BLOCKCHAIN BASICS

TABLE OF CONTENTS

BLOCKCHAIN BASICS

BLOCKCHAIN ACKNOWLEDGEMENT:

Bitcoin is exciting because it shows how cheap it can be. Bitcoin is better than currency in that you don’t have to be physically in the same place and, of course, for large transactions, currency can get pretty inconvenient,” Bill Gates, Co-founder of Microsoft, investor and philanthropist.

LEARNING OBJECTIVE:

1. Explain three fundamental characteristics that define a blockchain?
2. Discuss the important features of Ethereum blockchain?
3. Explain the algorithms and techniques that enable the blockchain, including a public gate cryptography and hashing.
4. Outline methods for realizing trust in a blockchain.

WEEK 1: BLOCKCHAIN DEFINED

BITCOIN AND BLOCKCHAIN

HOW DID BITCOIN REALIZE TRUST AND SECURITY?

By implementing software programs for validation, verification, consensus in a novel infrastructure called the blockchain.

WHAT IS A BLOCKCHAIN?

Blockchain is about enabling peer to peer transaction in a decentralized network. Establishing trust among unknown peers. Recording the transaction in an immutable distributed ledger.

Summarizing, blockchain technology supports methods for a decentralized peer-to-peer system, a collective trust model, and a distributed immutable ledger of records of transactions.

CENTRALIZED VERSUS DECENTRALIZED

Let's understand centralized versus decentralized network using a common scenario. Consider a scenario where customer wants to buy an item using her credit card.

Let's enumerate the intermediaries involved in accomplishing this task. We have a credit card agency, we have a customer bank, we have a credit cards bank, we have an exchange, we have the merchant's bank, and finally, the merchant. This is an example of a centralized system that we are so used to.

Now compare this with a system where peers can transact directly with each other irrespective of where they are located. Functions of the intermediaries are shifted to the periphery to the peer participant in the blockchain infrastructure. Peers are not necessarily known to each other. This is a decentralized system.

HOW DO WE ESTABLISH TRUST AMONG THE PEERS IN SUCH A DECENTRALIZED SYSTEM?

By having a process in place to validate, verify, and confirm transactions. Record the transaction in a distributed ledger of blocks, create a tamper-proof record of blocks, chain of blocks, and implement a consensus protocol for agreement on the block to be added to the chain. So, validation, verification, consensus, and immutable recording lead to the trust and security of the blockchain.

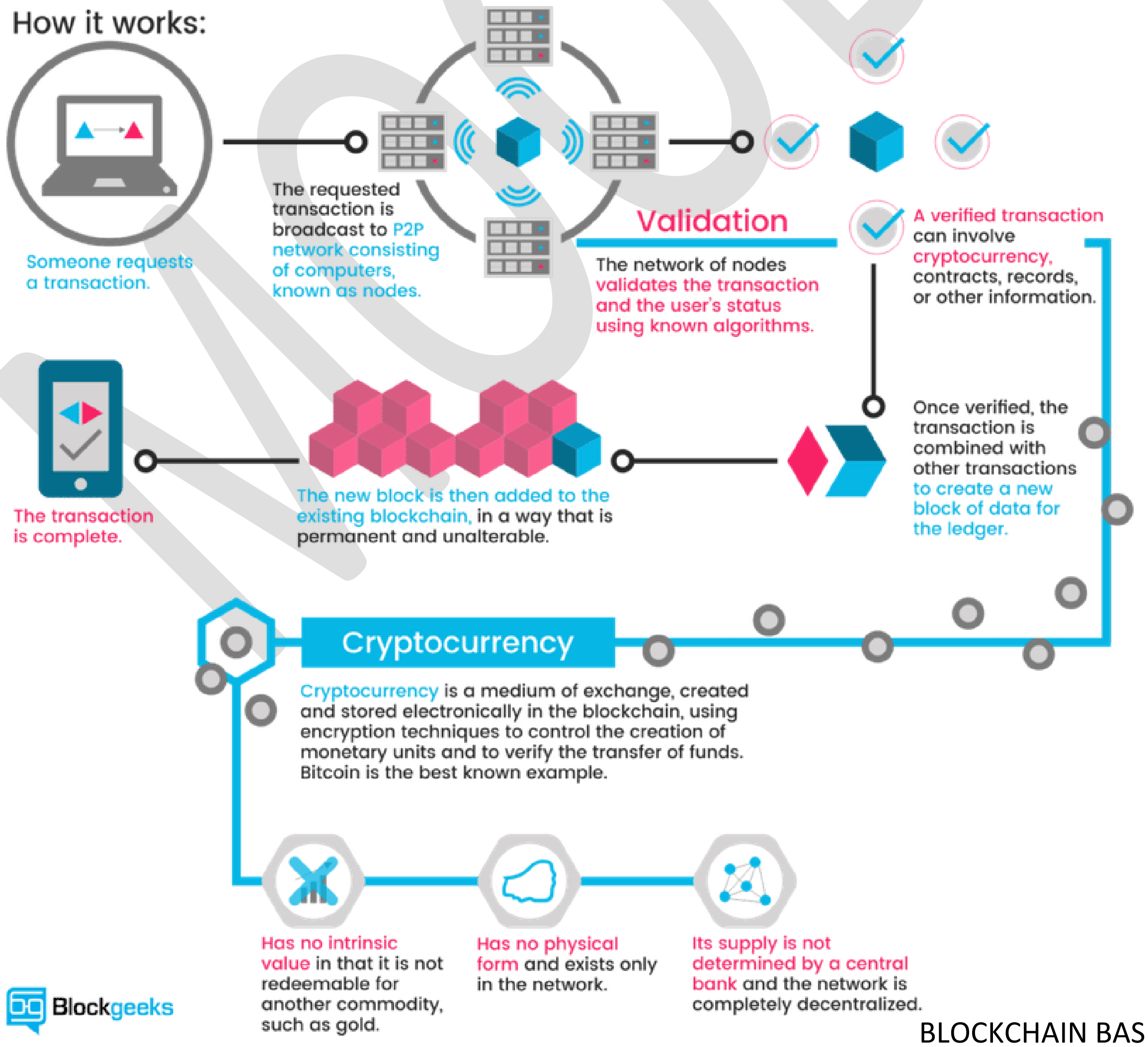
IMMUTABLE DISTRIBUTED LEDGER

I'm lending Amy $10,000. This is one single peer to peer transaction. We both make a note of it on a ledger.

What if I change my entry from 10,000 to 11,000? Alternatively, Amy changes hers from 10,000 to 1,000. To prevent this trust violation, we need to seek the help of people around us, Lisa, Allison, and Francis. Provide all of them a valid copy of this ledger.

This is the basic concept of an **immutable distributed ledger** defined in a blockchain process.

COMPLETE WORKING PROCESS


How it works:
Someone requests a transaction.
The requested transaction is broadcast to P2P network consisting of computers, known as nodes.
Validation
The network of nodes validates the transaction and the user's status using known algorithms.
A verified transaction can involve cryptocurrency, contracts, records, or other information.
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.
The transaction is complete.
Cryptocurrency
Cryptocurrency is a medium of exchange, created and stored electronically in the blockchain, using encryption techniques to control the creation of monetary units and to verify the transfer of funds. Bitcoin is the best known example.
Has no intrinsic value in that it is not redeemable for another commodity, such as gold.
Has no physical form and exists only in the network.
Its supply is not determined by a central bank and the network is completely decentralized.
Blockgeeks

LESSON 1 RESOURCES: BITCOIN & BLOCKCHAIN

The following resources were selected to provide an overview of the topic of Bitcoin & Blockchain. We would like to acknowledge the authors of the various web articles, videos, and papers for their insightful discussions and analytics which helped form the basis for some sections of the lessons and modules.

Title of resource: What is Blockchain Technology? A Step-by-Step Guide For Beginners

Resource type: Website

Description: A step by step guide that goes into the details of what Blockchain technology is.

BLOCKCHAIN STRUCTURE

Here is the basic structure of a blockchain. Transaction is the basic element of the Bitcoin Blockchain. Transactions are validated and broadcast. Many transactions form a block. Many box form a chain through a digital data link. Blocks go through a consensus process, to select the next block that will be added to the chain. Chosen block is verified, and added to the current chain. Validation and consensus process are carried out by special peer nodes called miners. These are powerful computers executing software defined by the blockchain protocol.

SINGLE TRANSACTION IN BITCOIN

A fundamental concept of a bitcoin network is an **Unspent Transaction Output**, also known as UTXO. The set of all UTXOs in a bitcoin network collectively defined the state of the Bitcoin Blockchain. UTXO's are referenced as inputs in a transaction. UTXO's those are also outputs generated by a transaction. All of that UTXO's is in a system, are stored by the participant nodes in a database.

ROLE OF THE UTXO'S

Now let's review the role of the UTXO's in a Bitcoin Blockchain. The transaction uses the amount specified by one or more UTXOs and transmits it to one or more newly created output UTXOs, according to the request initiated by the sender.

