LearnThings.Online

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

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 1)

Blockchain is a digital decentralized ledger.

Blockchains are important because they provide a safe and secure way for people to make any type of transaction without having to trust anyone.

Blocks in a blockchain can be thought of as a sheet of paper. Blocks, just like paper, can hold any type of data on them.

When blocks fill up with data, transactions are hashed into what is known as a Merkle tree. Merkle trees provide for an easy way to find any specific transaction in a blockchain.

A hash function is a one way function that takes any type of data and converts it into a unique character code. Merkle trees use hashing to convert every transaction in a block into a 20-digit character code known as the Merkle root. Hashes are also useful when comparing large amounts of data.

A block header is a hash of many things determined by the blockchain, but most frequently consists of the previous block header hash, the Merkle root of the current block, and the timestamp.

By including the previous block’s header hash, blocks are “chained” together.

Chaining is important because blockchains are kept on millions of nodes across the network.

Chaining allows blockchains to easily check and see if any data was altered just by comparing the hash of the current header. If the hash is the same on every node, then the blockchain is the same. If the header hash is different in any way, then the different hash's blockchain is updated to match the majority of blockchains. This is what makes blockchains fault tolerant and immutable.

Blockchains are fault tolerant because if any one node loses track, it will be updated to match the majority of nodes running the current blockchain.

Blockchains are immutable because the data on a block can never be changed or deleted.

Contrary to a traditional database, every transaction on a blockchain is made public, and everyone can write onto a blockchain. This requires users to be anonymous to avoid identities being tied to a specific transaction.

Anonymity is achieved through public key/private key cryptography. Your private key is for your eyes only. Your public key can be shared with the public. Your public key is the address you receive and send transactions from. To prove that your public key is associated with your private key, a digital signature is used. A digital signature uses math to show a relation to your public key from your private key, without revealing your private key.

Anonymity poses a problem when it comes to trust. How can we be 100 percent certain that anonymous users are being honest when adding transactions to a ledger that once added, cannot be changed or deleted. The answer is to validate every transaction before adding them to the chain. This problem of validation is often referred to as the byzantine general' problem, and the solution is found with consensus algorithms like Proof of Work and Proof of Stake. These consensus algorithms take advantage of the fact that the majority of users on a blockchain have a common interest to keep the blockchain honest. We will go further into some consensus methods in chapter 2.

Not all blockchains use anonymity however. Private blockchains allow for the use of permissions to control who can read and write onto a blockchain. Private blockchains often require trust, but are much more efficient due to the lack of need for a consensus algorithm like Proof of Stake. A private blockchain would be useful when you want an extra layer of transparency and higher level of security than a traditional database might be able to offer.

Check other chapters if you finish this chapter.

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

Chapter 2. Governance and Consensus

Chapter 2: Learning Objectives

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

- Discuss about governance and analyze governance in a blockchain.
- Discuss about Proof of Work and Prof of Stake consensus, and their advantages and disadvantages.
- Analyze examples of Decentralized Autonomous Organizations (DAOs).
- Discuss the issues blockchain could solve in consortiums.
- Summarize the advantages and disadvantages of a consortium blockchain.

Standard vs. Blockchain Governance

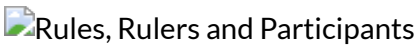
Learning Outcomes

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

- Discuss about governance and governance types.
- Analyze governance in a blockchain.

Introduction to Governance

Humans tend to attract each other and build tribes, villages, town, cities, or empires. With that comes social norms among those who are living with or near each other. These norms have different ways of manifesting into existence, but the ones relevant to this conversation will be “rules”. It doesn’t matter if the governance is the real world or the digital world, there are shared underlying principles within both. They are:

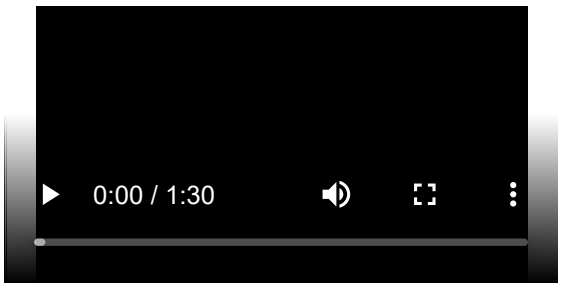

Rules, Rulers and Participants

Governance can be undertaken by a government, market, network, or social system (family, tribe, etc.).

