Menu

LearnThings.Online

News Coures Search

LearnThings.Online

Subscribe

Blockchain: Understanding Its Uses and Implications – Chapter 3. Blockchain Problem Solving

This course is from edX

Scroll down click “Read More” to check original post on edX.

Syllabus

Welcome & Introduction

Chapter 1. Introduction to Blockchain

This section covers some of the technical aspects that comprise a blockchain and explain why blockchain is different and “works” in comparison with technologies of the past.

Chapter 2. Governance and Consensus

This section covers the various methods of blockchain governance that currently exist in the marketplace as well as how consensus fits into governance. It also covers various levels of governance and how it works with both public and permissioned blockchains.

Chapter 3. Blockchain Problem Solving

This section takes a look at the very specific features of blockchain that solve problems that have been difficult to solve in the past with more centralized architectures.

Chapter 4. Blockchain Use Cases

This section covers various use cases of blockchain. It examines the problem, and then depicts a blockchain use case that solves the problem.

Final Exam

Summary from Last Chapter (Chapter 2)

Many different consensus mechanisms are needed in a decentralized world where there are no middlemen and where trust has truly become decentralized with the trustless moveme of value.

Subscribe

Consensus is a way to ensure the nodes on the network verify the transactions and agree with their order and existence on the ledger.

The most prominent consensus method is Proof of Work. Proof of Work is a process that has miners find a nonce or a number that is combined with the other data in the header. The nonce must change the header hash to be smaller than a specific number defined by the blockchain’s difficulty. A big issue with the Proof of Work consensus process is that it requires a lot of time and electricity to complete. The incentive for mining is often cryptocurrency.

Proof of Stake is the second most prominent consensus method. Proof of Stake has nodes put up a stake to be chosen as the next block creator. When a block is chosen, the creator will receive the transaction fees associated with that block. If a block winner attempts to add an invalid block, they lose their stake.

Proof of Stake solves many problems that Proof of Work has. One of these problems is the electricity requirement that is associated with miners finding a nonce.

There are many other consensus algorithms, including Proof of Capacity, and Proof of Burn.

Because blockchains are distributed, governance is usually not determined by a single point of authority. It is determined by the users. If the users like a change initiated, they have the option of using that change within their blockchain.

Consortium blockchains can determine who has governance in a blockchain. They can control who can write onto the blockchain and who has access to what data. Consortium blockchains have lower energy costs, and higher speed, but at the cost of requiring trust among users.

Check other chapters if you finish this chapter.

- Chapter 1
- Chapter 2
- Chapter 3
- Chapter 4

Chapter 3. Blockchain Problem Solving

Chapter 3: Learning Objectives

By the end of this chapter, you should be able to:

Subscribe

- Discuss immutability in blockchains.
- Explain what transparency is and review advantages and disadvantages of append-only ledgers.
- Explain how blockchain is looking to be autonomous through smart contracts.
- Discuss how blockchain removes third party intermediaries and analyze centralized vs. decentralized ledgers (blockchain).
- Discuss how blockchain solves the problem of double spending.

Immutability

Learning Outcomes

By the end of this section, you should be able to:

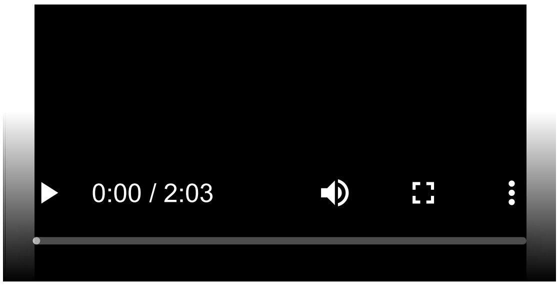
- Define immutability.
- Explain how blockchain is immutable.
- Distinguish between traditional database vs. blockchain immutability.

Immutability Defined

Immutability is when something is unable to be changed.