STRUCTURE OF A UTXO

1. It includes a unique identifier of the transaction that created this UTXO.
2. An index or the position of the UTXO in the transaction output list.
3. A value or the amount it is good for.
4. An optional script, the condition under which the output can be spent.

STRUCTURE OF TRANSACTION

The transaction itself includes

1. A reference number of the current transaction.
2. References to one no more input utxos.
3. References to one or more output utxos newly generated by the current transaction.
4. The total input amount and output amount.

SUMMARY

To summarize, transaction bring about transfer of value in the Bitcoin Blockchain. The concept of UTXO defines the inputs and outputs of such a transaction. Once a block is verified an algorithmic-ally agreed upon by the miners, it is added to the chain of blocks, namely the Blockchain.

LESSON 2 RESOURCES: BLOCKCHAIN STRUCTURE

The following resources were selected to provide an overview of the topic of Blockchain Structure. We would like to acknowledge the authors of the various web articles, videos, and papers for their insightful discussions and analytics which helped form the basis for some sections of the lessons and modules.

Title of resource: Unspent Transaction Output, UTXO

Resource type: Website

Description: An explanation on how UTXO's operate vs other methods.

BASIC OPERATIONS

OPERATIONS

let's consider the basic operations in a blockchain. Operations in the decentralized network are the responsibility of the peer participants and their respective computational nodes.

These operations include

- Validation transactions.
- Gathering the transactions for a block.
- Broadcasting the ballot transactions in the block.
- Consensus on the next block creation.
- Chaining the blocks to form an immutable record.

PARTICIPANTS

First, we have to discuss the participants. There are two major roles for the participants.

1. Participants that initiate transfer of value by creating a transaction.
2. Additional participants called miners; who

- Pick on added work or computation to verify transactions.
- Broadcast transaction.
- Compete to claim the right to create a block.
- Work on reaching consensus by validating the block.
- Broadcasting the newly created block.
- Confirming transactions.

THE FUNDAMENTAL OPERATIONS OF THE BITCOIN BLOCKCHAIN

- **Transaction validation** is carried out independently by all miners. The process involves validation of more than 20 criteria, including size, syntax, et cetera. Some of these **criteria** are:
    - ➢ Referenced Input Unspent Transaction Output
    - ➢ UTXOs are valid.
    - ➢ Reference output UTXOs are correct.
    - ➢ Reference input amount and output amount matched sufficiently.

- **Invalid transactions** are rejected and will not be broadcast. All the **valid transactions** are added to a pool of transactions.
- Miners **select a set of transaction** from this pool to create a block.
- This creates a challenge. If every miner adds the block to the chain, there will be many branches to the chain, resulting in inconsistent state. Recall, the blockchain is a single consistent linked chain of flux. We need a system to overcome this challenge, the solution. Miners compete to solving a puzzle to determine who earn the right to **create the next block**. In the case of bitcoin blockchain, this parcel is a computation of parcel and the central processing unit or CPU intensive. Once a miner solves the puzzle.
- the announcement is **broadcast to the network** and the block is also broadcast to the network. Then, **other participant verify** the new block. Participants reach a consensus to add a new block to the chain.
- This new block is added to their local copy of the blockchain. Thus, a new set of transactions are **recorded and confirmed**. The algorithm for consensus is called proof-of -work protocol, since it involves work a computational power to solve the puzzle and to claim the right to **form the next block**.

SUMMARY

To summarize, the main operations in a blockchain are transaction validation and block creation with the consensus of the participants. There are many underlying implicit operations as well in the bitcoin blockchain.

LESSON 3 RESOURCES: BASIC OPERATIONS

The following resources were selected to provide an overview of the topic of Basic Operations. We would like to acknowledge the authors of the various web articles, videos, and papers for their insightful discussions and analytics which helped form the basis for some sections of the lessons and modules.

Title of resource: How Bitcoin Works (investopedia.com)

Resource type: web article

Author: David Floyd

Description: This article provides a basic description of Bitcoin, including key takeaways.

Title of resource: How Does the Blockchain Work?

Resource type: Website

Description: An article written by Michele D'Aliessi on Medium that explains blockchain technology in simple words.

Title of resource: How Do Bitcoin Nodes Verify Transactions?

Resource type: Website

Description: An article describing some of the features that mining nodes check for transaction validation.

BEYOND BITCOIN

BITCOIN BLOCKCHAIN

Bitcoin blockchain is open-source and the entire code is available on the GitHub.

SMART CONTRACT

Bitcoin supports an optional and special feature called scripts for conditional transfer of values. Ethereum Blockchain extended the scripting feature into a full-blown code execution framework called smart contract. A smart contract provide the very powerful capability of code execution for embedding business logic on the blockchain.

TYPES OF BLOCKCHAINS

Three major types of blockchains emerge from Bitcoin foundation.

- **Type one** deals with the coins in cryptocurrency currency chain. Example, Bitcoin.
- **Type two** supports cryptocurrency and a business logic layer supported by code execution. Example, ethereum.
- **Type three** involves no currency but supports software execution for business logic. Example, The Linux Foundation's Hyperledger.

CLASSIFICATION OF BLOCKCHAINS

The classification of public, private, and permissioned blockchains based on access limits.

1. Public Blockchain: Public blockchains are open to anyone who wants to participate. A notable example of a public blockchain is Bitcoin. In a public blockchain, anyone can join the network, validate transactions, and create new blocks. The entire transaction history and the blockchain itself are publicly accessible, although participants remain anonymous. Public blockchains are decentralized and typically open-source, allowing anyone to view and contribute to the codebase. Participants can also create new digital currencies by modifying the blockchain's code. Wallet applications enable users to interact with the blockchain and transfer value using the native cryptocurrency.

2. Private Blockchain: In contrast to public blockchains, private blockchains have restricted access and are limited to a select group of participants. These participants are often within a single organization or a controlled environment. The restriction of access in private blockchains simplifies operations, such as block creation and consensus mechanisms. Private blockchains are often used for internal purposes within businesses or organizations, where transparency and openness to the public are not necessary or desired.

3. Permissioned Blockchain (Consortium Blockchain): Permissioned blockchains, also known as consortium blockchains, are designed for a consortium or group of collaborating parties to transact on the blockchain. These parties have a shared interest or purpose and need a blockchain for ease of governance, provenance, and accountability. For instance, a consortium of automobile companies or healthcare organizations could use a permissioned blockchain. Permissioned blockchains offer some of the benefits of public blockchains, such as transparency and security, but they only allow authorized users to participate and transact on the network. This ensures a higher level of control and privacy compared to public blockchains.

SUMMARY

In summary, significant innovations such as smart contracts have opened up broader applications for blockchain technology. Private and permissioned blockchain allow for controlled access to the blockchain enabling many diverse business models.

LESSON 4 RESOURCES: BEYOND BITCOIN

The following resources were selected to provide an overview of the topic of Beyond Bitcoin. We would like to acknowledge the authors of the various web articles, videos, and papers for their insightful discussions and analytics which helped form the basis for some sections of the lessons and modules.

Title of resource: A Gentle Introduction to Blockchain Technology

Resource type: Website

Description: This article is a gentle introduction to blockchain technology and assumes minimal technical knowledge. It attempts to describe “what it is” rather than “why should I care”.

Title of resource: On Public and Private Blockchains

Resource type: Website

Description: A blog posted by Vitalik Buterin, the founder of Ethereum. He goes on to explain the differences between the different types of blockchains.

Title of resource: What is Cryptocurrency. Guide for Beginners

Resource type: Website

Description: An easy-to-understand guide on cryptocurrencies, including its history and future.

Title of resource: 2017 Was Bitcoin's Year. 2018 Will Be Ethereum's

Resource type: Website

Description: The following article written by Jez San, CEO of FunFair Technologies, an Ethereum-powered casino platform, explains why Ethereum will continue to evolve throughout the year 2018.

Title of resource: What is Cryptocurrency: Everything You Need To Know

Resource type: Website

Description: This introduction explains the most important things about cryptocurrencies and where they are headed.

Title of resource: What is the Difference Between Public and Permissioned Blockchains?

