ENERGYXCHAIN

A Digital Technology Course

Transaction Management: An Overview of Digital Tools for Managing Complex Transactions

EnergyXchain, LLC 9319 Robert D Snyder Road, Suite 324 Charlotte, NC 28223 www.energyxchain.com

Transaction Management: An Overview of
Digital Tools for Managing Complex Transactions

Module 1: Blockchain Basics

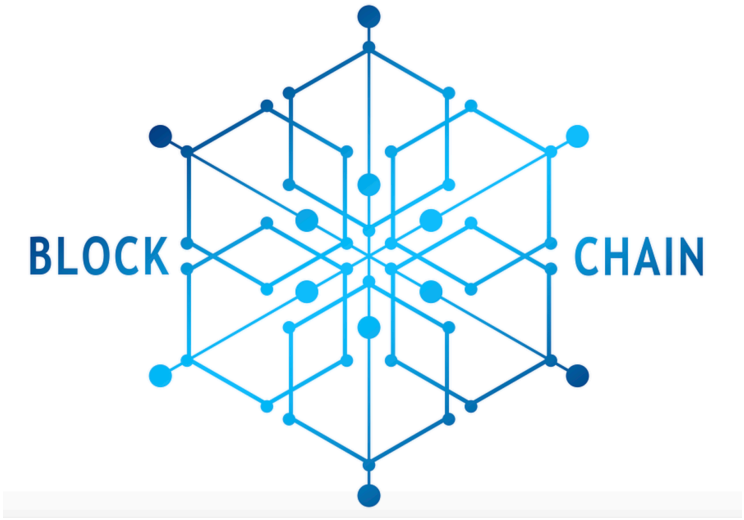
EnergyXchain, LLC 9319 Robert D Snyder Road, Suite 324 Charlotte, NC 28223 www.energyxchain.com

Module 1: Blockchain Basics (90 minutes)

Preliminaries

Blockchain seems complicated, and it definitely can be, but its core concepts are really quite simple. Blockchain boils down to just 3 simple things: *software, accounting and data storage*. These are all things we use every day on our smart phones, but blockchain just snaps these concepts together in a robust, secure way.

Blockchain and Distributed Ledger Technology (DLT) is simply the next step in the continual evolution of best business practices. We've progressed from locking data in file cabinets to storing data on a computer's hard drive to encrypting and storing data on the cloud. Blockchain is simply the next step in data storage. We've progressed from wearing green eye shades and writing data on ledger sheets to entering data on a PC's Excel spreadsheet to entering data in automated, cloud-based, accounting system, like Quickbooks. DLT is simply the next step in data accounting.



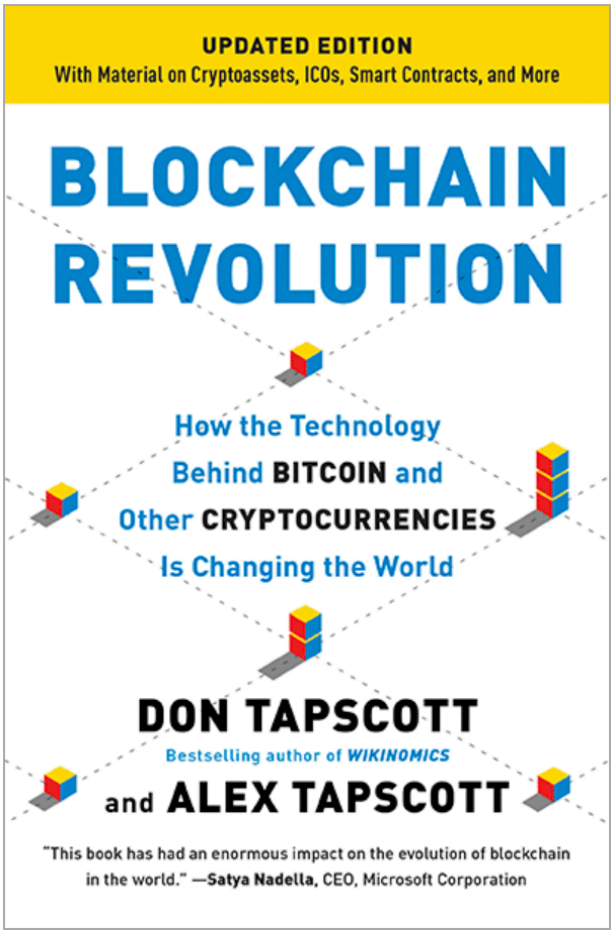
With the benefit of evolving best practices to the cloud comes some potential significant risks that Blockchain can eliminate. Since the internet boomed in the '90's we have seen more hacks and more stolen information than in previous generations. Blockchain can restore TRUST. Microsoft, Facebook, Marriott, Target, Equifax, Yahoo, BoA, and the US Government are just a few of the dozens of the large data repositories of data that have recently been hacked. More than 9000 breaches have been reported and 100's of millions of Americans have had their personal data compromised in just the past 10 years.

