Module 5- BlockChain

Module Overview

This module aims explaining Blockchain, Bitcoin and other concepts that record transactions.

Module Objective

At the end of the module, you will be able,

- Understand Basic of Bitcoin
- Learn about BlockChain, Ethereum
- Explore different Use cases and Applications of BlockChain

Bitcoin

The 2008 financial crisis caused a lot of people to lose trust in banks as trusted third parties. Many questioned whether banks were the best guardians of the global financial system. Bad investment decisions by major banks had proved catastrophic, with rippling consequences.

Bitcoin — also proposed in 2008 — presented an alternative.

Bitcoin is a decentralized, public ledger. There is no trusted third party controlling the ledger. Anyone with bitcoin can participate in the network, send and receive bitcoin, and even hold a copy of this ledger if they want to. In that sense, the ledger is “trustless” and transparent.

The Bitcoin ledger tracks a single asset: bitcoin.

Note: “Bitcoin” capitalized refers to the Bitcoin ledger, or protocol, while “bitcoin” in lowercase refers to the currency or a unit of account on the Bitcoin ledger.

The ledger has rules encoded into it, one of which states that there will only ever be 21M bitcoin produced. Because of this cap on the number of bitcoins in circulation, which will eventually be reached, bitcoin is inherently resistant to inflation. That means that more bitcoin can’t be printed at a whim and reduce the overall value of the currency.

All participants must agree to the ledger’s rules in order to use it.

Bitcoin is politically decentralized — no single entity runs bitcoin — but centralized from a data standpoint — all participants (nodes) agree on the state of the ledger and its rules.

A bitcoin or a transaction can't be changed, erased, copied, or forged – everybody would know.

Example: The Story of Alice and Bob

To understand better how this peer-to-peer electronic cash system allows for online payments to move from one party to another without going through a financial institution, let's use a simple example.

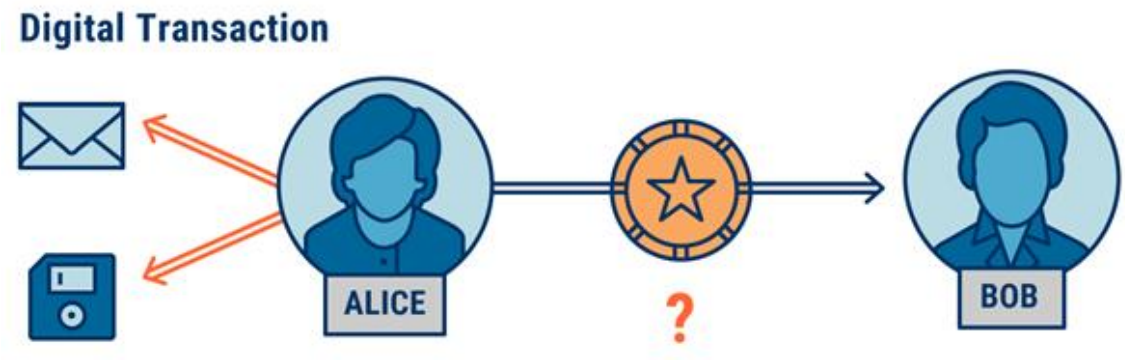
Here's a scenario:

Alice hands Bob a physical arcade token. Bob now has one token, and Alice has zero. The transaction is complete. Alice and Bob do not need an intermediary to verify the transaction. Alice can't give Charlie the same token, because she no longer has the token to give — she gave it to Bob.

But what if the same transaction were digital? Alice sends Bob a digital arcade token — via email, for example. Bob should have the digital token, and Alice should not.

Right?

Not so fast. What if Alice made copies or "forgeries" of the digital token? What if Alice put the same digital token online for all to download? After all, a digital token is a string of ones and zeros.