Resource type: Website

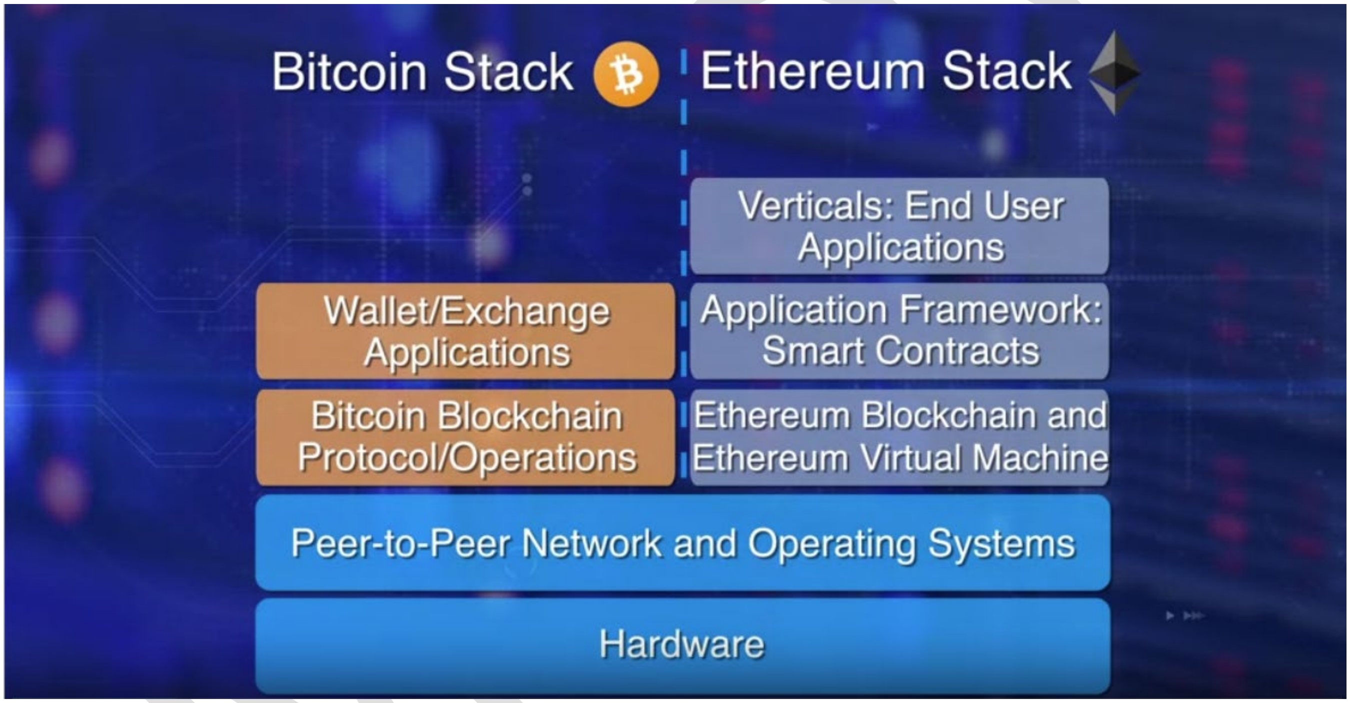
Description: An article that introduces a description of the three technologies that make up blockchain technology: cryptographic keys, a distributed network and a network servicing protocol.

WEEK 2: ETHEREUM BLOCKCHAIN

SMART CONTRACTS

DIFFERENCES BETWEEN BITCOIN AND ETHEREUM BLOCKCHAINS

The Bitcoin blockchain is often considered the pioneering blockchain, primarily designed for peer-to-peer transfer of value (cryptocurrencies) with a strong focus on security and decentralization. On the other hand, in 2013, Ethereum founders introduced a groundbreaking concept: a blockchain framework that supports code execution. The central feature of Ethereum is the smart contract, which enables programmable, self-executing agreements on the blockchain.


Bitcoin Stack
Ethereum Stack
Verticals: End User Applications
Wallet/Exchange Applications
Application Framework: Smart Contracts
Bitcoin Blockchain Protocol/Operations
Ethereum Blockchain and Ethereum Virtual Machine
Peer-to-Peer Network and Operating Systems
Hardware

In the diagram comparison, the left side represents Bitcoin's blockchain with a wallet application for initiating transactions, emphasizing its primary use for value transfer. The right side illustrates Ethereum, which expanded the possibilities of blockchain technology by becoming a computational framework. It introduced the concept of a virtual machine on which smart contracts can execute, enabling the creation of decentralized applications (DApps) that can accomplish various tasks beyond simple value transfers. One such application is efficient automation of supply chains.

Launched in 2015, Ethereum builds on Bitcoin's innovation, with some big differences.

- Both let you use digital money without payment providers or banks. But **Ethereum is programmable**, so you can also build and deploy decentralized applications on its network.

- Bitcoin enables us to send basic messages to one another about what we think is valuable. Establishing value without authority is already powerful. Ethereum extends this: rather than just messages, you can write any general program, or contract. There is no limit to the kind of contracts which can be created and agreed upon, hence great innovation happens on the Ethereum network.
- While Bitcoin is only a payment network, Ethereum is more like a marketplace of financial services, games, social networks and other apps.

SMART CONTRACT DEFINITION:

- A smart contract is a self-executing piece of code deployed on a blockchain node.
- It gets triggered by a message embedded in a transaction on the blockchain.
- Smart contracts can perform specific tasks automatically based on predefined conditions and rules.
- Once deployed, they operate without the need for intermediaries, providing transparency and trust in the execution of agreements.

Execution of a smart contract is initiated by a message embedded in the transaction.

CAPABILITIES OF SMART CONTRACTS ON ETHEREUM:

- Ethereum's smart contracts go beyond simple currency transfers.
- They enable more sophisticated operations, such as conditional transfers, evaluations, multi-signature requirements, and time-based actions.
- For example, a smart contract could verify if a bidder's age is greater than 18 and if their bid amount exceeds a minimum bid before accepting or rejecting a bid in an auction.

STRUCTURE OF SMART CONTRACTS:

- Smart contracts are structured similarly to class definitions in object-oriented programming.
- They consist of data (variables) and functions (methods) with public or private access modifiers.

- They may also have getter and setter functions to interact with the data.
- Solidity is a popular programming language for writing smart contracts on Ethereum.

ETHEREUM VIRTUAL MACHINE (EVM):

- The Ethereum Virtual Machine (EVM) is a crucial component for executing smart contract code.
- It acts as a runtime environment that enables any node on the Ethereum network to execute the same code regardless of hardware or operating system differences.
- Smart contracts are written in high-level languages like Solidity and then compiled into EVM bytecode.
- This bytecode is deployed on the EVM, and each node on the network hosts a copy of the smart contract's code.

SUMMARY:

- Smart contracts introduce logic and computation to the blockchain's trust infrastructure.
- They allow for the execution of code beyond basic value transfers, providing new possibilities for decentralized applications (DApps).
- The code for smart contracts is written in high-level languages like Solidity, which is then compiled into bytecode.
- The EVM ensures that all nodes in the Ethereum network can execute the smart contract's code consistently, making the network trustless and reliable.

LESSON 1 RESOURCES: SMART CONTRACTS.

The following resources were selected to provide an overview of the topic of Smart Contracts. We would like to acknowledge the authors of the various web articles, videos, and papers for their insightful discussions and analytics which helped form the basis for some sections of the lessons and modules.

Title of resource: What is Ethereum?

Resource type: Website

Description: Introduction to Ethereum, Ethereum Virtual Machine, and how they work.

Title of resource: Smart Contracts: The Blockchain Technology That Will Replace Lawyers

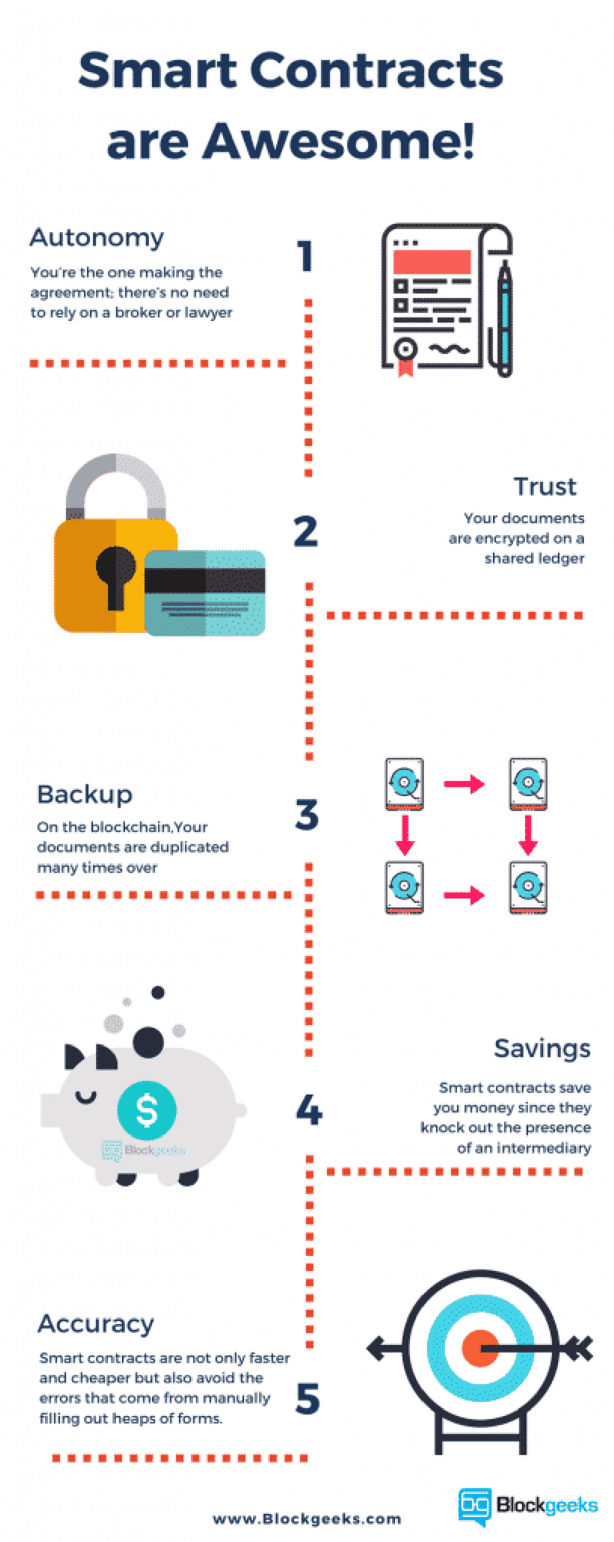
Resource type: Website

Description: Article explains what smart contracts are and how they allow for the disposal of intermediaries which will saves time and conflict for governments and corporations.