Immutability

Video: Immutability



Traditional Database (Transaction) Immutability

The very nature of centrally-operated databases can't be completely immutable, but that's the case for blockchain as well. A centrally-run database can embed things into it with features that mention immutability (unchangeable). But if there is a central authority, they have all the ability in the world to override that feature.

Another point to keep in mind is that immutability has been around for many years, just like the majority of the tech used via blockchain; it is the combination of these that makes it unique.

Subscribe

accounting example

Blockchain Immutability Concept

Let's review the aspects of the public blockchain that improve the chances of it being immutable.

There are many different variables, but the main one is consensus. In a blockchain, it refers to the logs of transactions which are created by consensus among the chain's participants. The basic notion is that once a blockchain transaction has received a sufficient level of validation and posted on the chain, it can almost never be replaced or reversed or edited.

If all the nodes within the network (Bitcoin specifically) are working to solve a really hard math problem by running many computers simultaneously, the chances of anyone overriding that are slim to zero.

But, if someone wanted to undermine the immutability of the Bitcoin blockchain, here's how they would do it:

- First, they would install more mining capacity than the rest of the network put together, creating a so-called "51% attack."
- Second, instead of openly participating in the mining process, they would mine their own "secret branch", containing whichever transactions they approve and censoring the rest.
- Finally, when the desired amount of time has passed, they would anonymously broadcast their secret branch to the network.

Since the attacker has more mining power than the rest of the network, their branch will contain more Proof of Work than the public one. Every Bitcoin node will therefore switch over since the rules of Bitcoin state that the more difficult branch wins. Any previously confirmed transactions not in the secret branch will be reversed and the Bitcoin they spent could be sent elsewhere. The computing power required to achieve this is enormous and probably only theoretical, but it's important to consider.

One other less technical and malicious example would be from the Ethereum hard fork that directly happened after the DAO hack. In this example, the majority of the Ethereum nodes in the network decided to update the software preventing those hackers from withdrawing the cryptocurrency "earned" (stolen). This update could not be enforced, since every Ethereum user controls their own computer. Nonetheless, it was publicly supported by Vitalik Buterin, Ethereum's founder, as well as many other community leaders. As a result, most users complied, and the blockchain with the new rules kept the name "Ethereum". A minority disagreed with the change and continued the blockchain according to its original rules, earning the title "Ethereum Classic".

Subscribe

Transparency

Learning Outcomes

By the end of this section, you should be able to:

- Explain what transparency is.
- Discuss what CRUD (Create, Read, Update, Delete) is in a traditional database.
- List advantages and disadvantages of append-only ledgers.

Transparency Defined

Transparency: Anything that is see-through, where there is very little fog or obstruction in the way. Just like immutability, transparency comes on a spectrum. Certain things are more transparent than others. In the context of business/technology, this can be seen as a way of operating that is easy for others to see what actions are being performed.

For example, open source projects where all the source code is available for the masses.

Transparency of a Blockchain

Traditional CRUD Explanation

Before we jump into how blockchain technology can be seen as transparent in certain aspects, let’s review the traditional CRUD method used by most databases.

In a traditional database, a client can perform four functions on data: Create, Read, Update, Delete. In a traditional database, there is usually an administrator, the authority giver who allows certain known participants in the database to do more than read/create; it allows them to update (change) and/or delete.

Due to the fact that the administrator is controlling who has access and who doesn’t, it’s easier to track these changes and prevent actors from tampering. In the public blockchain world, this isn’t necessarily the case.

CRUD

Blockchain Append-Only

Within the public blockchain world, every full node on the network is its own administrator, where it can Create (e.g. add) and Read; this is also known as Read/Write access (e.g. append-only). These nodes only add more data over time in the form of blocks, but all previous data is permanently stored and cannot be altered.

- Read: query (e.g. search) and retrieve data from the blockchain
- Write: add more data onto the blockchain.

