NATIONAL INSTITUTE OF TRANSPORT

Blockchain Technology Training

Introduction to Blockchain

Facilitator: Dr. Cleverence Kombe (PhD)

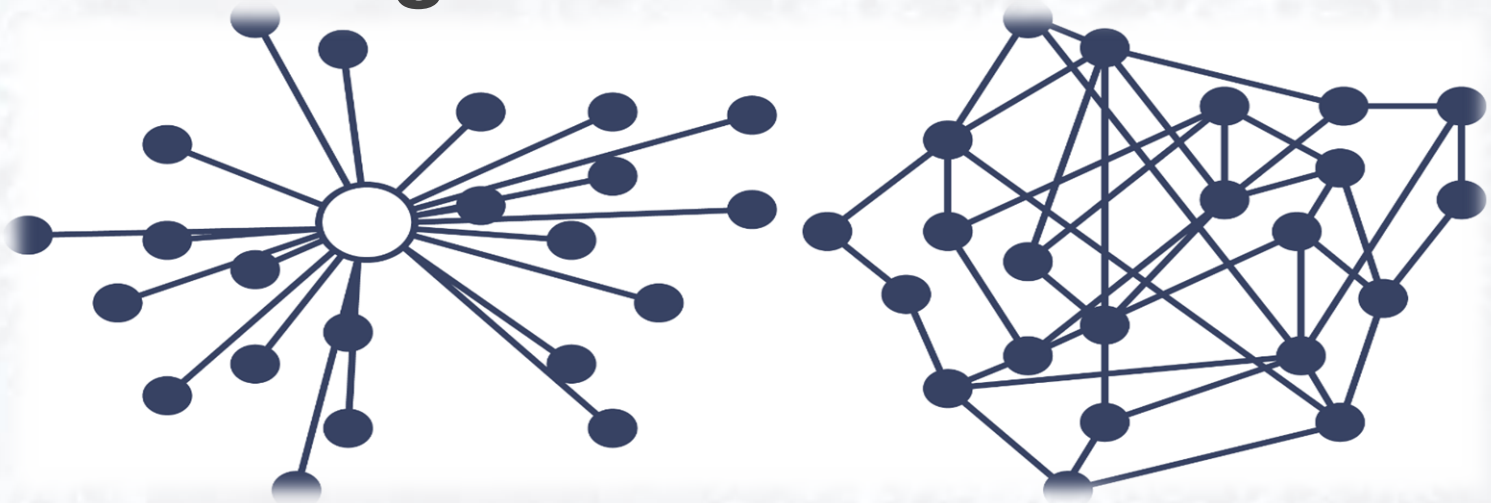
Introduction to Blockchain | Overview

- Discuss blockchain technologies and the early Internet
- Discuss blockchain features
- Explain blockchain components
  - *Explain what the block in blockchain is*
  - *Explain how blocks are chained together*
  - *Discuss the concept of immutability in a blockchain*
- Cryptography in Blockchain

Introduction to Blockchain and The Early Internet

Blockchain | Definition

- **Blockchain** is a is a **peer-to-peer ledger** system that allows peers to transact directly with each other **eliminating the need** for a **central authority**



Blockchain | Definition

- At its core, blockchain is a system for **recording information** about **a transaction** in a new **decentralized way** that **makes it difficult** or **impossible to alter**.

- These transactions are **stored on sheets** or **blocks** in a **digital ledger** that is **shared** among the **participants of the network**

Blockchain | Definition

- **Consensus** on the transactions, **brings the peer-to-peer network** into **agreement**

- Once **the agreed-upon transactions blocks** are **recorded in the immutable ledger**, **trust** becomes a **fundamental component** built into **the system**

The Early Internet

- What started as a **DARPA (Defense Advanced Research Project Agency)** experiment in decentralized computing communications between two university labs in California in 1970, became the **Transmission Control Protocol/Internet Protocol**

- **INTERNET PROTOCOL SUITE (TCP/IP)** developed as a standard in networking protocol or computer communication standards, and it is the **backbone of today's Internet**.

- With the TCP/IP protocols in place, **users had the ability to link hypertext documents** in an information system accessible from any node or computer using the TCP/IP protocol.

- The resulting information system or database is today's **World Wide Web**.