For a governance process to work effectively, the above three principles will need to play nice with each other. For example, the rules should be aligned with the overall participants’ goals, and the rulers should enforce positive and negative actions within this governance structure.

Now that we have a simple understanding of governance, let’s analyze how this is taking place in both the standard world and the blockchain world.

Video: Governance Explained



Standard Governance

Governance is a process that can apply to states, corporations, non-profits, non-governmental organizations, partnerships, business relationships, project teams, and any other grouping of humans with a purposeful activity.

To keep things simple, we are going to cover standard governance through a lens that most blockchain systems evolved from. They are:

- Representative Democracy
- Direct Democracy.

Standard: Representative Democracy

With **representative democracy**, you have a select few who are voted upon by the people; those people have the power to suggest new rules. These rules are then voted upon by the select few. There are many pros and cons to different governance systems. Let's examine t pros and cons:

Standard: Direct Democracy

With a strict **direct democracy**, it is exactly that, direct. Any and all decisions made within that group will be voted upon directly by the people, without an intermediary.

Two examples of semi-direct democracies would be Ancient Athens back in 500 B.C. and specific parts (the Swiss cantons of Appenzell Innerrhoden and Glarus) of current day Switzerland.

How Does Blockchain Fit into Governance?

Each and every blockchain ecosystem that has or is being created will need some kind of governance mechanism in place. When participants (miners, developers, and users) in the network are interacting, ideally they are acting in a way that's best for the overall group. Being able to build a governance structure in a decentralized (sometimes anonymous, as well) world has proven to be extremely difficult, but this is a problem that many DLT companies are in the midst of solving.

Most governance structures in the blockchain ecosystem are looking to achieve similar goals, such as:

- Protocol changes and tech upgrades
- Critical bug and vulnerability fixes
- Using pooled funds for R&D.

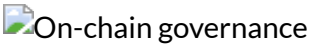
These goals can be achieved through many different methods of governance. Some of the popular ones being discussed at the moment are:

Futarchy	Decentralized Autonomous Organization (DAO)	Liquid Democracy	Quadratic Voting
Participants in a system decide its values and those with the most info stake their ideas by betting on the outcome	Allows for group governance through a combination of smart contracts and issuing tokens.	System where everyone can vote for themselves or delegate their votes	System of buying votes where each additional vote costs twice as much

After all of this is decided, it becomes time for implementation, which is choosing the right mix of "on-chain" and "off-chain" governance. Let's examine these topics.

On-Chain Governance

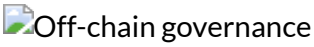
In this type of governance, rules for instituting changes are encoded into the blockchain protocol. This means that any decision being made is automatically being translated into code (e.g. decisions concerning block size). Developers propose changes through code updates and each node votes on whether to accept or reject the proposed change.



Off-Chain Governance

Off-chain governance can be seen as decision-making that first takes place on a social level and is later actively encoded into the protocol by the developers. For instance, Bitcoin developers share their improvement proposals (BIPs) through a mailing list, whereas Ethereum collects improvement protocols (EIPs) on GitHub.

Fred Ehrsam (Coinbase co-founder) argues that the Bitcoin governance system resembles the checks and balances system of the US government. Just like the Senate, developers submit pull requests BIPs to the community, the miners take the role of the Judiciary who decides whether or not proposals are adopted in practice. Lastly, the users are just like citizens in a nation or state and can revolt and switch protocols or sell their tokens.



Consensus

Learning Outcomes

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

- Explain what is Proof of Work and Proof of Stake.
- Describe the Proof of Work and Proof of Stake processes.
- Explain the advantages and disadvantages of each.

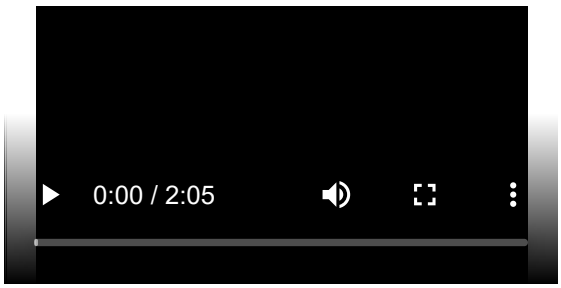
Consensus

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 movement of value.

Consensus is a way to ensure the nodes on the network verify the transactions and agree with their order and existence on the ledger. In the case of applications like a cryptocurrency, this process is critical to prevent double spending or other invalid data being written to the underlying ledger, which is a database of all the transactions.