Since congress passed the CARES Act last summer, billions of dollars have been stolen by fraudsters filing false unemployment claims using stolen identities. Estimates are as high as $200 billion in employment fraud loss - and California may have as much as $50 billion of that total. Many victims are just finding this out as they file their 2020 tax returns. More than 40 million medical patient records were also stolen last year. These data hacks are increasing. Search for 'data breach' in your favorite search engine and you will see they're almost daily news.

How can Blockchain solve the issues described in this brief introduction?

No one explains Blockchain better than Don Tapscott - author of the *Blockchain Revolution* - a book I still recommend to everyone who asks me about blockchain.

- http://blockchain-revolution.com/order/



As a start on this 4 part digital blockchain course, we will begin with 7 minute overview Tapscott did for Lloyds Bank in 2018. This will set the stage for the next 4 weeks.

- https://www.youtube.com/watch?v=isuAPyuqS7Y

What is blockchain technology?

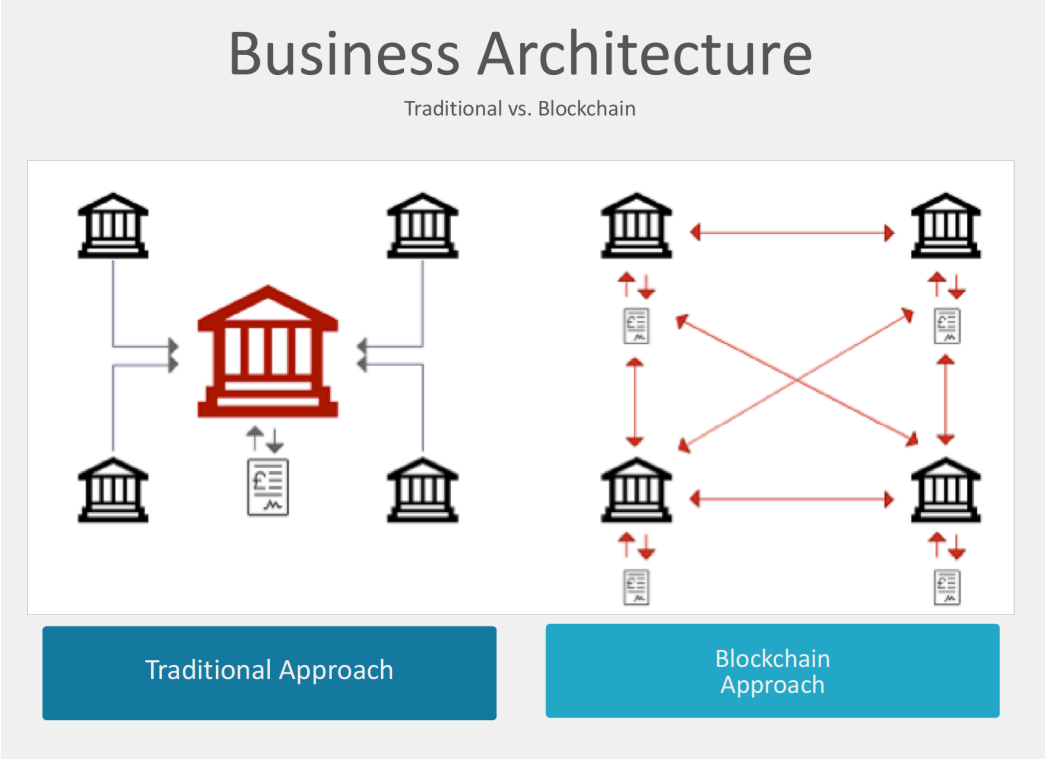
Blockchain is a type of database. To be able to understand blockchain, it helps to first understand what a database actually is.