Title of resource: Introduction to Smart Contracts

Resource type: Website

Description: Introduction to the basics of smart contracts and solidity.



Smart Contracts are Awesome!

1 Autonomy

You're the one making the agreement; there's no need to rely on a broker or lawyer

2 Trust

Your documents are encrypted on a shared ledger

3 Backup

On the blockchain,Your documents are duplicated many times over

4 Savings

Smart contracts save you money since they knock out the presence of an intermediary

5 Accuracy

Smart contracts are not only faster and cheaper but also avoid the errors that come from manually filling out heaps of forms.

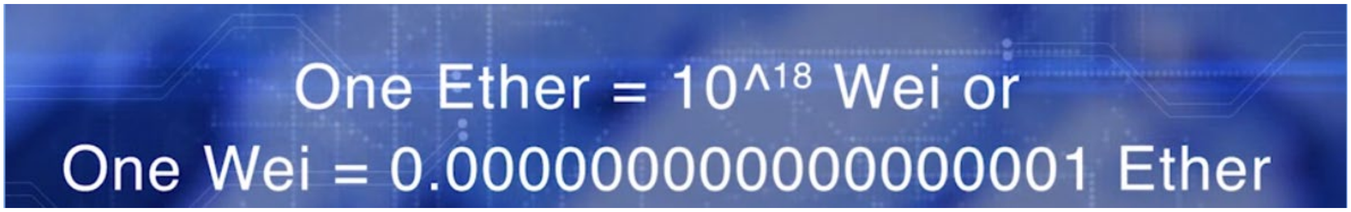
www.Blockgeeks.com

ETHEREUM STRUCTURE

ACCOUNTS IN ETHEREUM:

- Accounts in Ethereum serve as fundamental units of the protocol and are essential for interacting with the blockchain.
- There are two types of accounts: Externally Owned Accounts (EOA) and Contract Accounts (CA).
- **Externally Owned Accounts (EOA)** are controlled by private keys and represent user-controlled accounts.
- **Contract Accounts (CA)** are controlled by code and represent smart contracts deployed on the Ethereum blockchain.

- An EOA is required to participate in the Ethereum network and can interact with the blockchain using transactions.
- Each account has a coin balance, denoted in Ether (ETH), which is the native cryptocurrency of the Ethereum network.
- Transactions initiated by accounts can transfer Ether (value) or invoke smart contract code (messages) or both.
- Fees are paid in Wei. Wei is a lower denomination of Ether.



One Ether = $10^{\wedge 18}$ Wei or

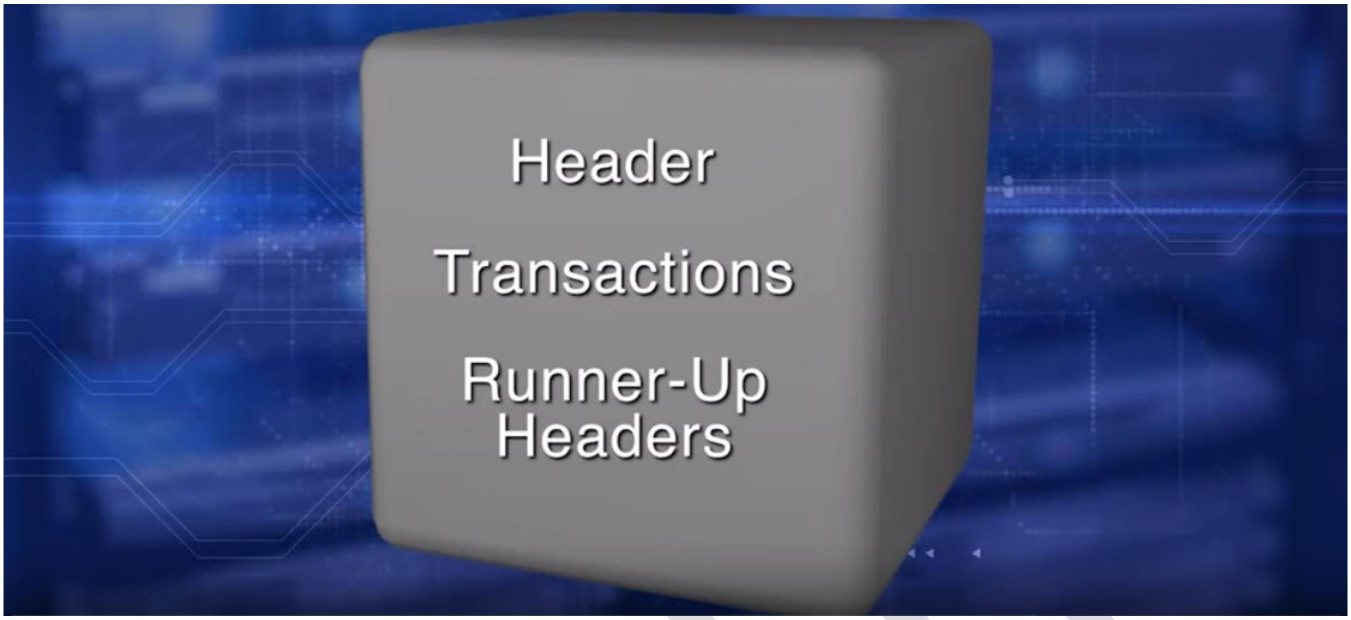
One Wei = 0.000000000000000001 Ether

ETHEREUM TRANSACTIONS:

- An Ethereum transaction contains various important fields that define its behavior and purpose.
- These fields include the **recipient address**, the **digital signature** of the sender (to authorize the transfer), the **amount of Ether** to transfer (in Wei), an **optional data field** (for messages to smart contracts), **STARTGAS** (representing the maximum computational steps allowed for the transaction), and the **gas price** (the fee the sender is willing to pay for computations).
- Gas is used as a measure of computational effort in Ethereum and is paid for by the sender of the transaction.
- The gas limit sets the maximum amount of gas allowed for a transaction, preventing infinite loops or excessive computation.
- The gas price, specified by the sender, determines the fee they are willing to pay for each unit of gas consumed during the execution of the transaction.

ETHEREUM BLOCK STRUCTURE:

- Ethereum blocks have a structured layout that includes headers, transactions, and runner-up block headers.
- A block header contains essential information like the block number, timestamp, block hash, previous block hash, difficulty level, total difficulty, gas used, gas limit, nonce, and block reward (amount of Ether given to the miner as a reward for mining the block).
- Transactions within a block represent the actions taken by various accounts on the Ethereum network.
- The runner-up block headers refer to other block headers that were candidates to be included in the chain but were not selected during the mining process.



SUMMARY:

- Ethereum relies on different types of accounts: Externally Owned Accounts for users and Contract Accounts for smart contracts.
- Transactions in Ethereum allow for the transfer of Ether and messages to invoke smart contract code.
- The gas mechanism ensures computational resource allocation and incentivizes miners to process transactions.
- Blocks in Ethereum store critical information about transactions and their execution, forming a chain of blocks that make up the blockchain.

LESSON 2 RESOURCES: ETHEREUM STRUCTURE

The following resources were selected to provide an overview of the topic of Ethereum Structure. We would like to acknowledge the authors of the various web articles, videos, and papers for their insightful discussions and analytics which helped form the basis for some sections of the lessons and modules.

Title of resource: Ethereum Whitepaper: A Next-Generation Smart Contract and Decentralized Application Platform

Resource type: White paper

Description: Offers an overview of smart contracts, their types depending on the transaction involved, and blockchain technology providers.

Title of resource: Account Management

Resource type: Website

Description: Documentation on account management from Ethereum Homestead, an ongoing collaborative effort of volunteers from the Ethereum Community.

