges. Currently, there is very little regulation with regards to what is and isn't allowed in the blockchain space. Because of this, there have been numerous instances of hackers being able to make off with millions of dollars of investor money because of loopholes in the online blockchain systems. Despite the promise of security on the current blockchains, there are teething issues that hackers are taking advantage of to the detriment of every blockchain user.

Recently, there was a case with Enigma, a decentralized platform that was preparing to raise money through an ICO. Hackers were able to hack Enigma's website and numerous social accounts

successfully. This allowed the hackers to send out spam to Enigma's community and make off with almost $500,000. The Enigma project was launched by a group of MIT graduates, who sent out invites for people to join the Enigma community. The hackers grabbed money from those who joined the company's official mailing list and Slack group. In all, there were around 9,000 users and participants who were affected by this security breach.

The hacker's effectively posted messages on Slack altered the official website and spoofed emails to the community list to make it look like the company was making a formal request for money. Members of the community responded by sending money that was deposited directly into the hacker's crypto wallet.

Last year there was a similar hack but on a much larger scale. When the Decentralized Autonomous Organization or DAO that was built on Ethereum was hacked and resulted in a loss of $50 million to hackers.

The DAO was supposed to be a decentralized investment fund where decisions wouldn't rest on just a few partners, but rather anyone who invested in the fund would have a vote in which companies or projects the company should invest in. It was set up so that the more that you contributed, the more votes you got.

Since the fund was built to be distributed, no one could take the money and run. Unfortunately, due to human error and programming errors, hackers were able to exploit the system to receive a $50 million payday, which has of yet been recovered.

Another example of the challenges facing blockchain technology comes from a company called OneCoin. Recently, a company

known as Gnosis sold $12..5 million worth of a token called GNO in just over ten minutes. The sale was intended to pay for the development of an advanced prediction market. The initial coin offering, ICO, received rave reviews across the global press.

On that same day, a company called OneCoin, based in Mumbai, India, was in the middle of a sales pitch for its own digital currency when their offices were raided by financial enforcement officers. In the end, eighteen OneCoin reps were jailed, and more than $2 million in investor funds were seized. Multiple authorities describe OneCoin, which was being touted as the next bitcoin, as a Ponzi scheme. By the time the offices in Mumbai were raided, the company had already moved at least $350 million in scammed funds.

Since there are no checks and balances to govern the execution of ICOs, if you are going to invest in a coin, you need to ensure that you aren't investing in any random idea that could turn out to be a scam.

Major Hurdles of Blockchain

Currently, there are significant hurdles in the way of formally legalizing and regulating crypto trades. Similar challenges exist with market growth and adoption. Some of the issues surrounding blockchain include, what kinds of tax structures are right for

blockchain markets, how to trace and aggregate funds, and where will spending and income information come from and how it will be gathered. As long as these problems remain question marks on the policy boards of decision makers, widespread adoption of blockchain technology will be difficult.

However, there is some promise for the future of blockchain technology. South Korea and Japan have made significant advances recently that will allow for legal bitcoin transactions, and various applications have opened investment channels in the blockchain space to traditional investors. These advancements have led to an influx of funds to different blockchain companies, which, in turn, have been able to invest in growth, research, and the promotion of their particular blockchain services.

Risks of Blockchain Technology

As a new technology, resolving challenges like transaction speed, the verification process, and data limits are standing in the way of making blockchain widely adopted technology. The regulatory status of blockchain projects is also a risk of blockchain technology and is currently uncertain.

If financial institutions and governments don’t buy into the idea of blockchain technology, or if it is pushed away because of a lack of clear guidelines on how the industry should be regulated,

blockchain will never gain the widespread adoption that investors and experts are hoping for, leaving it to be a novelty idea and nothing more.

The mining of blocks is highly energy intensive and is becoming even more expensive with the creation of each new block on the chain. There may end up being a limit to how much miners are willing to continue to spend to solve mathematical puzzles in order to earn a few bitcoins as their reward.

There are also cybersecurity and integration concerns that will have to be addressed before the general public will be willing to entrust their personal data to a blockchain solution. This also goes for getting the go-ahead from any body of users or a Board of Directors in order to make significant changes to or even completely replacing an existing system.

Finally, there is the problem of social and cultural adoption of blockchain technology. Blockchain represents a complete shift to a decentralized network. This requires a significant buy-in of all users and operators on the network. Also, since it is such a significant development, it is not entirely understood by a majority of the population. Will all of these risks and hurdles, it may be several years before we see widespread adoption of blockchain solutions.

Chapter 7 – Deciding if Blockchain Technology is Right for You

The most common reasons that someone might consider an experiment with blockchain is a continuous desire to experiment with new technologies, a need for blockchain's timestamp technology or an interest in the many different ways blockchain can safeguard existing data. As with any new technology, it is essential that you look before you leap and consider if blockchain technology is really right for you and your business.