A database is a collection of information that is stored electronically on a computer system. Information, or data, in databases is typically structured in table format to allow for easier searching and filtering for specific information. What is the difference between someone using a spreadsheet to store information rather than a database?

Spreadsheets are designed for one person, or a small group of people, to store and access limited amounts of information. In contrast, a database is designed to house significantly larger amounts of information that can be accessed, filtered, and manipulated quickly and easily by any number of users at once.

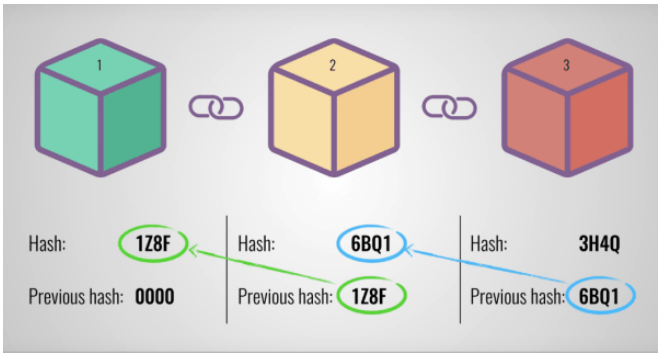
Large databases achieve this by housing data on servers that are made of powerful computers. These servers can sometimes be built using hundreds or thousands of interconnected, distributed computers, which today we call "the cloud" in order to have the computational power and storage capacity necessary for many users to access the database simultaneously. While a spreadsheet or database may be accessible to any number of people, it is often owned by a business, liked Amazon, Bank of America, Walmart, Target, etc. and managed by an appointed entity within that company individual that has complete control over how it works, and the data within it and customer and supplier access and use. We've all seen how our this data is used by these big companies to place targeted advertisements in our online path.

So how does a blockchain differ from a database?



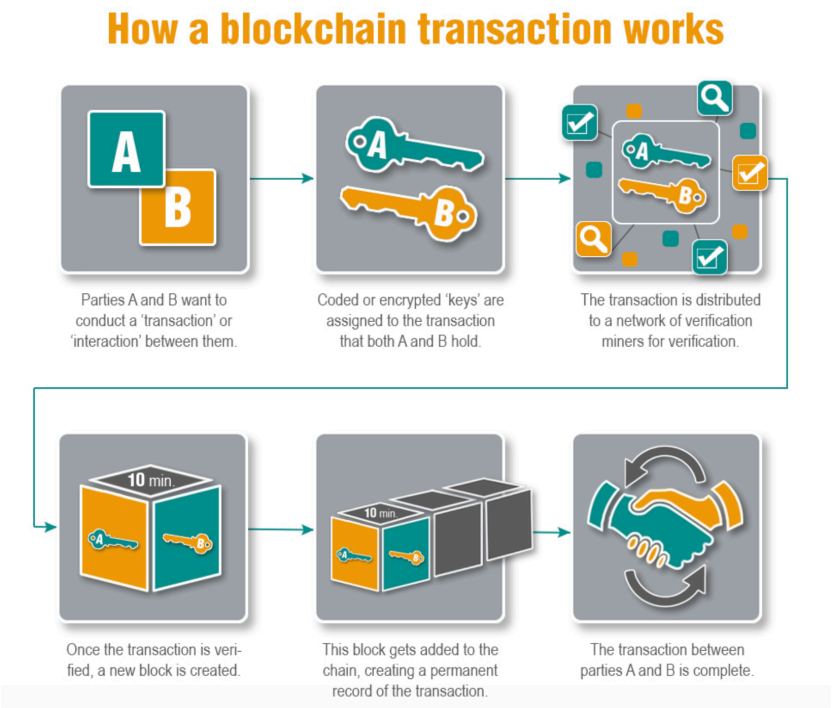
Storage Structure

One key difference between a typical database and a blockchain is the way the data is structured. A blockchain collects information together in groups, also known as blocks, that hold sets of information. Using the accounting analogy, a block may be thought of as a page in an accounting ledger. A page may have many entries which provide the details of a series of transactions. When the page is filled the accountant begins filling the next page in the ledger. A block has a certain storage capacity and, like the ledger page, when filled, is chained onto the previously filled block, forming a chain of data known as the "blockchain." All new information that follows that freshly added block is compiled into a newly formed block that will then also be added to the chain once filled. Each discrete piece of information stored in a block has a unique identifier, so that it can be found within the block and each block has an identifier called a "hash code" which include a time stamp.