Title of resource: Native: Account management

Resource type: Website

Description: Introduces account management and how it can provide Ethereum integration for your native applications.

ETHEREUM OPERATIONS

ETHER TRANSFER

- Ether transfer is a straightforward process where you provide the amount of Ether you want to send, the recipient's address, and the necessary fees (also known as gas points).
- The specified amount of Ether and the fees are directed to their respective accounts.
- For instance, if you're transferring 100 Ether from your account to someone else's, you'll provide their address, the amount, and the fees for the transaction.
- In addition, when you perform this transfer, a certain number of gas points (specifically 21,000) are given to the miner responsible for adding your transaction to the blockchain. This is a reward for their work in maintaining the network.

ETHEREUM NODE

- Ethereum nodes represent participants within the Ethereum network, which could be individuals or business entities.
- Among these nodes, there are full nodes that host the necessary software for various actions, including initiating transactions, validating them, participating in mining, creating blocks, executing smart contracts, and managing the Ethereum Virtual Machine (EVM).
- The Ethereum Virtual Machine (EVM) is a crucial part of the network that handles the execution of smart contracts, transaction validation, and other operations.

SMART CONTRACTS

- Smart contracts are essential components of the Ethereum ecosystem.

- They are designed, developed, compiled, and eventually deployed on the Ethereum Virtual Machine (EVM).
- The EVM can accommodate more than one smart contract, each serving a specific purpose.
- If a transaction's target address is a smart contract, the code associated with that contract is activated and executed on the EVM.
- This execution requires input, which is taken from the transaction's payload.
- The "state" of a smart contract refers to the values of variables defined within it. These values can be modified during the execution process.
- The results of this execution are presented in receipts, which provide information about the changes made by the execution.
- The blockchain maintains both a state hash (a summary of the current state) and a receipt hash (a summary of the receipts).

TRANSACTIONS AND VALIDATION

- All transactions are subject to validation.
- During validation, factors like the timestamp and nonce (a unique number) are checked to ensure the legitimacy of the transaction.
- Furthermore, it's verified whether the fees provided are sufficient for the transaction to be executed.
- Miner nodes, which play a key role in the network, receive, verify, gather, and execute transactions.
- When it comes to smart contracts, their code is executed by all miners, contributing to the overall network's functionality.
- Validated transactions are shared across the network and collected for the purpose of creating blocks.
- The consensus protocol employed in Ethereum is a memory-based proof of work mechanism.

INCENTIVE MODEL

- One might wonder who covers the costs of operations such as validation, verification, and reaching consensus.
- This question is addressed by the Incentive Model, which explains how participants are motivated to contribute their computational resources to maintain the network's integrity.
- The specifics of this model and how it encourages involvement will be explored in a forthcoming lesson.

LESSON 3 RESOURCES: ETHEREUM OPERATIONS

The following resources were selected to provide an overview of the topic of Ethereum Operations. We would like to acknowledge the authors of the various web articles, videos, and papers for their insightful discussions and analytics which helped form the basis for some sections of the lessons and modules.

Title of resource: What Is Meant By The Term "Gas"?

Resource type: Website

Description: Answers on Ethereum stack exchange that explains gas and where it comes from?

INCENTIVE MODEL

INTRODUCTION

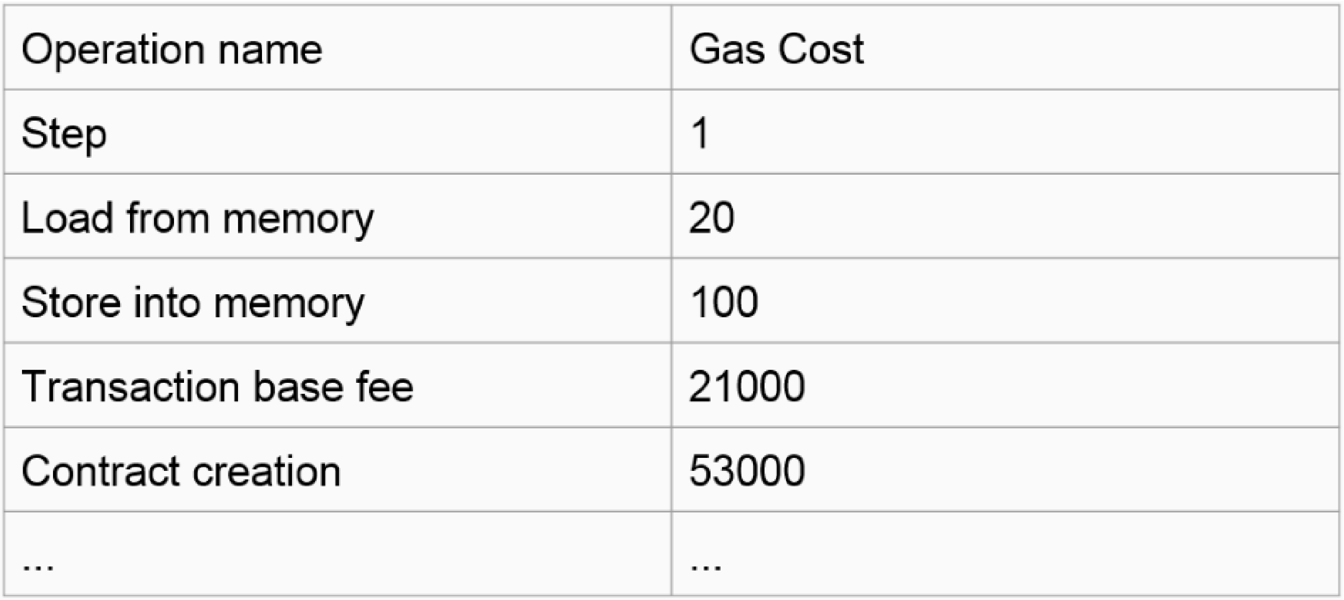
In Ethereum, mining is a pivotal process that ensures the network's security. It encompasses various steps such as validating computations, assembling blocks, confirming their accuracy, and broadcasting them to the network. This lesson delves into Ethereum's incentive-driven approach to block creation.

GAS POINTS AND FEE STRUCTURE

- Gas points are the backbone of Ethereum's transaction system. They represent a unit of computational work required to process transactions and execute smart contracts.
- Transactions on the Ethereum network involve fees, and these fees are specified in terms of Ether, the cryptocurrency of Ethereum.
- Gas points offer a standardized way to measure transaction costs, irrespective of Ether's market value. This stability makes it easier to predict and manage costs.

GAS POINTS IN TRANSACTIONS

- Every action performed on the Ethereum network consumes gas points. This includes sending Ether, invoking smart contracts, and executing other operations.
- Ethereum categorizes each type of operation with a specific gas cost. Miners calculate the total gas points needed for a transaction's execution during the mining process.
- A critical aspect is ensuring that the fees and gas points provided in a transaction are sufficient. Similar to mailing a letter without enough postage, transactions without adequate fees and gas points are rejected.
- To perform an action, the account initiating the action must have enough gas points in its balance. Any excess gas points after the transaction's execution are returned to the sender.



Operation name	Gas Cost
Step	1
Load from memory	20
Store into memory	100
Transaction base fee	21000
Contract creation	53000
...	...

GAS RELATED ITEMS IN BLOCKS

- **Gas Limit:** Each block in Ethereum has a predefined "gas limit," which signifies the maximum number of gas points that can be spent within that block.
- **Gas Spent:** This indicates the actual amount of gas points used up during the process of creating a block. It's the cumulative total of gas points utilized by all transactions within the block.

MINING INCENTIVE MODEL

- Ethereum's mining process employs a proof-of-work puzzle, and the miner who successfully solves it and creates a new block is rewarded.
- The rewards for block creation encompass both base fees and transaction fees. The miner receives a base fee of three Ethers along with the cumulative transaction fees present in the block.
- In addition to transaction fees, miners executing smart contract transactions within the block earn gas points for their efforts.

OMMERS AND OMMER BLOCKS

- In the mining process, several miners may solve the proof-of-work puzzle simultaneously, but only one can win the block.
- The miners who solved the puzzle but didn't win are referred to as "Ommers."
- The blocks they create are termed "Ommer Blocks" or "side blocks." These Ommer Blocks are integrated into the main blockchain structure.

- To encourage their contribution and enhance network security, Ommer miners are rewarded with a portion of the total gas points.

SUMMARY

- Ethereum's entire transaction ecosystem is underpinned by the concept of gas points. These points reflect the computational effort needed for different actions.
- Miners play a critical role in the network's functioning, and their efforts are compensated through various means: base fees, transaction fees, and gas points earned from executing smart contracts.
- This lesson provides a high-level overview of Ethereum's blockchain architecture.

LESSON 4 RESOURCES: INCENTIVE MODEL

The following resources were selected to provide an overview of the topic of Incentive Model. We would like to acknowledge the authors of the various web articles, videos, and papers for their insightful discussions and analytics which helped form the basis for some sections of the lessons and modules.