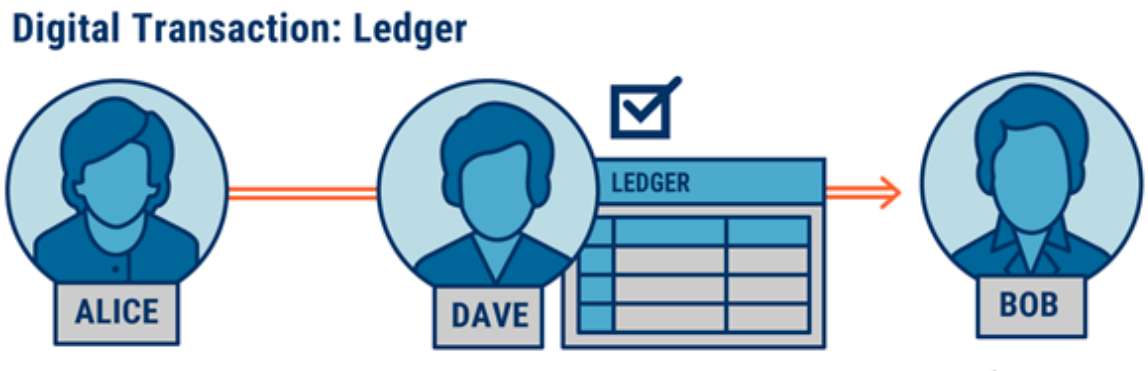
If Alice and Bob "own" the same string of ones and zeros, who is the true owner of the digital token? If digital assets can be reproduced so easily, what stops Alice from trying to "spend" the same digital asset twice by also sending it to Charlie?

One answer: use a database — a ledger. This ledger will track a single asset: digital arcade tokens. When Alice gives Bob the digital token, the ledger records the transaction. Bob has the token, and Alice does not.

Now, they face a new problem: whose job will it be to hold the ledger? Alice can't hold it because she might erase the transaction and say that she still owns the digital token, even though she gave it to Bob. It also can't be Bob, because he could alter the transaction and lie to say that Alice gave him two tokens, doubling his arcade time.

Bob and Alice can solve this problem by using a trusted third party, an intermediary who is not involved in the transaction at all — let's call him Dave. Dave will hold the ledger and make sure that it's up-to-date.

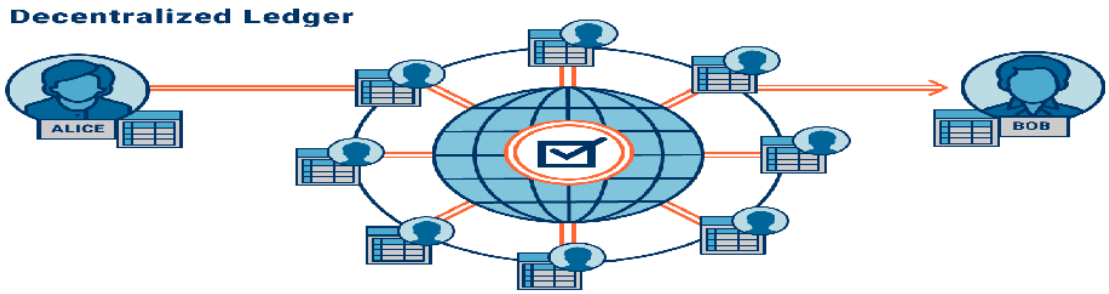
This situation is fine — until it's not.



Alternate Solutions to the previous example:

Think back to the first physical transaction between Alice and Bob. Is there a way to make digital transactions look more like that?

Here's a thought: Alice and Bob could distribute the ledger to all their trusted friends, not just Dave, and decentralize trust. Because the ledger is digital, all copies of the ledger could sync together. If a simple majority of participants agree that the transaction is valid (e.g. confirm that Alice actually owns the token she wants to send), it gets added to the ledger.