A database structures its data into tables whereas a blockchain, like its name implies, structures its data into chunks (blocks) that are chained together. This makes it so that all blockchains are databases but not all databases are blockchains. This system also inherently makes an irreversible timeline of data when implemented in a decentralized nature. When a block is filled it is set in stone – becoming "indelible" and becomes a part of this timeline. Each block in the chain is given an exact timestamp when it is added to the chain.

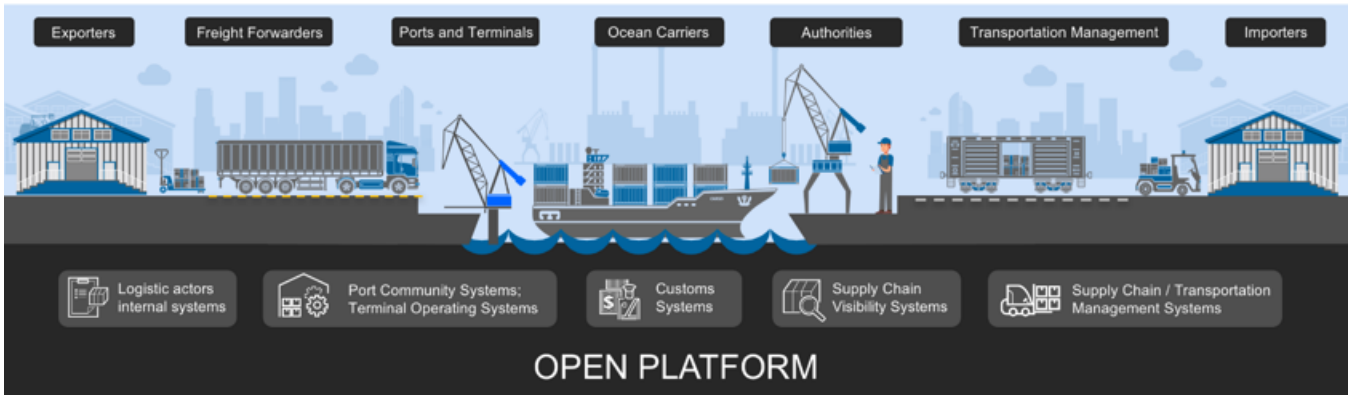
A block can contain any relevant data about a transaction. For example, data stored in a block documenting a natural gas transaction could include any or all of the following; buyer, seller, date, price, nominated volume, contract volume, receipt point, delivery point, firm v. interruptible, transaction start/end date/time, duration, quality specifications, payment provisions, bank routing information, credit limits, transaction managers, contract number and much more.



Decentralization

For the purpose of understanding blockchain, it is instructive to view it in the context of how it has been implemented by Maersk to manage shipping transactions. Maersk handles 1 in 7 containers shipped globally. Documentation and bureaucracy can be as much as a fifth of the total cost of moving a container. This project started with a few key partners in 2018 to detect opportunities to avoid delays caused by documentation errors.

Like when using a database, Maersk needs a collection of computers to store its blockchain. For Maersk, this blockchain is just a specific type of database that stores every Maersk transaction ever being made. In Maersk's case, and unlike most databases, these computers are not all under one roof, and each computer or group of computers is operated by a unique individual or group of individuals (Maersk customers and suppliers; its transaction parties).



Imagine that a company owns a server comprised of 10,000 computers with a database holding all of its client's account information. This company has a warehouse containing all of these computers under one roof and has full control of each of these computers and all the information contained within them. Similarly, the Maersk blockchain consists of thousands of computers, but each computer or group of computers that hold its blockchain is in a different geographic location and they are all operated by various global partners.