Title of resource: Vitalik Buterin Doubles Down on Ethereum Incentive Strategy

Resource type: Website

Description: An article written by Amy Castor that goes into Vitalik’s incentive strategy for Ethereum during the Workshop on Trusted Smart Contracts.

Title of resource: Ether

Resource type: Website

Description: Official website of ethereum that lists the most important things to know about ethers.

Title of resource: Proof of Work vs Proof of Stake: Basic Mining Guide

Resource type: Website

Description: This article will explain the main differences between Proof of Work vs Proof of Stake and will provide a definition of mining.

WEEK 3: ALGORITHMS & TECHNIQUES

PUBLIC-KEY CRYPTOGRAPHY

TWO STRONG SHIELDS

- When it comes to making sure a blockchain is secure and everything is accurate, two main techniques step in: hashing and asymmetric key encryption.
- These techniques rely on clever math tricks to keep things safe and organized.

WHAT'S THE PLAN

- This module aims to explain how these math tricks work and why they matter a lot for keeping the blockchain safe.
- It's divided into four parts: one about special codes for safety, another about checking if transactions are real, a third about making sure blocks are trustworthy, and finally, one about secret codes that keep blocks honest.

START WITH SECRET CODES: ASYMMETRIC KEY ENCRYPTION

- Imagine you have a secret club and only certain people can join. Asymmetric key encryption helps with this.
- Instead of using just one key, there are two keys: a public key (everyone can see) and a private key (only you know).

EASY SECRET MESSAGES: SYMMETRIC KEY ENCRYPTION

- Another way to keep things secret is by using secret passwords or codes. This is symmetric key encryption.
- It's like shifting letters in a message by a certain number. For example, "A" turns into "D" if you shift by 3. But in real life, it's more complicated.

PROBLEMS WITH SECRETS: SYMMETRIC CODES

- Using secret codes has some issues:
    1. People can guess the code from the secret message.
    2. Sharing the code safely is hard, especially when people don't know each other.

SMART SOLUTION: PUBLIC-KEY MAGIC

- Here comes public-key cryptography to solve these issues.

- It's like having a lock with two keys. One is your private key (super safe), and the other is your public key (you can show this one).
- These keys work so that even if you use one key to lock something, the other key can unlock it.

EXAMPLE: SENDING SECURE MESSAGES

- Imagine a person in Buffalo wants to send a secret message to someone in Kathmandu. Here's how it works:

    1. Buffalo locks the message with their private key (a personal secret code).
    2. Then, they lock the already locked message with Kathmandu's public key (a special lock for Kathmandu).
    3. When the message reaches Kathmandu, they use their private key to unlock the outer layer.
    4. Inside, they find the message locked with Buffalo's private key. They use Buffalo's public key to fully unlock the message.
    5. This way, only Kathmandu can read the message, and they know Buffalo sent it.

SPECIAL CODES: RSA AND ECC

- One special code is called RSA. It's famous for secret stuff and is used in many places.
- But for blockchains, we need faster and stronger codes. That's where ECC comes in.
- ECC is like a super-strong secret code maker used in Bitcoin and Ethereum. It's better because it's strong and quick.

SUMMARY

- Hashing and asymmetric key encryption are like superheroes keeping the blockchain safe.
- Public-key cryptography helps make sure only the right people join the party and secrets are safe.
- ECC is a super-secret code maker, making blockchains even more secure and speedy.

LESSON 1 RESOURCES: PUBLIC-KEY CRYPTOGRAPHY

The following resources were selected to provide an overview of the topic of Public-Key Cryptography. We would like to acknowledge the authors of the various web articles, videos, and papers for their insightful discussions and analytics which helped form the basis for some sections of the lessons and modules.

Title of resource: What Is Public-Key Cryptography?

Resource type: Website

Description: A look at the encryption algorithm and its security benefits

Title of resource: Asymmetric Cryptography (Public-Key Cryptography)

Resource type: Website

Description: Article explains what Asymmetric cryptography is and how it works

Title of resource: Public Key Cryptography - Computerphile

Resource type: Video (Run time- 6:19)

Description: YouTube video that explains how public key cryptography works.

Title of resource: Basic Intro to Elliptic Curve Cryptography

Resource type: Website

Description: Article explains ECC (Elliptic Curve Cryptography)

HASHING

IMPORTANCE OF ENCRYPTION HASHING

- Private-public key pair acts as a metaphorical passport for blockchain transactions.
- Similar to safeguarding a credit card, securing the private key is essential for asset protection.
- Hashing plays a critical role in ensuring blockchain's integrity and keeping transaction data confidential.
- Terms like hash rate and hash power are common in the blockchain realm, emphasizing the need for basic hashing knowledge.

UNDERSTANDING HASHING

- Hashing involves converting input data into unique fixed-length values.
- Input data could be documents, trees, or blocks.
- Even a tiny change in input data leads to a completely different hash output.

REQUIREMENTS OF A GOOD HASH FUNCTION

- The chosen algorithm must satisfy two crucial requirements.
- Firstly, it should be a one-way function—impossible to reverse-hash to obtain the original data.
- Secondly, it must be collision-free or exhibit an extremely low probability of collisions.
- Collision refers to different inputs producing the same hash output.
- This ensures that hashed data remains secure and reliable.

ENSURING HASH VALUE STRENGTH

- Achieving the requirements is done by selecting strong algorithms like secure hash functions.
- Using an adequate number of bits(256-512) in the hash value enhances security.
- Currently, the common hash size is 256 bits.
- Widely used algorithms include SHA-3, SHA-256, and Keccak-256.
- A 256-bit hash space offers an astronomically large number of possibilities: 2^256 or around 10^77 combinations.
- This level of uniqueness makes the chances of generating two identical 256-bit hashes negligible—comparable to the odds of a meteor hitting your house.

COMPARING HASHING TECHNIQUES

- There are **two** main approaches: Simple Hashing and Merkle Tree Hashing.
- **Simple Hashing** involves arranging data items linearly and then hashing them.
- Merkle Tree Hashing employs a tree structure where leaf nodes are pairwise hashed to reach the final hash value.
- **Merkle Trees** are efficient for varying data sizes and repeated operations.

WHEN TO USE EACH TECHNIQUE

- **Simple Hashing:**
  - Suitable when you have a fixed number of items, like in a block header.
  - Used for verifying the overall integrity of a composite block.
- **Merkle Tree Hashing:**
  - Applied when the number of items differs across blocks, such as transactions, states, or receipts.

- Efficient for accommodating variable-sized data and enhancing blockchain performance.

BENEFITS OF TREE-STRUCTURED HASH

- Merkle Trees improve the efficiency of operations and state changes between consecutive blocks.

HASHING'S ROLE IN ETHEREUM

- Hashing functions are pivotal for various aspects in Ethereum.
- They're used to generate account addresses, digital signatures, transaction hashes, state hashes, receipt hashes, and block header hashes.
- Common algorithms like SHA-3, SHA-256, and Keccak-256 are frequently utilized for hash generation in Ethereum's blockchain.

SUMMARY

- Hashing is a cornerstone of blockchain security and data integrity.
- Learning about hashing offers insights into the mechanics of blockchain transactions.
- Think of creating unique data fingerprints, ensuring confidentiality and trust in a decentralized environment.

LESSON 2 RESOURCES: HASHING

The following resources were selected to provide an overview of the topic of Hashing. We would like to acknowledge the authors of the various web articles, videos, and papers for their insightful discussions and analytics which helped form the basis for some sections of the lessons and modules.

Title of resource: What Is Hashing? Under The Hood of Blockchain

Resource type: Website

Description: An article that not only explains the basics of hashing but introduces a more specific type of hashing and how it affects the mining process.

TRANSACTION INTEGRITY

SECURING TRANSACTIONS THROUGH STEPS

- For reliable transactions in the blockchain, we focus on three main factors:

1. UNIQUE ACCOUNT ADDRESS

- Every participant in the decentralized network needs an exclusive identity.
- Achieved with a distinct account address using public-private key pairs.
- Steps to Create an Account Address:

  a. Generate a private key with a secure 256-bit random number.

  b. Keep this private key safe using a passphrase.

  c. Use an ECC algorithm to generate a unique public key from the private key.

  d. This forms the private-public key pair.

  e. To create a shorter account address (160 bits), hash the public key.

2. TRANSACTION AUTHORIZATION WITH DIGITAL SIGNING

- To ensure validity and sender confirmation of transactions:
- Achieved through digital signatures for non-repudiation and data integrity.
- Steps for Transaction Authorization:

  a. Hash and encrypt the transaction data, creating a digital signature.

  b. The receiver receives the original data and the digitally signed hash.

  c. The receiver recalculates the hash to confirm the data's integrity.

3. VERIFYING UNMODIFIED CONTENT

- Preventing changes to transaction content:
- Utilizes knowledge of hashing and public key cryptography.
- Steps for Verifying Unmodified Transactions:

  a. Calculate the hash of the transaction's data fields.

  b. Encrypt the hash using the sender's private key.

  c. Attach this encrypted hash to the transaction.

  d. Others can decrypt it using the sender's public key and compare the hashes.