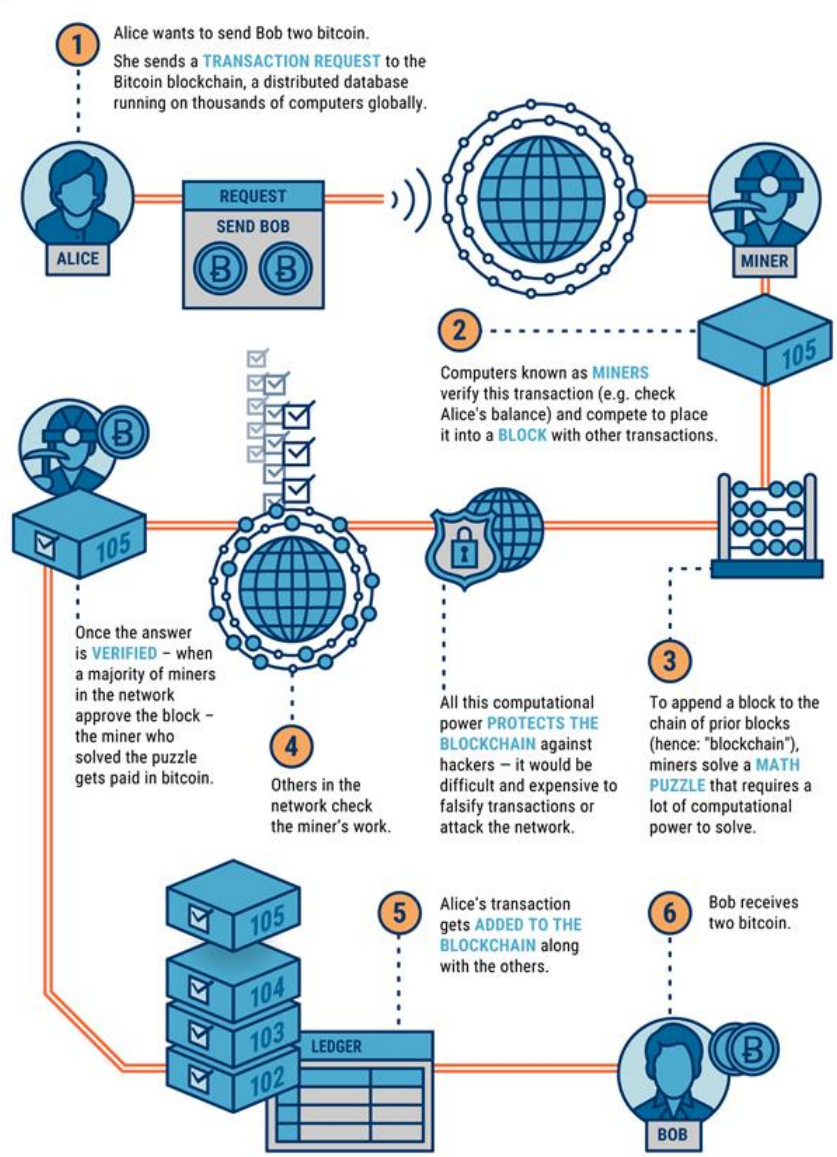
When a lot of people have a copy of the same ledger, it becomes more difficult to cheat. If Alice or Bob wanted to falsify a transaction, they would have to compromise the majority of participants, which is much harder than compromising a single participant.

Alice can't claim that she never sent a digital token to Bob — her ledger would not agree with everyone else's. Bob couldn't claim that Alice gave him two tokens — his ledger would be out of sync. And even if Alice bribes Dave to change his copy of the ledger, Dave only holds a single copy of the ledger; the majority opinion would show the digital token was sent.

In sum, this distributed ledger works because everyone is holding a copy of the same digital ledger. The more trusted people that hold the ledger, the stronger it becomes.

Such a ledger allows Alice to send a digital token to Bob without going through Dave. In a sense she is transforming her digital transaction into something that looks more like a physical one in the real world, where ownership and scarcity of an asset is tangible and obvious.

How Blockchain Technology powers Bitcoin?



Blockchain

The first, Alice's and Bob's distributed ledger for digital arcade tokens, is private.

The second, Bitcoin's decentralized ledger for bitcoin, is public. Anyone can participate. To ensure its public, decentralized ledger remains secure, Bitcoin uses a blockchain.

If we were to define "blockchain" as a technology separate from Bitcoin, it might look something like this:

Blockchain technology offers a way for untrusted parties to reach agreement (consensus) on a common digital history. A common digital history is important because digital assets and transactions are in theory easily faked and/or duplicated. Blockchain technology solves this problem without using a trusted intermediary.

Let's think about why Bitcoin needs blockchain technology. There are three main reasons.

- Bitcoin is a public ledger of bitcoin transactions
- There are untrusted nodes recording transactions on the Bitcoin ledger
- Bitcoin does not want to trust a third party to administer the ledger

Effectively, Bitcoin uses a blockchain to decentralize payments.

Where else could we use this unique database architecture to get rid of the middleman?

Are there other things that would be more valuable if they were decentralized?

Let's take this step-by-step. What's another scenario where everyone needs a record of ownership, and where a trusted third party isn't preferred?

A couple of immediate use cases come to mind.

Land title is one. It could be quite useful for everyone to have access to a decentralized source of record saying who owns a given parcel of land.