In this scenario, Maersk's blockchain is used in a decentralized way. However, private, centralized blockchains, where the computers that make up its network are owned and operated by a single entity, do exist. For private blockchains this approach can provide its users most of the blockchain benefits we have and will describe.

In a blockchain, each node (transaction party) has a full record of the data that has been stored on the blockchain since its inception. For Maersk, the data is the entire history of all Maersk transactions since adopting blockchain. If one node has an error in its data it can use the thousands of many other transaction party nodes as a reference point to correct itself. This way, no one node within the network can alter information held within it. Because of this, the history of transactions in each block that make up the blockchain is irreversible. Were a hacker to breach the security of one transaction party's computer system and manage to change the data in one block, which would be extraordinarily difficult, the block stored on all other transaction party nodes would flag that error.

This system helps to establish an exact and transparent order of events. For Maersk, this information is a list of transactions, but it also is possible for a blockchain to hold a variety of information like legal contracts, state identifications, or a company's product inventory.

In order to alter blockchain operation or the information stored within it, a majority of the decentralized network's nodes computing power would need to agree on said changes – there must be consensus. The consensus mechanism is built into the blockchain and is part of it. This ensures that whatever changes do occur to the blockchain, they are agreeable to all nodes (transaction parties).

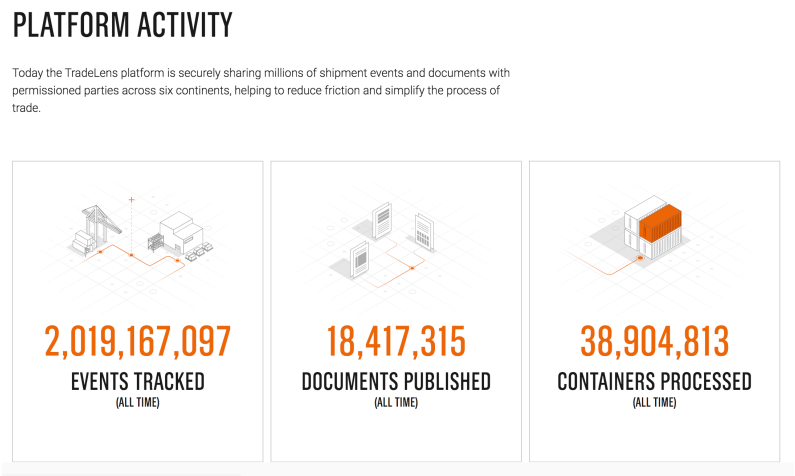
Transparency

Because of the decentralized nature of Maersk's blockchain, all transactions can be transparently viewed by either having a personal node or by using blockchain explorers that allow any authorized party to see transactions occurring live. Each node has its own copy of the chain that gets updated contemporaneously as fresh blocks are confirmed and added. This means that transaction parties can track in real time any aspect of the Maersk transactions which may involve them. They don't have to wait for Maersk to inform them of the status. Maersk saved early partners billions of dollars with transparent - near real time data.

TradeLens was officially announced to the world in 2019, and almost simultaneously, the TradeLens beta product and early adopter program were launched. ClearWay, the trade document module that was introduced under the beta program, enabled importers, exporters, and customs brokers as well as government agencies and NGOs to take part in data sharing and various business processes, which are all supported by a secure audit trail.

The Maersk and IBM blockchain initiative TradeLens managed to attract four out of the world's six largest ocean carriers. As of December 2019, the TradeLens platform could already boast of having more than 175 unique organizations in its team. Here is a quick overview of how the transparency of bills-of-lading looks on the blockchain-based TradeLens platform.

https://www.tradelens.com/marketplace/tradelens-ebl



Is Blockchain Secure?

Blockchain technology accounts for the issues of security and trust in several ways. First, new blocks are always stored linearly and chronologically. That is, they are always added to the "end" of the blockchain. If you take a look at Maersk blockchain, you'll see that each block has a position on the chain, called a "height" which is measured as of the start of the blockchain.

After a block has been added to the end of the blockchain, it is very difficult to go back and alter the contents of the block unless the transaction parties majority reached a consensus to do so. That's because each block contains its own hash, along with the hash of the block before it, as well as the previously mentioned time stamp. Hash codes are created by a math function that turns digital information into a string of numbers and letters. If that information is edited in any way, the hash code changes as well.