For example, if the blockchain has recorded that our Bitcoin wallet has 1 million BTC, that figure is permanently stored in the blockchain. When we spend 200,000 BTC, that transaction is recorded onto the blockchain, bringing our balance to 800,000 BTC. However, since the blockchain can only be appended, our pre-transaction balance of 1 million BTC also remains on the blockchain permanently, for those who care to look. This is why the blockchain is often referred to as an immutable and distributed ledger.

Autonomy

Learning Outcomes

By the end of this section, you should be able to:

- Discuss what it means to be autonomous.
- Explain how blockchain is looking to be autonomous through smart contracts.
- Explain how smart contracts work.

Autonomy Defined

Autonomy: Independence or freedom, the ability to make your own decisions without being controlled by anyone else. This sense of freedom can be at the macro level of a country or at the micro level of a person.

As children and adults, we all want a little autonomy in our lives, careers, or relationships, but it’s just a matter of how much autonomy one truly wants and can handle.

Autonomy in Blockchain

Autonomy: Human Process-Driven Complexity

The blockchain world is looking to solve all of this complexity with autonomy from intermediaries via automated smart contracts.

No wasted paper

In the traditional world of doing any kind of transaction with another party, there tends to be a lot of administrative paperwork, with third parties intervening every step of the way. Some of this is needed, but most of it becomes wasted time and effort which could be spent elsewhere. Depending on how complex a transaction is between two parties, designated specialists (contract drafters, signatories, regulators of the contract execution, authorities to help with disputes, etc.) can make the process more efficient.

This complexity can be seen within many areas of life. Take a moment to dissect the backend of certain services or products you use and this concept will become exposed very quickly.

Autonomy with Smart Contracts

Autonomy in the blockchain world can be seen from many different angles. We are going to focus solely on **smart contracts** in this section, due to the amount of autonomy it gives everyone involved. The concept of smart contracts has been around for a long time and was first proposed by Nick Szabo, who coined the term in 1994. The most simplified explanation is:

“IF THEN ELSE” statement, which means IF X happens, THEN do Y, ELSE do Z.

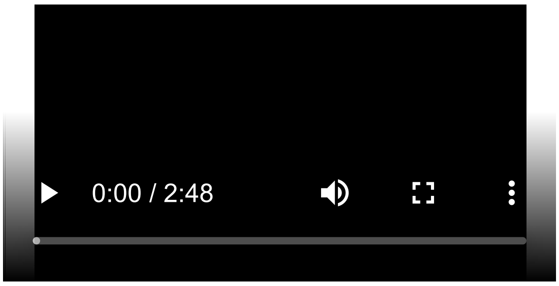
Take this concept and apply it to two or more parties, all interacting on a mutually agreed upon contract that executes based on their actions (or non-actions). An example of a smart contract could be, “if this happens before the end of the year, then you pay me, else I pay you”.

These “smart” contracts aren’t very smart, at least for now. That’s due to the simple explanation above because these contracts are “if, then, else” statements, which can vary in complexity based on how they’re stacked.

At the present moment, they can’t make decisions without human intervention, or AI, which is a highly debated topic at the moment by many neuroscientists/philosophers.

Anyone is able to create their own smart contracts without a central authority giving the right to do so. These contracts are executed without too much human intervention, and they’re stored on blockchain technology which provides a sense of permanence. These are three of the main attributes that can bring more autonomy to exchanging information between parties. Setting up a pre-agreed upon contract that’s coded into a blockchain and executes automatically when certain actions are taken is one step in the direction of not only improving our autonomy as individuals or companies, but shifting wasted resources (middle men/women) toward more impactful work.

Video: Smart Contracts



Multi-Party Transactions

Learning Outcomes

By the end of this section, you should be able to:

- Describe traditional third-party intermediaries.
- Explore how blockchain removes third party intermediaries.
- Analyze centralized ledgers vs. decentralized ledgers (Blockchain).