Considering that coups and wars often redistribute land unfairly and/or incorrectly, this could not only prove useful: it could also have humanitarian implications. Once a land distribution is agreed upon, it can be recorded in a distributed ledger and no longer be subject to ongoing debate. A number of companies are working on this, including velox.RE.

In the same vein, a blockchain could be used to establish ownership over any number of physical assets — cars, art, musical instruments, and so on. A paper record of title is prone to forgery and/or physical degradation. Centralized databases are prone to hacking, human error, and/or tampering. A blockchain means there is no single entity controlling the ledger. Therefore, recording physical assets on a blockchain is a prime example of where the technology might come in handy to track ownership with a tamper-proof, neutral, and resilient system.

Taking this one step further, blockchain technology could even prove applicable in virtual reality. If a virtual world is created — for gaming, or for any number of other reasons — blockchain technology could allow users to purchase and own pieces of that virtual world, just like they might purchase a plot of land.

Where does distributed ledger technology make sense?

We mentioned that Alice's and Bob's private implementation — where everyone knows and trusts everyone involved — doesn't need a blockchain (nor does it need miners to verify and append transactions to the cryptographically-protected blockchain).

Without the blockchain's verification step, we're left with a "distributed ledger," or a decentralized spreadsheet that is only accessible to a select group of trusted parties. Because this ledger is private, it doesn't need the same security measures as the blockchain.

The hype around Bitcoin, blockchain, and cryptocurrencies has contributed to renewed interest in distributed ledger technology. This is the idea of distributing a database among participants to ensure a common record of truth. Bitcoin uses distributed ledger technology and adds a consensus layer on top — the blockchain.

Because Alice and Bob's participants are trusted and their ledger is private, Bitcoin's blockchain isn't needed. In fact, a blockchain might prove unwieldy, slow, and overly complex for Alice and Bob's ledger, for reasons which we'll address below. Instead, a trusted third party could be used to lightly administer a distributed ledger.

Bitcoin and Ethereum (which we'll dive into below) are considered public, "permissionless" blockchains: anyone can access them. On the other hand, if all parties are known and trusted, distributed ledger technology could provide sufficient security. One example of distributed ledger technology is R3's Corda, which is working with major financial services organizations to improve banking processes.

While distributed ledger technology and blockchain technology each have their own pros and cons, the important thing to remember here is that blockchain technology is not a cure-all. For Bitcoin, a public, permissionless blockchain is the only possible solution. In many other instances, a blockchain would be a terrible idea.

Major issues with Blockchain Technology

Blockchain technology is really good at some things and absolutely awful at others.

The three major questions about blockchain technology concern its scalability, its anonymity, and its economical viability.

IS BLOCKCHAIN SCALABLE?

For a blockchain to work, lots of participants need to hold up-to-date copies. This means that the same database is held by thousands of nodes. This is fairly inefficient.

If we were to look at how technology has developed over the past fifteen years, blockchain runs counter to the logic behind cloud computing. Cloud computing trends toward a single database that multiple nodes can access. These nodes don't have to hold their own private copy of this database.

Further, nodes holding copies of the blockchain receive constant updates. These nodes are distributed around the world. Because of this, blockchains have high latency (latency is the amount of time it takes for data to move through the network).

As a result, blockchain technology faces scaling issues. Bitcoin can process about 4-5 transactions per second. Ethereum maxes out at about 25 transactions per second. Visa can process over 24,000 transactions per second.

IS BLOCKCHAIN ANONYMOUS?

In the early days of Bitcoin, blockchain technology — like many nascent technologies — was popularly associated with illicit activities.

Why was blockchain technology like Bitcoin effective for this kind of enterprise? Even though Bitcoin's record of transactions is publicly available, the network's global, decentralized nature means that no single entity — like the US government or Visa — can shut it down, freeze funds, or reverse transactions. And in those early days, it was very hard to link a Bitcoin wallet to a given individual, even if there was evidence that the wallet was used in illicit activities.

One of the reasons why Bitcoin has gained more mainstream popularity as a store of value and financial instrument is that it's no longer as anonymous as it was in those early days. Most major services that allow you to buy and sell Bitcoin use "know your customer" (KYC) standards, and law enforcement agencies have gotten more adept at linking Bitcoin transactions to specific people. There are other projects that have emerged in an effort to use blockchain technology to protect user anonymity (e.g. Monero and ZCash), but these are significantly less mainstream.