Here's why that's important to security. Let's say a hacker breaches a company computer system security, finds the company's blockchain, is able to access it and attempts wants to alter the blockchain and steal data. If they were to alter their own single copy, it would no longer align with everyone else's copy. Each time a change is made to any block that change is updated on the identical blockchains residing on the nodes of all transaction parties. When all other nodes cross-reference their copies against the altered data, the hacker's version of the blockchain would be cast away as illegitimate.

Perhaps an even more important security is the simple concept of *refresh rate*. Every blockchain data set refreshes across the network at some interval. The worldwide, public bitcoin network refreshes approximately every 20 minutes. Sometimes it takes less and sometimes it takes more. So a hacker would need to steal an identity and login as that stolen identity during the data refresh period. And in the time it takes to refresh - would need to change more than half of all the previous transactions that that identity had created over time.

Succeeding with such a hack would require that the hacker simultaneously control and alter at least 51% of the copies of the blockchain so that their new copy becomes the consensus copy. Such an attack would also require an immense amount of money and resources as they would need to redo all of the blocks in the blockchain, because all would now also have different timestamps and hash codes and all versions would need to be changed identically and simultaneously.

The larger the blockchain, the more difficult it becomes to hack. Due to the size of a blockchain network and how fast their transactions create new blocks makes the cost to accomplish such a feat insurmountable in relation to the value derived from stealing the target data. Not only would this be extremely expensive, but it would also likely be fruitless. Doing such a thing would not go unnoticed, as network members would see such drastic alterations to the blockchain. The transaction parties could quickly isolate the corrupt data, maintain the transaction integrity and would then "fork off" to a new version of the chain that has not been affected retaining transaction integrity.

Finally - no network is 100% secure. But blockchain networks have more built in security and have shown promise in many industries.

Bitcoin Transaction foster Blockchain Technology

The goal of blockchain is to allow digital information to be recorded and distributed, but not edited. Blockchain technology was first outlined in 1991 by Stuart Haber and W. Scott Stornetta, two researchers who wanted to implement a system where document timestamps could not be tampered with. But it wasn't until almost two decades later, with the launch of Bitcoin in January 2009, that blockchain had its first real-world application.

The Bitcoin protocol is built on a blockchain. In a research paper introducing the digital currency, Bitcoin's pseudonymous creator, Satoshi Nakamoto, referred to it as "a new electronic cash system that's fully peer-to-peer, with no trusted third party."

The key thing to understand here is that Bitcoin merely uses blockchain as a technology to transparently record a ledger of payments, but blockchain can, in theory, be used to immutably record any number of data points. As discussed above, this could be in the form of transactions, votes in an election, product inventories, state identifications, deeds to homes, and much more.

Currently, there is a vast variety of blockchain-based projects looking to implement blockchain in ways to help society other than just recording transactions. We will address these in the coming weeks. But one good example is that of blockchain being used as a way to vote in democratic elections. The nature of blockchain's immutability means that fraudulent voting would become far more difficult.

For example, a voting system could work such that each citizen of a country would be issued a single cryptographic token. Each candidate would then be given a specific wallet address, and the voters would send their token or crypto to whichever candidate's address they wish to vote for. The transparent and traceable nature of blockchain would eliminate the need for human vote counting as well as the ability of bad actors to tamper with physical ballots. Perhaps even more importantly, voters could guarantee that their vote was counted and correctly attributed to the candidate of their choice.

How does blockchain technology work?

6:30 min video overview from Centre for International Governance Innovation

- https://www.cigionline.org/multimedia/what-blockchain

Advantages of Blockchain

Accuracy of the Chain

Transactions on the blockchain network are approved by the network of transaction party computers. This removes almost all human involvement in the verification process, resulting in less human error and an accurate record of information. Even if a computer on the network were to make a computational mistake, the error would only be made to one copy of the blockchain. In order for that error to spread to the rest of the blockchain, that same error would need to be made by other transaction party's computers—a near impossibility for a private blockchain with multiple transaction parties.