The Early Internet

- With the birth of the World Wide Web, expanded usages of this new technology arose along with expanded **business opportunities**.

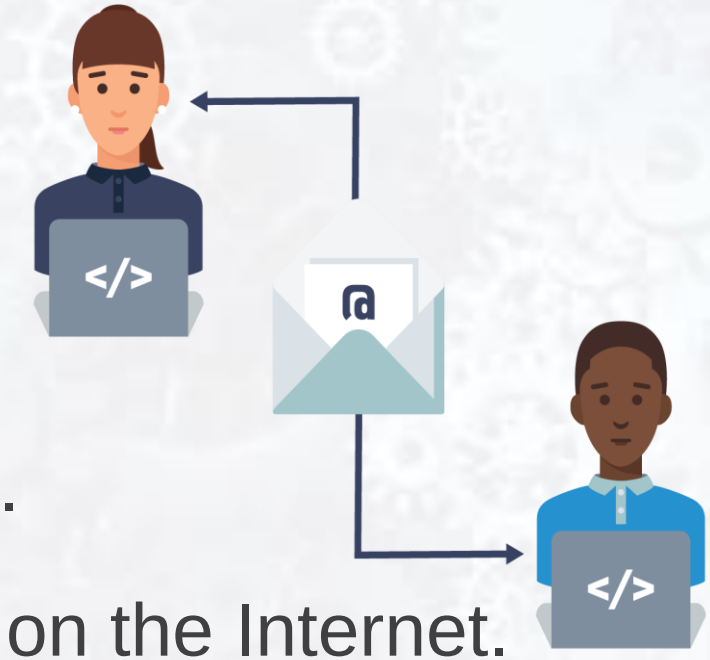
- Web servers, people who host and store the documents and web browsers, companies set up to help you view linked documents, help create a household need for this technology and the **Internet explosion began**.

The Growth of the Internet

- The Internet can be grouped into **three distinct segments** characterized by the way people interact with this new technology.
  - **Web 1.0 - Internet of Connection**
  - **Web 2.0 - Internet of Information**
  - **Web 3.0 - Internet of Value**

The Growth of the Internet | Web 1.0 - Internet of Connection

- Characteristics of Web 1.0:
  - Development of a host of **web-based applications**, which fostered in **online services**, such as **email**.
  - Content from **administrator**.
  - Managed by a **central authority**.
  - **Read-only**, information was “pushed” to users.
  - **Email** was the first widely adopted application on the Internet.



The Growth of the Internet | Web 1.0 - Internet of Connection

- Computers and items for connection became **necessities.**

- **Technology advancements** in computers brought on changes, **floppy disks became hard drives** that stored MB that turned into GB that turned into TB.

- **Internet speeds** switched from **kilobits to tens of megabits per second**, to **gigabits per second** and **RAM grew** from **hundreds of kilobytes to gigabytes** and the **dot-com bubble began**.

- Companies appeared attempting to cash in on this new technology, most notable was a company called **Netscape** which developed the **first commercial Web browser.**

 *- Netscape Logo*

The Growth of the Internet | Web 2.0 - Internet of Information

- Characteristics of Web 2.0:
  - User-generated **content**.
  - **Read-write**, individuals can **interact with information**.
  - Information became **siloed**.
  - **Data** became a **commodity**.

Real World Examples of File Sharing: Use Case | Music Sharing Companies

- **Approach:** Music stored on **many computers connected peer-to-peer**. Napster software supplied its users with a **centralized index of all music files** and directed users to where these files were located **on the connected peers' computers**.

- **Result:** The industry cracks down music sharing companies **copyright infringement**. Napster is forced to take **down its index**, shutting down the platform.