With consensus, there are different solutions that fit different situations. When deciding to use a specific consensus mechanism, you're taking on an opportunity cost (e.g. security, speed, etc.). The main difference between consensus mechanisms is the way in which they delegate and reward the verification of transactions. It's important to mention that most blockchain ecosystems have a hybrid of different consensus mechanisms. There is no need to choose one over the other.

Video: Proof of Work



Understanding Proof of Work

Miners in the Bitcoin network are solving hard math problems to verify transactions and secure the overall network.

Within PoW we have “Miners”, which are GPUs or ASICs chips running computational cycles to solve a math problem with the goal of reaching a set number previously provided to them. This set number is called a “target”, which is an SHA-256 hash with a long list of leading zeros and the “difficulty” (another term in the Bitcoin world) of this “target” adjusts every 2016 blocks (roughly 2 weeks), to ensure it takes roughly ten minutes for the miners to crack.

There are three major ingredients needed to find this “target”:

- A nonce (number only used once)
- The transactional data
- The previous blocks hash.

This is all then hashed (combined) over and over with the nonce changing each time until the hash created from these three ingredients is lower than the “target” provided.

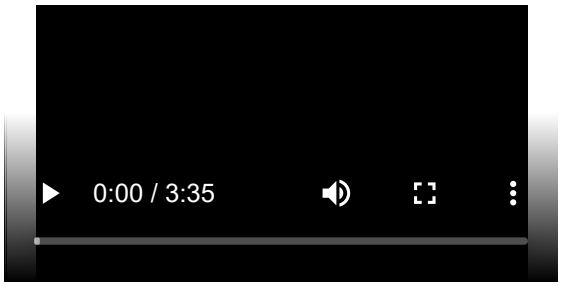
Once the Miner has reached this “target”, they’re gifted with a transaction fee and mining reward (at the time this course was released, 12.5 bitcoins). The reward gets cut in half every 210,000 blocks (roughly 4 years).

The next step is for the miner to broadcast to all the other miners that they have achieved the set “target” and have confirmed the block. Once that has been completed, they’ll move on to the next block.

A good analogy is a lock and its combination. It takes a lot of work to figure out the combination, but once you do, it’s easy to verify.

Proof of Work: Pros and Cons

Video: Proof of Stake



Understanding Proof of Stake

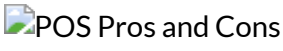
With Proof of Stake (PoS) we have “Validators” – “Forging”, instead of “Miners” – “Mining”. There are no computational cycles running through massive amounts of math problems trying to solve a problem like PoW. With PoS, we have validators sending a special type of transaction across the network, which gets locked into a deposit (otherwise known as validator pool) and that’s called “staking”.

Once this validator has thrown his hat into the proverbial arena, then an algorithm pseudo-randomly selects a validator during each time slot (for example, every period of 10 seconds might be a time slot), and assigns that validator the right to create a single block. This block must point to some previous block (normally the block at the end of the previously longest chain), and over time, most blocks converge into a single constantly growing chain.

The next step is for the validator to validate a grouping of transactions. Once that’s completed, they receive their staked funds back, plus the transaction fees (sometimes rewards when coin supply is being inflated from time-to-time) for that block.

If the validator decides to act in a bad way (i.e. bad actor) and validate fraudulent transactions, they lose their stake that’s being held at the moment and are booted from the validator pool going forward (losing rights to forge). This is a built-in incentive mechanism to ensure they are forging valid transactions and not fraudulent ones.

Proof of Stake: Pros and Cons



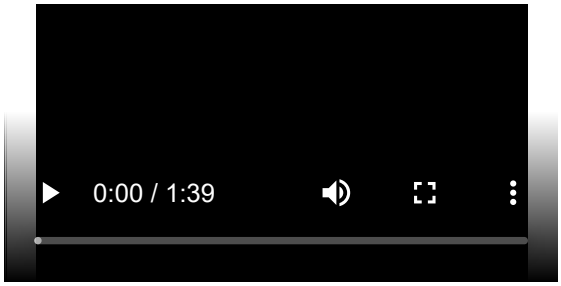
Governance with Autonomy

Learning Outcomes

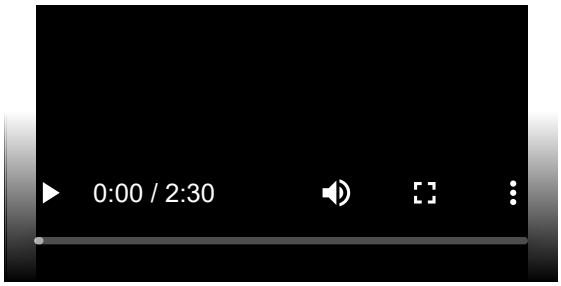
By the end of this section, you should be able to:

- Analyze examples of Decentralized Autonomous Organizations (DAOs).
- Explain how DAOs will be governed.