Ordering Between Parties: Traditional Multi-Party Sync vs. Blockchain Multi-Party Sync

In our current world of transactions, there’s always a third party to assist with connecting the sender and receiver. This has always been the most efficient way to move something from Point A to Point B. But with a third party making the connection comes the need to trust that they’ll get whatever is being sent in an efficient, economical, and effective way. This trust is open to human and process error. But we’ve discovered through experimentation that certain use cases could be automated via smart contracts.

One example is cross-border payments. Sending money from one country (border) to another country (different border). The major issue with how this is traditionally done today (e.g.

correspondent banking) is that certain transactions end up stopping off at 7–10 different checkpoint banks. This constant stopping is making the money movement more expensive (each bank takes a fee), slower, and less reliable (sometimes it might never make it). This type of transaction is heavily reliant upon third parties to facilitate the movement of information (money, in this case).

Cross Border Payments

Blockchain Multi-Party Sync (Removing Middlemen)

Blockchain technology has been shown to provide many benefits, but one of the most prominent and immediate benefits is removing middlemen (third parties) from a variety of processes. There is a long list of examples for middlemen currently being removed, such as:

- Energy distributors
- Payment networks (Visa and Mastercard)
- Content distributors (YouTube, Facebook, Medium, etc.)
- Central exchanges (NASDAQ, London Stock Exchange, New York Stock Exchange, etc.)
- Cloud database providers (AWS, Azure, etc.).

How is the blockchain world removing this middleman? The answer is all around trust. Within the public blockchain world, where everyone is theoretically anonymous, there needs to b trust so we're able to exchange valuable things without the concern of bad actors. Trust is built into the consensus mechanism that we've mentioned multiple times throughout this course. This incentivizes all the participants to help secure and validate good actions throughout the network. With that built-in "trustless" trust, we're able to remove those middlemen that provide no additional value, plus it could potentially increase the efficiency based on which public blockchain is being used.

Traditional vs. Blockchain Multi-Party Comparison

Below, you will find comparison between centralized ledger vs. blockchain.

Traditional vs Blockchain

Double Spend

Learning Outcomes

By the end of this section, you should be able to:

- Explain the concepts of digital currency and double spending.

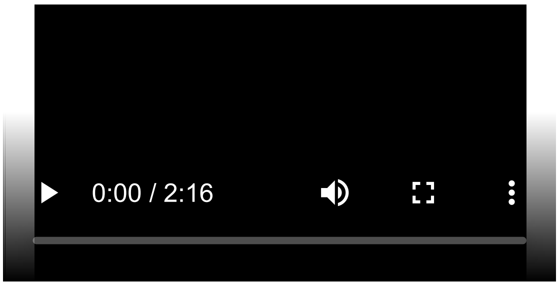
- Discuss how blockchain solves the problem of double spending.
- Review the problems of digital currency before blockchain.

Digital Currency Defined

Digital Currency: Electronic money available only in the digital world and not in the physical world.

Digital Currency

Video: Double Spend



How Blockchain Solves The Double Spend Problem

Back in the early 1990's, developers, cryptographers, and different groups of people were trying to solve the double-spend problem as it related to digital cash, previously known als as electronic cash. Double spending within Bitcoin is the act of using the same bitcoins (digital money files) more than once.

Double Spend Problem

If I buy an apple for $1, I cannot spend that same $1 to buy an orange. If I could, money would be worthless since everyone would have unlimited amounts and the scarcity that gives the currency value would disappear. The network protects against double-spending by verifying each recorded transaction within the blockchain utilizing a Proof of Work (PoW) mechanism (explained in the previous section).

Bitcoin was the first decentralized protocol to solve this problem and now more protocols are following, such as: Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Directed Acyclic Graphs (DAG) structures, Proof of Authority (PoA), etc.

Digital Currency: Difficulties Prior to Blockchain

Today, when someone mentions digital currency, usually Bitcoin or crypto is the first thing that comes to mind, but digital currency had a long history before Bitcoin popularized it. This history goes all the way back to 1983, when David Chaum introduced the idea of digital cash in a research paper. Then, in 1992, he founded DigiCash, an electronic cash company, which eventually went bankrupt in 1998 due to adoption (buyout by another financial institution).