Real World Examples of File Sharing: **Use Case | Music Sharing Companies**

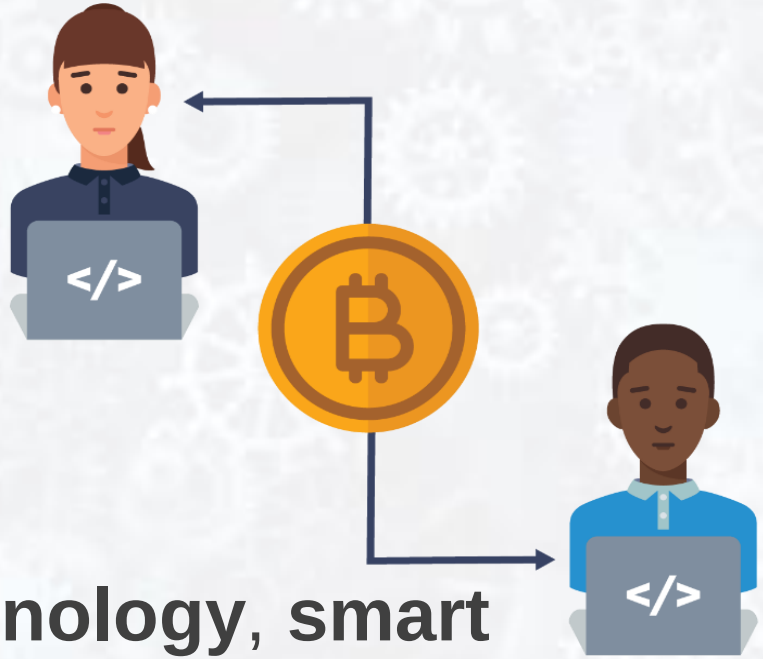
- **Approach:** Music stored **on many computers** connected **peer-to-peer**. BitTorrent's software was **purely decentralized**, the files were stored as **packet on the peers' computers** and when a request was made for a song, the software would find the **packet** and **send it to the user**.

- **Result:** The industry cracks down music sharing companies **copyright infringement**. BitTorrent **is asked to shut down** their platform. Since they do **not control the software once downloaded** to a peer, if two computers are running the software **sharing can still occur**

The Growth of the Internet | Web 2.0 - Internet of Information

- Music sharing companies gave us the **first glimpse** into **peer-to-peer networking**.
- Besides copyright infringement, the main challenge for the music sharing companies was **file integrity**.
- You could **never be sure the file you requested** was the **file you would get** and there was **no one to complain to**.
- Both **Napster** and **BitTorrent** are operating today, with different business models.

The Growth of the Internet | Web 3.0 - Internet of Value



- Characteristics of Web 3.0:
  - Community **interaction**.
  - More connected, open, and intelligent.
  - **Distributed ledgers** or **blockchain technology**, **smart contracts**, machine learning and artificial intelligence.
  - Identity and information will be held by the individual, breaking data silos.

The Growth of the Internet | Web 3.0 - Internet of Value

- **Bitcoin** is the **first widely accepted application** for the **Internet of Value** (just as **email** was the **first big application** for the **Internet of Information**).

- The **Internet of Value** represents a world where **value is exchanged at the speed** in which information **moves today**.

- The **Internet** is still the **basic platform** that these new technologies operate from.

- The new **Web 3.0 browsers are being built** to help you manage your **cryptocurrency**, **keys**, **passwords** and **other blockchain features**.

Blockchain Basics

Blockchain Basics

- A block on a **blockchain** can be thought of much like a page in a **notebook**.

- Data is **stored on a block**, just like **data is written** on a page of a **notebook**.