Know Who Will Be Looking at Your Data

In a majority of the traditional centralized databases, anyone with access to it has their activities stored in case they need to be reviewed later. If you need to have many individuals look at your

data on a regular basis, but don't want them to have write access to the data, then you may benefit from using a blockchain. Utilizing a blockchain in your business may help to streamline the process by providing users with read-only access in addition to a having a log in a more traditional sense when it is required.

Writeable Data

An average user database is generally protected through a mix of usernames and passwords, as well as several levels of restricted access. You can then implement even more security measures to prevent your high-level data from being accessed when it shouldn’t. Even with all of these precautions, it is still less than the standard blockchain security protocols that make it perfectly clear who created which blocks and the time and place they created those blocks.

These measures ensure that every transaction is always completed with the full knowledge of the creator, who can then confirm, and sign off on the transaction. This, of course, assumes that the individuals aren't adding information directly to the node. The signature is then further confirmed before the block can be attached to the chain. Even if a username and password combination is not required for users to have access, the chain will still automatically log the IP address of any user who creates new blocks.

Data Alteration

If you think that you are going to need to alter data that is being stored in a blockchain, then blockchain technology might not be right for you and your business. With a centralized database, its simple to alter data by merely tracking down the appropriate clearance, changing the required data, and having those changes saved in a log. With blockchain technology, the only way to do the same with data that has already been stored is to simultaneously change the data across 51 percent of the nodes that are available on the network. While this is a useful security feature of blockchains, in some scenarios, it will automatically disqualify blockchain databases from running in several others.

Data Restoration

If you find yourself doing nothing but updating backup data, then you might discover blockchain technology beneficial. When you use a traditional database, you have to instigate backups manually, leaving you to worry about making sure that everything is where it needs to be. On the other hand, when it comes to a distributed database, the information in it is automatically updated across all available nodes every time new information is added to the chain. As long as all of your nodes don't catastrophically fail at the same time, then you don't have anything to worry about.

Depending on the costs that are associated with backing up and updating all of your data, you may find that the additional operating expenses associated with a decentralized database may make it the cheaper of the two alternatives.

Easy to Share

Centralized databases are often limited concerning access, while a blockchain database can be temporarily connected to another blockchain database easily. This ability to connect to other blockchain databases makes the process of transferring information between the too, nearly painless.

The other blockchains that you are connecting to could be related to a specific department within your company, or even related to entirely different companies. If you are considering doing this, it is essential to keep in mind that when you give someone access to your blockchain, you are giving them access to your entire blockchain. This may require significant planning to effectively utilize if you deal with sensitive information.

Storage Limitations

One area where a traditional database beats a blockchain database is in the amount of data that can be comfortably stored.

When a new node is created in a decentralized database, the entirety of the blockchain is downloaded to it. This, along with the fact that nodes can be thousands and thousands of miles apart from one another, means that it is in your best interest to keep the total amount of data in your blockchain manageable. As a general point of reference, the database for bitcoin only has about 100 gigabytes, and it has been around for nearly ten years. If you need a high capacity option, you might need to look elsewhere.

Verification Process

If you are planning on running a private blockchain, then you don't need to worry about funding a reward for the validation of blocks. In fact, you won't even have to worry about a proof of work system at all. Instead, you will want to use a proof of stake model, because everyone in the private blockchain will have a stake in keeping the chain up-to-date and reliable. This means that the process for validating blocks can be more straightforward. However, you will still need to factor in the amount of time it will take to process and ensure that you have the workforce to facilitate the work.

Taking the Next Step

After analyzing the specifics, if you decide to take advantage of blockchain technology, it is crucial that you consider exactly how you plan to use the technology.

If you are an existing business owner, who hope to get ahead of the curve, then you'll want to focus your attention and energy on the potential ways that blockchain and smart technology can work together to improve the ancillary aspects of your business. More specifically, you'll want to take a long look at things that have the potential to decrease costs and improve efficiency.

This means that you will need to consider all the many ways that utilizing blockchain will make you more competitive in the eyes of your competition by allowing you to get a jump start on emerging trends in your industry.

Alternately, you will need to consider the various disruptions to the way your business works that implementing blockchain technology might bring to light.

This will require you to move things around now so that the disruptions you might experience are kept to a minimum. Being aware of what is likely to happen next will make it a lot easier to face head-on.

If you are considering forming a new business based around blockchain, then you'll want to work with as many different blockchains as possible. This will help you to improve your grasp of the technology, as well as to help to make the technology more mainstream, which is what is needed for new blockchain companies to take off.

If you hope to break into the mainstream with the help of blockchain, then you will want to do everything you can to ensure blockchain technology becomes mainstream.