IS BLOCKCHAIN ECONOMICAL?

One of the keys to blockchain technology being viable in the long-run is making sure that transactions like Alice and Bob's can be executed with minimal fees. Fees are important because they incentivize miners to add your transactions to the blockchain in a timely manner — but high fees make it harder to convince potential users to get on board.

In December 2017, the median transaction fee on the Bitcoin network peaked at $34 per transaction. Companies like Stripe and Valve announced they would no longer accept Bitcoin payments due to high fees.

Today, the median transaction size on the Bitcoin network is about $300, while the median transaction fee wavers around $0.10 — that's a 0.03% median transaction fee, much better than the 0.7% fees of its peak.

Though the fees have come down, Bitcoin is still not capable of everyday commerce — the platform would have to solve issues with scaling, transaction block time, and more before it's ready for the big leagues.

Ethereum

We asked earlier what other applications could be built with blockchain technology.

Recall that Bitcoin is, effectively, a decentralized application for payments. Ethereum adds another layer by allowing users to put code on its blockchain that executes automatically. This code is called a "smart contract." In this way, Ethereum hopes to create a decentralized computing platform — a global supercomputer.

What is a smart contract?

To illustrate a smart contract, let's say Alice and Bob enter into a bet.

Alice thinks that the temperature tomorrow morning will reach 70 degrees. Bob thinks that it will stay lower. They wager 10 bitcoin on the outcome. If Alice and Bob don't trust each other, they will have to use a trusted third party as an escrow agent. In other words, they will each have to give the agent that amount of bitcoin, and the agent will distribute the winnings and the amount staked to the winner.

There's no way around the middleman in this scenario, even using bitcoin.

Ethereum, though, offers a decentralized solution. Alice and Bob could agree to use some basic code — a contract of sorts — to alert the system to what the temperature ended up being and pay out based on who was correct. If the temperature goes higher than 70 degrees, the code pays Alice,

otherwise, it pays Bob. Alice and Bob could then place this code (their bet) on Ethereum's blockchain.

This looks like a "contract," because all participants in the Ethereum blockchain hold a copy of this agreement. Just like the Bitcoin blockchain knows that Alice sent Bob a bitcoin (in our example above), the Ethereum blockchain knows that Alice and Bob have entered into an agreement. Therefore, this contract is self-enforcing.

Smart contracts like these are what make Ethereum so compelling. Because Ethereum is a blockchain, it's very hard to attack, change, or forge these smart contracts, just like it's economically self-defeating to attack Bitcoin.

What is Ethereum?

A smart contract allowed Alice and Bob to build a very small decentralized application. What if we could build larger and more complex decentralized applications?

Ethereum wants to be the platform on which these decentralized applications are built.

Recall that Bitcoin is a very simple decentralized application, for payments. Ethereum builds on Bitcoin by incorporating robust computing capabilities and smart contracts. In simple terms, this means that developers can use more complex code to build decentralized applications on top of Ethereum. These apps would be less error prone, more neutral, and more transparent. They would have lower administrative costs and greater built-in security.

Why is the price of Ethereum so high?

Ethereum's blockchain allows for the creation of a decentralized supercomputer. This supercomputer is the first one of its kind.

Computational power is limited, and developers pay with ether to use the Ethereum blockchain. Users also buy and spend ether to interact with its various decentralized applications. For example, CryptoKitties is a popular app built on top of the Ethereum blockchain that allows individuals to buy collectible cartoon cats. In order to purchase a CryptoKitty, you have to use ether.

Ether's dollar value is subject to supply-and-demand — if investors find the Ethereum blockchain valuable, and developers are building valuable decentralized applications on top of the platform that require the use of ether, then demand might rise and the price of ether could rise. The opposite can also happen.

As more and more applications are built on Ethereum, the demand for ether has gone up, driving up the price of the token. However, the price of the coin has fallen nearly 85% since its peak.

What are initial coin offerings?

We've now discussed Bitcoin and Ethereum. Both blockchains use a "token" that provides utility. Bitcoin uses bitcoin, while Ethereum uses ether.

Remember how we mentioned other decentralized applications?

An initial coin offering is a way for these applications to raise money. Instead of going the traditional venture capital route, a team could announce that — just like bitcoin or ether — it's issuing a token.