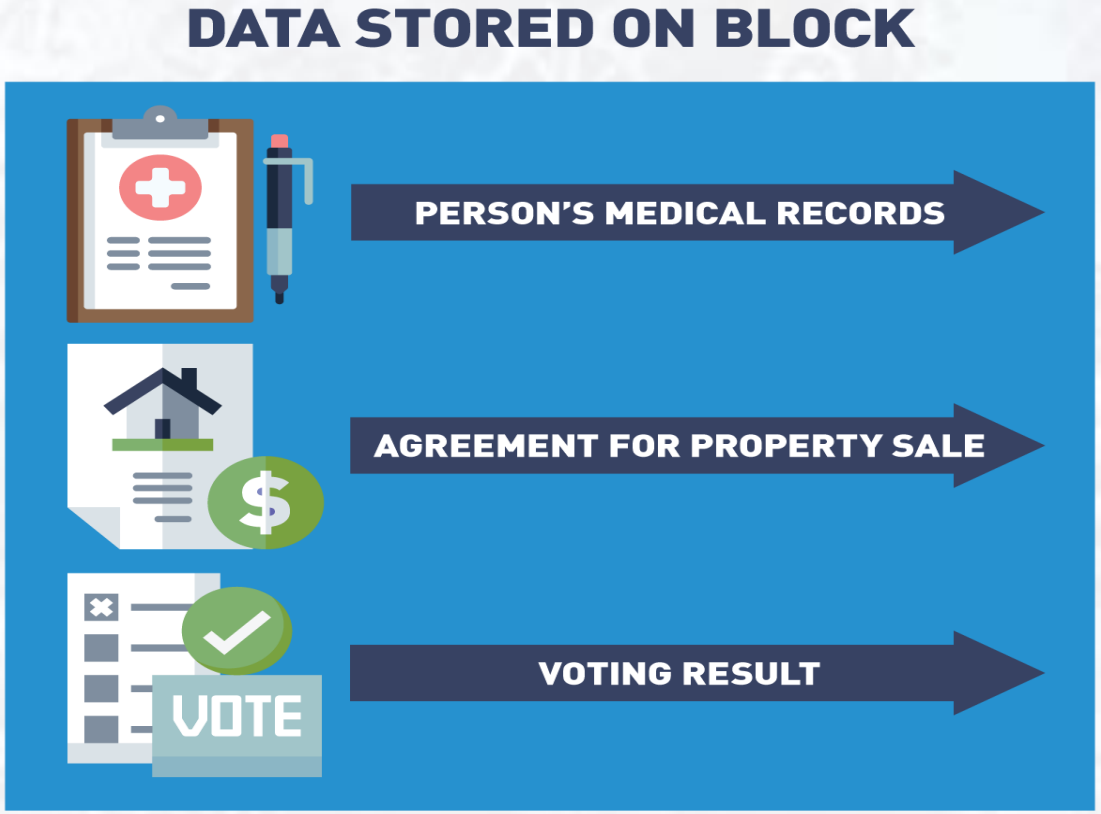
- Similar to **a sheet of paper**, the digital ledger doesn't care what kind of information you're putting on it.

- So, while most of what we're recording today **are financial transactions**, we could also record things like voting records and results, **land titling** and **medical records**, etc.

Blockchain Basics | Data Stored

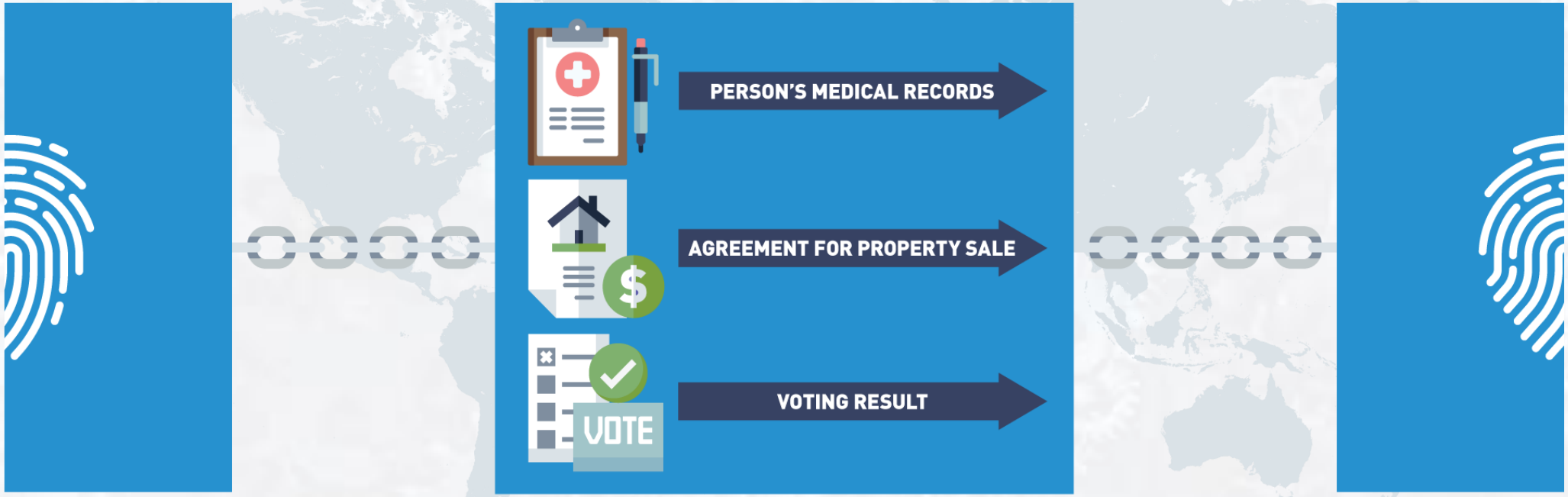
- Any data can be stored on the same block.