Video: Governance With Autonomy: Driverless Cars



Video: Decentralized Autonomous Organization (DAO)



Decentralized Autonomous Organization (DAO)

Decentralized Autonomous Organization (DAO) is a complex stack of smart contracts.

It's important to understand that, at the moment, there is no such thing as a completely autonomous DAO. There are specific parts that are autonomous and others that are not so autonomous.

In simple terms, a DAO is an organization that runs on a stack of computer programs (called smart contracts in the blockchain world) that are all interconnected to maintain a set of pre-programmed rules that have been previously voted upon by a community.

When thinking about regular corporations stripped all the way down to their bare bones, they are basically different groups following rules, responsibilities, and duties given from those sitting at the top of the organization. The bigger they are, the more complex these pieces become. At the moment, a DAO's goal is to automate this complex system piece by piece.

Within each DAO, there is a kind of pooling process for humans to contribute new rules into the system. These rules are then presented to the community and voted upon, based on the DAOs previously created rules. These new rule commitments will need majority agreement (may be different for each DAO) from the community to make this rule real. If this new computer-coded rule is accepted by the community, then it will be placed into the stack of other computer coded rules to improve the overall autonomous organization.

Governance for Enterprise

Learning Outcomes

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

- Discuss the issues blockchain could solve in consortiums.
- Summarize the advantages and disadvantages of a consortium blockchain.

Governance for Enterprise

We're focusing on governance in the consortium space, not governance within an enterprise company. So what is a "consortium"? A **consortium** is just a grouping of institutions (possibly individuals) getting together to achieve a mutual goal.

This goal can be setting some standard for their industry (Department of Justice), selling product (Airbus), sharing resources (Universities), etc. In a consortium, the only real obligation you have to others who are taking part would be providing resources for specific tasks and sticking to the rules laid out prior to you joining. Within blockchain, there are many different industries creating their own consortiums, such as financial services, life science and health care, energy, media and telcos, and the public sector.

Governance becomes much easier when it's in a controlled environment, with each member agreeing upon set rules prior to jumping in with everyone else. Governance structures vary by industry and profit vs. non-profit, so there will be no set governance model everyone uses, but there are two we've come across in the blockchain space.

- One is including the formation of smaller subgroups to work on specific issues.
- The second is providing several levels of potential engagement, ranging from participation in monthly calls to active technology development.

The point we would like to get across here is that a consortium governance model is currently more efficient than most decentralized blockchains.

Governance for Enterprise: Consortiums

Almost all consortiums up to this point have been permissioned and not decentralized permissionless blockchains, which is an opportunity cost most companies make when joining. At a high level, a permissioned blockchain is just that, a chain in which others must have permission to operate on. So, all the nodes operating on a permissioned chain have been verified by the central institution that is the authority of the network and the transactions that are confirmed don't necessarily have to go through all the nodes.

These consortium blockchains have historically taken two approaches:

- **Business-focused consortia**
  They aim to build and operate blockchain-based business platforms to solve a specific business problem (e.g. Digital Trade Chain – focused on cross-border payments).
- **Technology-focused consortia**
  They seek to develop reusable blockchain platforms based on technical standards

(e.g. Hyperledger) .

There are some consortiums that do a hybrid of both business and technology, such as R3. Examples: Hyperledger, R3, Ripple, Digital Asset Holdings, Corda, B3i, EWF, etc.

Consortiums: Pros and Cons

Below are some of the pros and cons to consortium blockchains:

Summary

Chapter 2: Summary

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 movement of value.

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 l 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.

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

Subscribe

Learn more

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

Leave a Reply

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

COMMENT

NAME *

EMAIL *

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

Post Comment

Subscribe

Search …

LEARNTHINGS.ONLINE TELEGRAM GROUP

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.

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.