That token might do any number of things. Most of the time, it provides some sort of access to the decentralized application, in the same way that bitcoin provides access to the Bitcoin blockchain (like if you want to send a payment across the globe).

If a team issued a token for a decentralized social media platform, the team could mandate that a user needs to hold a token to access the platform. If demand for the platform goes up, then the token might rise in value.

So, an ICO is simply:

- The sale of tokens by a blockchain company looking to raise funds.
- These tokens are often subsequently traded on cryptocurrency exchanges.

Bitcoin Cash

Bitcoin Cash is not the same thing as Bitcoin, although it shares much of its history with that protocol.

Bitcoin Cash is a new network that "forked" from the Bitcoin network at the beginning of August 2017. In the blockchain space, a "fork" is what happens when developers in the network decide to materially change the code of the platform. Nodes, run by miners, can update to the new code — if enough nodes make the switch, it can become a completely new platform with its own token.

When a significant number of nodes running a protocol like Bitcoin agree to update to a new and significantly different software, it creates a new blockchain that (1) has the same history as the previous protocol leading up to the fork but (2) has a different history than the previous protocol following the fork.

Last year, a group of developers came to an agreement that the Bitcoin protocol was straying from what they saw as its primary function: serving as a ubiquitous, low-fee, fast-execution, peer-to-peer means of transferring value.

They decided to fork Bitcoin in order to create a new cryptocurrency, Bitcoin Cash, that would be solely focused on serving as that kind of value transfer.

Litecoin

Another altcoin that's gradually entered the popular vernacular is Litecoin. It was invented in 2011 by former Google engineer Charlie Lee to act as cheaper and faster version of Bitcoin. It's a lower-priced cryptocurrency that's almost identical to Bitcoin — there are just a few minor tweaks that are intended to make it a more fitting tool for daily commerce.

In May 2017, Litecoin was listed on Coinbase, where Lee was a head engineer. It instantly became the fourth most valuable cryptocurrency in the world, and prices jumped 25% overnight.

Litecoin vs. Bitcoin: what's the difference?

Litecoin has an intended function that's identical to Bitcoin Cash, but with a different origin story. Both of these cryptocurrencies are designed for small, daily transactions, but Bitcoin Cash forked from Bitcoin while Litecoin was early spinoff that never relied on the Bitcoin blockchain — which probably explains why it isn't as controversial.

There are a couple of key differences between Litecoin and Bitcoin:

- Litecoin has a different "hashing algorithm" than Bitcoin. This basically means that the kind of computational process that miners use to add new blocks in the blockchain is different.
- The upshot of this is that there are fewer highly specialized Litecoin mining pools than there are Bitcoin mining pools, making it more accessible for the population at large to mine (although specialized Litecoin-mining computers are now on the rise).
- Litecoin is faster than Bitcoin. The altcoin adds new blocks added to its blockchain roughly every 2.5 minutes, in contrast to Bitcoin's 10 minute block frequency. In practice, this means that transactions can be confirmed more quickly on Litecoin than on Bitcoin.

Application and Use Cases of Blockchain

Blockchain technology is a revolution in systems of record. Let us understand application and use case for Blockchain:

As a system of record

Digital identity

Cryptographic keys in the hands of individuals allow for new ownership rights and a basis to form interesting digital relationships. Because it is not based on accounts and permissions associated with accounts, because it is a push transaction, and because ownership of private keys is ownership of the digital asset, this places a new and secure way to manage identity in the digital world that avoids exposing users to sharing too much vulnerable personal information.

Tokenization

For the purposes of authenticating a unique physical item, the items are paired with a corresponding digital token. This essentially means tokens are used as to bind the physical and digital worlds. These digital tokens are useful for supply chain management, intellectual property, and anti-counterfeiting and fraud detection.

For Governments

Governments have an interest in all three aspects components of blockchain technology.

Firstly, there's the ownership rights surrounding cryptographic key possession, revocation, generation, replacement, or loss.

They also have an interest in who can act as part of a blockchain network.

And they have an interest in blockchain protocols as they authorize transactions, as governments often regulate transaction authorization through compliance regimes (eg stock market regulators authorize the format of market exchange trades).

For this reason, regulatory compliance is seen as a business opportunity by many blockchain developers.