There were many other attempts to create digital cash over the years, but many failed due to a variety of reasons, such as:

Other Attempts at Blockchain Failed

Other attempts include:

- CyberCash in 1994 (failed after the Y2K bug of 2000)
- E-gold in 1996 (sunk by continuous money laundering, hacking, and extortion)
- Liberty Reserve in 2006 (shut down in 2013 due to this becoming a great hangout spot for cybercriminals).

Summary

Chapter 3: Summary

Subscribe

Blockchain is an immutable ledger. Once a block has been added to the chain, the data in the block is permanent and cannot be altered or deleted.

This append-only ledger needs a way to verify valid transactions and delete invalid transactions before a block is added to the chain.

Transactions cannot be validated and added chronologically, because that would allow for a double spend attack. Double spending occurs when an address rapidly initiates two transactions. One of these transactions could be invalid, but, because they are initiated at the same time, both transactions could be approved. To solve this, transactions are put into a pool of unverified transactions, then nodes add these unverified transactions to a block.

When a block is full, consensus occurs, which is a process that selects the owner of a new block to be added to the chain. When consensus is achieved, nodes then validate each transaction in the selected block by referencing transactions associated with an address.

Transactions can also be added in the form of smart contracts. Smart contracts are business logic in the form of self-executing code that lives on the blockchain.

Blockchain: Understanding Its Uses and Implications – Chapter 4. Blockchain Use Cases

Learn more

Blockchain: Understanding Its Uses and Implications – Chapter 3. Blockchain Problem Solving

Learn more

Blockchain: Understanding Its Uses and Implications – Chapter 2. Governance and Consensus

Learn more

Subscribe

Blockchain: Understanding Its Uses and Implications – Chapter 1. Introduction to Blockchain

Learn more

Read More

Share with:
Facebook Twitter LinkedIn Email this page

Join @LearnThingsOnline on Telegram

1 thought on “Blockchain: Understanding Its Uses and Implications – Chapter 3. Blockchain Problem Solving”

Marta says:
June 4, 2020 at 4:54 am

Thank you for your blog post.Really thank you! Awesome.

Reply

Subscribe

Leave a Reply

Your email address will not be published. Required fields are marked *

COMMENT

□ Save my name, email, and website in this browser for the next time I comment.

NAME * EMAIL *

Post Comment

Search …

LEARNTHINGS.ONLINE TELEGRAM GROUP

Don't have **Telegram** yet? Try it now!

Learn Things Online
65 members, 2 online
This group build to share some materials to learn blockchain online & news. Check LearnThings.Online
View in Telegram
If you have **Telegram**, you can view and join
Learn Things Online right away.

Subscribe

RSS

IPFS for Beginners – Interact With IPFS By Javascript

In this article, we'll learn how to interact with IPFS by javaScript programming language. It's one way to make your own application to interact with IPFS. The post IPFS for Beginners – Interact With IPFS By Javascript appeared first on LearnThings.Online.

KPMG
KPMG in India's Lean Six Sigma Green Belt training programme.
Batches starting every week. Enroll today

Subscribe

Facebook Rename Its Libra Wallet Project Calibra to Novi

2020 May 26, Facebook rename its Libra wallet project Calibra to Novi. It makes its name more separate from Libra. Novi plans to launch its App in 2020. The post Facebook Rename Its Libra

Wallet Project Calibra to Novi appeared first on LearnThings.Online.

Libra Appoints It's General Counsel, a Former HSBC, and Goldman Sachs

Subscribe

On May 19th, 2020, the Libra association appoint Robert Werner, an Ex-HSBC & Ex-Goldman Sachs the founder and CEO of GRH Consulting, as its general counsel. The post Libra Appoints It's General Counsel, a Former HSBC, and Goldman Sachs appeared first on LearnThings.Online.