LESSON 3 RESOURCES: TRANSACTION INTEGRITY

The following resources were selected to provide an overview of the topic of Transaction Integrity. We would like to acknowledge the authors of the various web articles, videos, and papers for their insightful discussions and analytics which helped form the basis for some sections of the lessons and modules.

Title of resource: How Safe Are Blockchains? It Depends.

Resource type: Website

Description: Article explains the inherent security risks in blockchain technology, by going into the differences between public and private blockchains.

SECURING BLOCKCHAIN

COMPONENTS OF AN ETHEREUM BLOCK

- Ethereum blocks consist of several vital components that together form the foundation of the blockchain's functionality.
- The main elements of an Ethereum block are the block header, transactions, and state information.
- The block header includes crucial metadata about the block, such as timestamps, a unique block number, the nonce (a random value used in proof-of-work), and more.
- Transactions represent the actions and data transfers occurring on the blockchain.
- In Ethereum, transactions are identified by their transaction hashes, and they are grouped together in a block.
- The state information refers to the current state of the blockchain, encompassing account balances, contract storage, and more.

ENSURING BLOCK INTEGRITY

- The integrity of the blockchain is maintained by guaranteeing that its components remain unaltered and tamper-proof.
- Blockchain's tamper resistance is achieved through cryptographic methods and consensus mechanisms.
- The header of each block contains a hash of the previous block's header, creating a chain of blocks.
- This chaining ensures that altering any data in a previous block would lead to a mismatch in the subsequent block's hash, quickly revealing tampering attempts.

HASHING AND SECURITY

- Hashing algorithms play a pivotal role in ensuring the security and integrity of blockchain data.
- A hash function takes an input (data) and produces a fixed-size output (hash value).

- Even a tiny change in the input data results in a vastly different hash value.
- Ethereum uses hashing extensively, such as in creating transaction hashes, state root hashes, and the block hash.

MERKLE TREES FOR EFFICIENCY

- Merkle trees (also known as hash trees) are employed to efficiently verify the integrity of large sets of data.
- Transactions within a block are structured in a Merkle tree, where each leaf node represents a transaction hash.
- Parent nodes in the tree store the hash of their children's hashes.
- This hierarchical structure allows for efficient validation of specific transactions without needing to verify the entire block.

SMART CONTRACTS AND STATE TRANSITIONS

- Ethereum's revolutionary feature is smart contracts—self-executing programs that automatically execute contract terms when predefined conditions are met.
- When a smart contract is executed, it can trigger changes in the blockchain's state.
- These changes, called state transitions, are recorded in the blockchain's blocks.
- Each state transition requires recalculating the state root hash to maintain blockchain integrity.

BLOCK HASH AND CHAIN FORMATION

- The block hash is a critical component of a blockchain as it encapsulates the block's content.
- Ethereum's block hash is computed by combining the block header details, transaction root hash, and state root hash.
- This composite hash value is used in the consensus mechanism, often based on proof-of-work, to secure the block.
- Additionally, the block hash from the previous block is included in the current block's header, forming the chronological chain of blocks.

IMMUTABILITY AND TRUST

- The unchangeable nature of blockchain records—immutability—is the cornerstone of its reliability and trustworthiness.
- Any attempt to alter past transactions or blocks would lead to a cascade of hash mismatches and immediate detection.
- This immutability fosters trust, making blockchain a foundation for secure transactions and data storage.

PUBLIC KEY INFRASTRUCTURE (PKI) AND SECURITY

- Public key cryptography is fundamental to blockchain security.
- Participants possess public and private key pairs that secure their transactions and interactions.
- Hashing is used in generating keys, signing transactions, and verifying signatures.
- These cryptographic methods underpin the decentralized and secure nature of blockchain networks.

BEYOND TRUST BOUNDARIES

- Blockchains extend trust beyond traditional boundaries, enabling interactions and transactions between unknown parties.
- The combination of cryptographic methods, consensus mechanisms, and immutability ensures secure data sharing and collaboration.
- This is particularly valuable in scenarios where parties lack a pre-established relationship or mutual trust.

SUMMARY

- Ethereum's blockchain comprises vital components like block headers, transactions, and state information.
- Integrity is upheld through chaining blocks, hashing, and cryptographic methods.
- Hashing ensures data security and tamper resistance.
- Merkle trees and state transitions contribute to efficiency and integrity.
- Block hashes secure blocks, transactions, and maintain chain continuity.
- Immutability and trust are maintained through cryptographic techniques.
- Blockchain operates as a secure trust layer beyond traditional boundaries, fostering new possibilities for decentralized collaboration

LESSON 4 RESOURCES: SECURING BLOCKCHAIN

The following resources were selected to provide an overview of the topic of Securing Blockchain. We would like to acknowledge the authors of the various web articles, videos, and papers for their insightful discussions and analytics which helped form the basis for some sections of the lessons and modules.

Title of resource: Securing the Chain

Resource type: Website

Description: Article talks about the high profile blockchain incidents that have occurred and how organizations should move forward.

Title of resource: Is It Chain of Headers Rather Than a Chain of Blocks?

Resource type: Website

Description: Bitcoin Stack Exchange is a question and answer site for Bitcoin cryptocurrency enthusiasts. Users comment on whether its chain of headers or chain of blocks.

Title of resource: What is a Block Header in Bitcoin?

Resource type: Website

Description: Article explains how to calculate and identify a block header.

WEEK 4: TRUST ESSENTIALS

DECENTRALIZED SYSTEMS

TRUST IN CENTRALIZED VS. DECENTRALIZED SYSTEMS

- Centralized Scenario (Airport System):
  - Trust established through a secure environment prepared by the airport authority.
  - Additional trust gained via verification of passports, travel documents, and baggage screening.
  - Further trust built as airline staff check boarding passes before allowing passengers to board.
- Decentralized Scenario (Blockchain):
  - Trust must be achieved without a central authority, relying on algorithms and techniques.

TRUST IN DECENTRALIZED BLOCKCHAIN

- Trust achieved by securing, validating, and verifying transactions, and ensuring resources for transaction execution.
- Securing:
  - Utilizes specific protocols to ensure the security of the blockchain.

- Validating:
  - Involves checking transaction criteria, such as syntax, timestamp, sender balance.
  - Also verifies resources like gas required for executing smart contracts.
- Verifying:
  - Involves confirming the authenticity of transaction signatures and hashes.

STEPS IN THE TRUST TRAIL

1. Validate transaction:
   - Scrutinize transaction criteria (e.g., about 20 criteria for Bitcoin, similar for Ethereum).
2. Verify gas and resources:
   - Ensure adequate gas and resources are available for executing smart contracts.
3. Execute transaction:
   - Compute the Merkle tree hash of validated transactions, forming the transaction root.
4. Compute state root:
   - Miners execute transactions, and the resulting state is used to calculate the Merkle tree hash of states (state root).
5. Compute receipt root:
   - Calculate the receipt root of the block header.

LESSON 1 RESOURCES: DECENTRALIZED SYSTEMS

The following resources were selected to provide an overview of the topic of Decentralized Systems. We would like to acknowledge the authors of the various web articles, videos, and papers for their insightful discussions and analytics which helped form the basis for some sections of the lessons and modules.

Title of Resource: Blockchain Based Trust & Authentication For Decentralized Sensor Networks

Resource type: Website

Description: The article contained on this website summarizes and explores decentralized authentication and node trust information.

Title of Resource: How the Blockchain will Radically Transform the Economy

Resource Type: Video - TEDtalk (Run time- 14:58)

Description: In this valuable TEDtalk of the complex (and confusing) technology, Bettina Warburg describes how the blockchain will eliminate the need for centralized institutions like banks or governments to facilitate trade, evolving age-old models of commerce and finance into something far more interesting: a distributed, transparent, autonomous system for exchanging value.

CONSENSUS PROTOCOL

SECURE CHAIN AND TRUST BUILDING

- A secure chain is a primary chain where all data is consistent.
- Each valid block added to this chain increases trust in the chain's integrity.
- Miners aim to add their blocks to this chain, competing with each other.

CHALLENGES IN AGREEMENT

- A challenge arises when multiple miners want to add their blocks simultaneously.
- Each miner's proposed block is from their effort in competition.

CHOOSING THE NEXT BLOCK - PROOF OF WORK

- The "Proof of Work" (PoW) concept addresses this challenge.
- PoW utilizes hashing, which is a mathematical process to convert data into a fixed-size value.
- Hashing is versatile and finds use in various applications.