For audit trails

Using the client-server infrastructure, banks and other large institutions that help individuals form digital relationships over the internet are forced to secure the account information they hold on users against hackers.

While banks can spend the billions of dollars to keep information secure, the system is currently asking businesses to do the same. We are sharing the same information with these businesses as we are with the banks, after all. Yet, businesses are under attack and have been hacked, resulting sometimes in the exposure of customers' intimate financial details.

Blockchain technology offers a means to automatically create a record of who has accessed information or records, and to set controls on permissions required to see information. This also has important implications for health records.

As a platform

For smart contracting

Blockchains are where digital relationships are being formed and secured.

A consortium of the largest banks in the world, as well as several insurance companies, led by a startup, is seeking to build a platform to establish new digital relationships between banks themselves. In short, this version of smart contracts seeks to use information and documents stored in blockchains to support complex legal agreements.

As ethereum's primary purpose is to be a platform for smart contract code, comprising of programs controlling blockchain assets, executed by a blockchain protocol, and in this case running on the ethereum network.

For automated governance

Bitcoin itself is an example of automated governance, or a DAO (decentralized autonomous organization). It, and other projects, remain experiments in governance, and much research is missing on this subject.

For markets

Another way to think of cryptocurrency is as a digital bearer bond.

This simply means establishing a digitally unique identity for keys to control code that can express particular ownership rights (eg it can be owned or can own other things). These tokens mean that ownership of code can come to represent a stock, a physical item or any other asset.

Rules on how these instruments can be transacted can be coded by a blockchain protocol.

For automating regulatory compliance

Beyond just being a trusted repository of information, blockchain technology could enable regulatory compliance in code form – in other words, how blocks are made valid could be a translation of government legal prose into digital code.

In the case of banks, for example, this could mean improving efficiency in anti-money laundering (AML) compliance. Blockchain technology can be calibrated to do different things – permit transactions or report transactions of a certain type according to exact rules.

This means that banks could automate regulatory reporting or transaction authorization.

Blockchain Issues and Limitations

The issues and limitations of Blockchain are as follows:

Complexity

Blockchain technology involves an entirely new vocabulary.

It has made cryptography more mainstream, but the highly specialized industry is chock-full of jargon. Thankfully, there are several efforts at providing glossaries and indexes that are thorough and easy to understand.

Network size

Blockchains (like all distributed systems) are not so much resistant to bad actors as they are 'antifragile' – that is, they respond to attacks and grow stronger.

This requires a large network of users, however. If a blockchain is not a robust network with a widely distributed grid of nodes, it becomes more difficult to reap the full benefit.

There is some discussion and debate about whether this a fatal flaw for some permissioned blockchain projects.

Transaction costs, network speed

Bitcoin currently has notable transaction costs after being touted as 'near free' for the first few years of its existence.

As of late 2016, it can only process about seven transactions per second, and each transaction costs about $0.20 and can only store 80 bytes of data.

There's also the politically charged aspect of using the bitcoin blockchain, not for transactions, but as a store of information. This is the question of ''bloating' and is often frowned upon because it forces miners to perpetually reprocess and rerecord the information.

Human error

If a blockchain is used as a database, the information going into the database needs to be of high quality. The data stored on a blockchain is not inherently trustworthy, so events need to be recorded accurately in the first place.

The phrase 'garbage in, garbage out' holds true in a blockchain system of record, just as with a centralized database.

Unavoidable security flaw

There is one notable security flaw in bitcoin and other blockchains: if more than half of the computers working as nodes to service the network tell a lie, the lie will become the truth. This is called a '51% attack' and was highlighted by Satoshi Nakamoto when he launched bitcoin.

For this reason, bitcoin mining pools are monitored closely by the community, ensuring no one unknowingly gains such network influence.

Politics

Because blockchain protocols offer an opportunity to digitize governance models, and because miners are essentially forming another type of incentivized governance model, there have been ample opportunities for public disagreements between different community sectors.

These disagreements are a notable feature of the blockchain industry and are expressed most clearly around the question or event of 'forking' a blockchain, a process that involves updating the blockchain protocol when a majority of a blockchain's users have agreed to it.

These debates can be very technical, and sometimes heated, but are informative for those interested in the mixture of democracy, consensus and new opportunities for governance experimentation that blockchain technology is opening up.

Trainer will take the participants to the computer lab and ask the participants to do internet research on Blockchain Case Studies.