Cost Reductions

Typically, consumers pay a bank to verify a transaction, a notary to sign a document, or a minister to perform a marriage. The natural gas industry employs many people to review, control and validate contracts, pricing, nominations, scheduling confirmations, accounting, imbalances, invoicing and payment. The industry doesn't charge its customer for this central control function, but there is a cost to all transaction parties in dollars, time and precision. Blockchain greatly reduces and in many instances eliminates the need for third-party verification and, with it, their associated costs. Business owners incur a small fee whenever they accept payments using credit cards, for example, because banks and payment processing companies have to process those transactions. A blockchain, on the other hand, employs distributed authority and has limited much lower cost than traditional transaction systems.

Decentralization

Blockchain does not store any of its information in a central location. Instead, the blockchain is copied and spread across the a network of transaction party computers. Whenever a new block is added to the blockchain, every computer on the network instantaneously updates its blockchain to reflect the change. By spreading that information across a network, rather than storing it in one central database, blockchain becomes more difficult to tamper with. If a copy of the blockchain fell into the hands of a hacker, only a single copy of the information, rather than the entire network, would be compromised and the tampered block would immediately be identified by the other nodes on the blockchain.

Efficient Transactions

Transactions by human intervention at a central authority can take up to a few days to settle. If you attempt to deposit a check on Friday evening, for example, you may not actually see funds in your account until Monday morning and may not be able to use those funds until Tuesday morning. Whereas financial institutions operate during certain business hours, five days a week, blockchain is working every moment - 24 hours a day, seven days a week, and 365 days a year. Transactions can

be completed in as little as a few ten minutes and can be considered secure and "indelible" shortly thereafter. The blockchain ignores times zones, holidays, extraordinary weather events, human illness and other factors that disrupt central control, human engaged business transactions; blockchain is always on duty.

Private Transactions

Many blockchain networks operate as public databases, meaning that anyone with an internet connection can view a list of the network's transaction history. Although users can access details about transactions, they cannot access identifying information about the users making those transactions. It is a common misperception that blockchain networks like bitcoin are anonymous, when in fact they are only confidential.

That is, when a user makes public transactions, their unique code called a public key, is recorded on the blockchain, rather than their personal information. If a person has made a Bitcoin purchase on an exchange that requires identification then the person's identity is still linked to their blockchain address, but a transaction, even when tied to a person's name, does not reveal any personal information.

Secure Transactions

Once a transaction is recorded, its authenticity must be verified by the blockchain network. In a public blockchain, thousands of computers on the blockchain rush to confirm that the details of the transaction are correct. After a computer has validated the transaction, it is added to the blockchain block. In a private blockchain the "consensus" process can be custom designed and could consist of a simple, automated, digital review and validation between the transaction parties that key transaction parameters conform to the transaction criteria previously agreed to by the parties (we'll discuss Smart Contracts on Day 2).

A block has a certain capacity (just like a ledger page) and the block remains "open" to accept more transaction data to be stored until the block fills. This can take a number of minutes, depending on the number of parties which are members of the particular blockchain and their transaction volume. Once the block is filled, it is ready to be recorded and added to the chain.

Each block on the blockchain contains its own unique hash, along with the unique hash of the block before it. When the information on a block is edited in any way, that block's hashcode changes—however, the hash code on the block after it would not. This discrepancy makes it extremely difficult for information on the blockchain to be changed without notice.

Coursera has some excellent blockchain resources and detailed look at creating blocks on the bitcoin blockchain. Links are included on the last page.

Transparency

Most public blockchains are entirely open-source software. This means that anyone and everyone can view its code. This gives auditors the ability to review blockchains for security. This also means that there is no real authority on which controls the blockchain's code or how it is edited. Because of this, anyone can suggest changes or upgrades to the system. If a majority of the network users agree that the new version of the code with the upgrade is sound and worthwhile then the blockchain can be updated.

Private blockchain's work entirely differently. Private blockchain's are organized by a single party. You can think in terms of a producer, pipeline, distributor or marketer with a high transaction volume that wishes to begin realizing the value of blockchain operation. The private blockchain originator can select certain of its functions it wishes to power with blockchain technology and implement the blockchain. The originator could keep the blockchain operation totally internal, linking with its customers and suppliers through their existing data interfaces. However, the originator could also introduce the use of the private blockchain to its customers and suppliers by offering them the use of an update transaction interface which looks and work much the same as what now exists, but is now powered by blockchain technology.