You also want to keep in mind that it is, more than likely, going to be a tough road to travel. However, many of the most significant benefits of blockchain technology are only going to be available to companies who have an existing infrastructure already in place to take full advantage of them.

This means that the most realistic forecast for the rise of blockchain technology is that there will be a handful of companies that are going to come along and grab a share of the spotlight, leaving the rest of the room at the top being taken up by the members of the old guard who can get their acts together and make a move on blockchain technology before their competition.

Chapter 8 – Blockchain Implementation Mistakes to Avoid

With all the hype that surrounds blockchains, it can be easy to leap into the fray without looking at how to implement your own blockchain distribution system. This is a huge mistake. Before you can take the plunge, you need to make sure that you are avoiding the following errors.

Having Unrealistic Expectations

If you are planning on being able to use a blockchain efficiently, the first thing that you need to understand is that it is not a catchall solution to every problem. Fortunately, you can set up a

private system, and only a handful of people will have to know if the initial testing goes poorly.

This also goes for the amount of information that is routinely stored in each block. The bulk of the entire blockchain will ultimately be duplicated to each new node that is created, so an extremely bloated chain will be adding unnecessary bloat to all of the computers using the blockchain. It is essential to keep in mind that the entire bitcoin blockchain is only 55 gigs. While this is great when it comes to storing private databases securely, it is not the best choice when it comes to the usage of large-scale data. This these cases a centralized data storage system will be the better choice.

It is also important to remember, that while blockchain systems have numerous fail-safes in place to prevent user error, it doesn't mean that they are infallible. Since each block is only referred to by a hash key, it makes it much more likely for humans to mistake blocks for other blocks to everyone’s detriment. So, if you are going to utilize blockchains in your business, you need to be sure to implement a failsafe to check for this kind of thing to have the best results.

Underestimating the Time Commitment

It will take a lot of time to understand the intricacies of blockchain technology fully. If you plan on seeing the implementation of a blockchain system through to completion, you have to understand precisely how much time is required to learn to utilize blockchain technology to its fullest potential. After reading this book, you will still need to do more research to understand the best way for you to implement a blockchain that best serves the purposes of your business. This means that you will need to understand what you are going to be using blockchains for on a regular basis, but also what any secondary or tertiary duties might include.

Only after you have a clear idea of what you are going to be using the blockchain system for, you will be able to determine which kind of creation software is going to be right for you and your needs. The market for blockchain creation tools isn't crowded, which means you need to know exactly what you are looking for regarding finding one that is reliable and effective. Making a poor decision on this will make the creation process more difficult than it needs to be.

Being Impatient

After you have a clear understanding of how you are going to use your blockchain distributed database and how you are going to implement the blockchain, it is essential that you not hurry to

finish the process. When it comes to implementing blockchain technology you have to take things at a more measured pace. The process can be long and complicated, but you must follow it through to the letter as well as testing it thoroughly before you begin to rely on the blockchain in a real-world setting. Setting up a good blockchain takes time, and rushing will only cause you problems.

Keeping this in mind, it is vital that you decide on a timetable that accurately reflects how long it will take you to complete the project. You need to make sure that you consider the time that it will take to get buy-in from anyone else whose opinion is required before you can start the process.

Not Limiting Access

When it comes to exciting new technologies like blockchain, it's natural for numerous people to be interested in testing it out. If you are running a private blockchain, then it is crucial that you not let too many people have access until they've received proper training. Your fledgling blockchain can become easily derailed if you allow even a few inexperienced hands at the help. When it comes to accessing the core of the blockchain in a private system, you need to be sure to store the key for private access that is generated with a new blockchain in a safe location, because if it is lost, there will be no way for you to regain control of the blockchain.

Conclusion

There have been few discoveries and inventions over the course of history that have made long-lasting impacts on the direction and pace of human progress. Blockchain technology promises to be one such invention.

The promise that is holds for redefining air travel, ocean freight, and global logistics and what it can do to transform healthcare by providing safe and secure medical records, as well as the opportunities in the fields of microfinance, finance, credit investments, and prediction markets, suggests that the world is slowly waking up to what blockchain technology can do.

The capabilities of this emerging technology are still being determined, and there is still a lot of work that still needs to be

done. Millions of dollars in investments are being poured into this area of research and development, and every day we see new blockchain-based ideas, startups, and initiatives being launched, with each one hoping to be the one that will catch fire and transform the way things are done.

Now is the time for a change, and new blockchain technology is powering the drive to change. However, as we move forward, we need to take cautious steps to ensure that we use the technology in the right way and deliver as much benefit to as many people as possible.

If you are looking considering utilizing blockchain technology for your business, the only way that you will truly master it is if you dedicate yourself to becoming a lifelong learner in the space.