- Examples of **stored data** include:
  - **Medical records**
  - **Property agreements**
  - **Voting**



Blockchain Basics | Blocks Are Chained Together

- Each block is **chained or tied** to the **previous block** by **embedding the block** with **information from the previous block** (we will go through this in depth later in the course).



Blockchain Basics | Blockchain Is Immutable

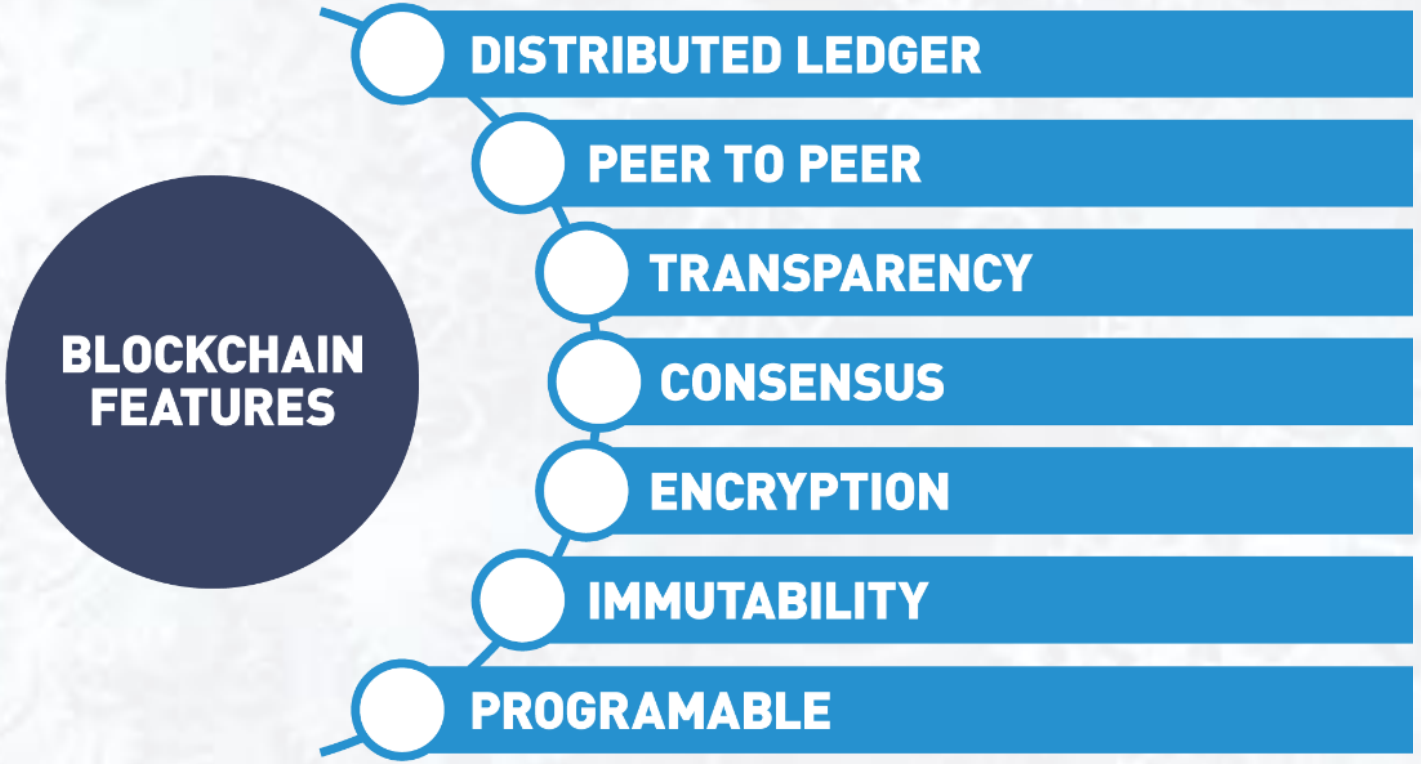
- If the **data** is tampered with **anywhere in the chain**, the links will break in a very obvious way:

This provides immutability and security.