Disadvantages of Blockchain

While there are significant upsides to the blockchain, there are also significant challenges to its adoption. The roadblocks to the application of blockchain technology today are not just technical. The real challenges are political and regulatory, for the most part, to say nothing of the thousands of hours (read: money) of custom software design and back-end programming required to integrate blockchain to current business networks. Many companies have expensive and complex legacy transaction management systems. Many of these conform to industry standards or have been approved by industry certification organizations.

Blockchain solutions typically are not implemented on an enterprise scale, so a good deal of modular programming occurs to allow blockchain technology to be added as a component of an existing, enterprise-scale system. The National Science Foundation has funded EnergyXchain from 2019 through 2022 to develop modules that can be integrated with legacy systems (we'll talk more about that on Day 4).

Speed Inefficiency

The Bitcoin blockchain is an example of inefficient of blockchain design that can be typical of public blockchains. Bitcoin's "proof of work" system takes about ten minutes to add a new block to the blockchain. At that rate, it's estimated that the blockchain network can only manage about seven transactions per second (TPS). Although other cryptocurrencies such as Ethereum perform better than bitcoin, they are still limited. Solutions to this "public design/proof of work" consensus mechanism issue have been in development for years. There are currently blockchains that are

boasting over 30,000 transactions per second. Private blockchains take a custom approach to consensus and are extremely fast relative to public, "proof of work" blockchain designs.

Illegal Activity

Certain public blockchain networks allow for illegal trading and activity. The most cited example of blockchain being used for illicit transactions is probably the Silk Road, an online "dark web" drug marketplace operating from February 2011 until October 2013 when it was shut down by the FBI.

The website allowed users to browse the website without being tracked using the Tor browser and make illegal purchases in Bitcoin or other cryptocurrencies. Current U.S. regulations require financial service providers to obtain information about their customers when they open an account, verify the identity of each customer, and confirm that customers do not appear on any list of known or suspected terrorist organizations. This system can be seen as both a pro and a con. It gives anyone access to financial accounts but also allows criminals to more easily transact. Many have argued that the good uses of crypto, like banking the unbanked world, outweigh the bad uses of cryptocurrency, especially when most illegal activity is still accomplished through untraceable cash.

Regulation

Governments have increasingly become interested in regulating cryptocurrencies both to curb its use in supporting illegal activities, but also to capture tax revenue from cryptocurrency-based transactions. Because no party manages and controls a public blockchain network, regulation is difficult. Theoretically governments could make it illegal to own cryptocurrency ownership or participate in their networks illegal. Such actions have not seriously advanced and over time this concern has grown smaller as large companies like PayPal, Fidelity and Morgan Stanley have started to allow the ownership and use of cryptocurrencies on their platforms.

Today a few ETF's are available for every-day investors to participate in the cryptocurrency markets through common vehicles like IRA's or retirement accounts. Tesla has announced that you will be able to buy your next electric vehicle using bitcoin. Tesla also bought $1.5 billion bitcoin recently. Square has bought over $200 million of the cryptocurrency. Cathie Wood of ARK Investments believes that more corporations will deploy their available investment cash into bitcoin.

The bottom line is that we can expect more regulation in the years to come.

Discussion - Q&A Day 1

Useful blockchain links

Don Tapscott

Blockchain Revolution -

- https://www.amazon.com/Blockchain-Revolution-Technology-Changing-Business/dp/1101980133/ref=tmm_hrd_swatch_0?_encoding=UTF8&qid=&sr=

Code Tech class

- https://www.youtube.com/watch?v=qOVAbKKSH10

Coursera class

- https://www.coursera.org/learn/blockchain-foundations-and-use-cases

Maersk and IBM

- https://www.reuters.com/article/us-maersk-blockchain-ibm/maersk-ibm-to-launch-blockchain-based-platform-for-global-trade-idUSKBN1F51DE
- https://pixelplex.io/blog/maersk-ibm-tradelens-blockchain-supply-management/
- https://www.tradelens.com/