FOCUS ON BITCOIN AND ETHEREUM

- PoW is essential in bitcoin and ethereum blockchains.
- Exploring this from a miner's viewpoint:

STEPS OF PROOF OF WORK (POW)

a. **Computing the Hash:**
   i. Miners calculate a hash of the block header combined with a variable called a "nonce."
   ii. The nonce value is changed iteratively to find the correct hash.

b. **Solving the Puzzle:**
   i. The objective is to find a hash value that is lower than a certain threshold.
   ii. In bitcoin, this threshold is below 2^128.
   iii. For ethereum, it's related to the blockchain's difficulty level.

c. **Verification and Broadcast:**
   i. If a miner finds a hash satisfying the threshold, they've solved the puzzle.

   ii. This winning block is then shared with the network for verification.

d. **Non-Winning Miners:**
   i. Miners who didn't find the solution continue with new nonce values.
   ii. They add the new block to their local chain copy and proceed to the next block.

e. **Incentives for Winners:**
   i. The miner who solves the puzzle gets rewarded for their effort.
   ii. This incentive encourages miners to invest computational power in securing the network.

PROOF OF WORK IN BITCOIN AND ETHEREUM

- Proof of Work is a consensus protocol used by these blockchains.
- While the protocol is the same, implementation details differ between bitcoin and ethereum.
- Developers continuously refine and optimize these implementations.

ALTERNATIVE APPROACHES AND ONGOING DEBATES

- Other consensus methods like Proof of Stake and Proof of Elapsed Time have been proposed.
- These approaches have sparked lively discussions among blockchain developers.
- You can actively participate and contribute to shaping the future of blockchain technology.

LESSON 2 RESOURCES: CONSENSUS PROTOCOL

The following resources were selected to provide an overview of the topic of Consensus Protocol. We would like to acknowledge the authors of the various web articles, videos, and papers for their insightful discussions and analytics which helped form the basis for some sections of the lessons and modules.

Title of Resource: A (Short) Guide to Blockchain Consensus Protocols

Resource Type: Website

Description: The article on this website summarizes the different types of proof.

Title of Resource: Review of blockchain consensus mechanisms

Resource Type: Website

Description: The article on this website summarizes the different types of proof.

Title of Resource: Blockchain Expert Explains One Concept in 5 Levels of Difficulty | WIRED

Resource Type: Video (Run time 17:49)

Description: This video provides a great explanation of blockchain at varying levels of comprehension. Blockchain, the key technology behind Bitcoin, is a new network that helps decentralize trade, and allows for more peer-to-peer transactions. WIRED challenged political scientist and blockchain researcher Bettina Warburg to explain blockchain technology to 5 different people; a child, a teen, a college student, a grad student, and an expert.

ROBUSTNESS

TRUST AND ROBUSTNESS IN BLOCKCHAIN

- Trust extends beyond regular operations to managing exceptions effectively.
- Robustness involves handling exceptional situations satisfactorily.
- Vital in decentralized systems like blockchains where intermediaries are absent.

EXCEPTIONS IN BLOCKCHAIN OPERATIONS

- Decentralized networks like blockchains encounter exceptions that need attention.
- The current lesson explores two specific exceptions, while more topics are planned for future courses.

EXCEPTION 1: CONSENSUS PUZZLE CONFLICT RESOLUTION

- Scenario: Multiple miners simultaneously solve the consensus puzzle.

1. **Bitcoin Protocol Approach:**
    a. Temporary allowance of two chains.
    b. Probability of simultaneous chain continuation is minimal.
    c. Winner's chain becomes the valid main chain and the chain which complete next cycle first and created block consider as winner chain.
2. **Ethereum Protocol Approach:**
    a. Introduces "Uncle" or "Omar" blocks.
    b. Incentive for miners whose blocks become Uncles.
    c. Enhances network security while managing simultaneous puzzle solutions.

EXCEPTION 2: TACKLING DOUBLE SPENDING

- Double Spending Defined:
    - The concern of using the same digital asset in multiple transactions.

    - Draws an analogy with the issue of airlines double booking seats.
- Intermediary Absence in Blockchain:
    - Unlike traditional systems, blockchains lack intermediaries for conflict resolution.
    - Need for an automatic and pre-defined way to handle such issues.

BITCOIN'S SOLUTION TO DOUBLE SPENDING

- Policy Establishment:
    - Bitcoin defines a clear policy.
    - The first transaction referencing a specific digital asset is allowed.
    - Subsequent transactions referencing the same asset are rejected.
- Ensuring Uniqueness:
    - Focuses on maintaining the uniqueness of digital asset use.

ETHEREUM'S APPROACH TO DOUBLE SPENDING

- Addressing Double Spending:
    - Ethereum employs a different method using a combination of an account number and a global nonce.
    - Each transaction from an account includes a global nonce, which increments with each new transaction.
    - Timestamped nonce guarantees the prevention of double usage of digital assets.

ENHANCED TRUST THROUGH EXCEPTION MANAGEMENT

- Well-Defined Processes:
    - Clearly defined processes for handling exceptions significantly bolster trust in the blockchain.
- Upcoming Lesson Highlights:
    - Future lessons will delve into more complex topics, including difficulty adjustment, fork management, and others.
- Gaining a Holistic Understanding:
    - By understanding these key exceptions, participants gain a holistic perspective on blockchain's reliability and functioning.

LESSON 3 RESOURCES: ROBUSTNESS

The following resources were selected to provide an overview of the topic of Robustness. We would like to acknowledge the authors of the various web articles, videos, and papers for their insightful discussions and analytics which helped form the basis for some sections of the lessons and modules.

Title of Resource: How The Blockchain Is Redefining Trust

Resource Type: Website

Description: This helpful article highlights how the blockchain can remove intermediaries from numerous transactions between people, corporations, and a host of other financial interactions.

FORKS

UNDERSTANDING TRUST AND FORKS IN BLOCKCHAIN

- Trust and robustness are vital aspects in blockchain technology.
- "Forks," including hard and soft forks, are often discussed in the blockchain context.
- Ethereum's hard fork at block 4.7 million serves as a notable example.
- These forks play a pivotal role in maintaining the integrity of blockchain networks.

FORKS AS NATURAL PROGRESSION

- Forks are akin to the branching paths in the evolution of blockchain technology.
- They represent stages of development and improvement.
- Forks, whether soft or hard, are mechanisms that contribute to blockchain's adaptability and resilience.
- Their significance lies in handling both planned enhancements and unforeseen challenges.

DIFFERENTIATING SOFT AND HARD FORKS

- **Soft Fork:**
    - Comparable to releasing software patches or updates.
    - Introduces changes while ensuring compatibility with previous versions.
    - A minor process adjustment for better efficiency or security.
    - Facilitates a seamless transition without creating incompatible branches.

- **Hard Fork:**
  - Signifies a more substantial change in the blockchain's protocol.
  - May result in the creation of two incompatible chains.
  - Can be planned or emerge due to unplanned circumstances.
  - Marks a significant shift in the blockchain's direction or capabilities.

ETHEREUM'S PLANNED HARD FORK - OCTOBER 17, 2017

- An illustrative example is Ethereum's planned hard fork on October 17, 2017.
- Ethereum Improvement Proposals (EIPs) drive this planned change.
- EIPs encompass multiple improvements to enhance the Ethereum network.
- A key change involves the introduction of parallel processing of transactions.
- Proof of Stake (PoS) consensus is intermittently used with Proof of Work (PoW).
- A reduction in the minor incentive for block creation from 5 ethers to 3 ethers.
- EIPs embody a collaborative approach to advancing blockchain capabilities.

IMPORTANCE OF MANAGED FORKS

- Forks, whether soft or hard, bolster the robustness and credibility of blockchains.
- Skillful management of forks is integral to the blockchain's long-term success.
- Managed forks exhibit the adaptability of the technology in addressing challenges.
- They showcase the blockchain community's capacity to learn, evolve, and enhance the ecosystem.

EVOLVING THROUGH PLANNED HARD FORKS

- Currently, Ethereum's transition from Homestead to Metropolis exemplifies a planned hard fork.
- Observing this planned transition provides a valuable opportunity for learning.
- The blockchain's ability to manage and implement forks signifies its dynamic nature.

LESSON 4 RESOURCES: FORKS

The following resources were selected to provide an overview of the topic of Forks. We would like to acknowledge the authors of the various web articles, videos, and papers for their insightful discussions and analytics which helped form the basis for some sections of the lessons and modules.

Title of Resource: Have Blockchain Forks Shown Hayek to be Right or Wrong?

Resource Type: Website

Description: This valuable article explores the concept of free market money as proposed by Friedrich Hayek in the 1970's and its relationship to Blockchain and Bitcoin.

Title of Resource: Split on Forks? Blockchain Leaders Learn Tough Lessons from Bitcoin Scaling

Resource Type: Website

Description: This website focuses on how developers need to find ways to conduct upgrades to bitcoin in a smoother manner.

Title of Resource: Bitcoin, Blockchain Forks & Lightning

Resource Type: Video (Run time- 8:40)

Description: In this helpful video, an employee of UCL Security Group summarizes theories to scale bitcoin.