Blockchain Features

Blockchain Features

Blockchain is a **combination** of several other **underlying technologies** that have **never been combined so successfully**.



Blockchain Features | Distributed Ledger

- A ledger is a **collection of transactions**, it is **not** a **collection of assets**.
- Assets are **part of a transaction**, but the ledger records the transaction.
- With a digitally distributed ledger or a blockchain, **no one owns the ledger**.
- The ledger is **distributed among participants** in the network, all running the **same blockchain protocols**.

Blockchain Features | Distributed Ledger

- It is decentralized in that an identical copy of the ledger exists on every node/computer on the network.

- In 2009 with the publishing of Satoshi Nakamoto's whitepaper "***Bitcoin: A Peer-to-Peer Electronic Cash System***" , Bitcoin became the first application to leverage blockchain technology by **recording the first asset** transfer on a **public blockchain ledger**.

Blockchain Features | Peer to Peer Network

- The ledger is **stored**, **updated**, and **maintained** by a **peer network**.
- Nodes form the **infrastructure** of a **blockchain network**.
- They **store**, **spread** and **preserve** the **blockchain data**, so a blockchain **exists on nodes**.
- All nodes on a **network follow the same rules of operation or protocols**, but nodes **have different roles**.

Blockchain Features | Peer to Peer Network

- A **full node** contains a **copy of the blockchain protocol**, **transaction history of the blockchain** and **aids in the maintenance** of the blockchain.
- **User node** interacts with the ledger.
- With blockchain technology, a **lack of a centralized authority** is replaced with a **peer-to-peer network**.

Blockchain Features | Peer to Peer Network

- Blockchain **networks** can be **public** or **private**.
- A **public blockchain** is **open to anyone** with an **internet connection** and the **appropriate application**.
- A **private blockchain** grants **access and rights to its users** before they can interact.

Blockchain Features | Transparency

- In a blockchain, we can **see all the transactions** that have occurred on **the shared** or **distributed ledger**.

- A blockchain **stores details of every transaction** that occurred **since the first transfer**.

- This **first transfer**, along with some system information that we will discuss later, **becomes the first block in our chain** and is referred to as **the genesis block**.

Blockchain Features | Transparency

- Since **every node shares a copy** of the agreed-upon ledger, there **is no friction about the transactions**, everyone has the **same agreed-upon copy**.

- Centralized systems **are not transparent**, the information about the ledger is **controlled by one authority**.

Blockchain Features | Consensus

- Blockchain ledgers are **different from centralized ledgers** because **network participants have an agreement** upon what is in the **identical ledger**.

- In order for the blocks to be added, **all the nodes in the system come to agree** as to what **transactions are accurate** and should be **added to the chain of blocks**.

- Since there is no central authority telling the nodes which transactions are valid, a **new way to reach agreement** or come to **consensus is needed**.

Blockchain Features | Consensus

- The way in which each blockchain comes to consensus is built into **the protocol**, they **are the rules built into the code** that determine **how the nodes will add ledger transactions**.

Blockchain Features | Consensus

- The **Ethereum network** uses a **proof of work consensus model and proof of stake**.
- The **Hyperledger fabric network** uses modular consensus model that allows for pluggable consensus algorithms such as **Kafka**, **Raft,** and **PBFT** consensus algorithms
- This process of building agreement among a group of mutually distrusting participants is **a benefit of blockchain consensus**.

Blockchain Features | Encryption

- **Encryption** and **cryptography** are combined with **blockchain technology** to **assure** the information on the blockchain **is authentic**.

- In our previous real-world example, the music sharing companies **not only had legal issues** from **copyright infringement**, they also **could not solve the data integrity problem**.

- Music downloaded from these platforms was only as reliable as the **anonymous person storing** and **sending it**.

- The **data had no integrity**.

Blockchain Features | Encryption

- **Cryptography** and **blockchain** offer a **secure way to prove something is authentic**.

- Instead of **relying on third-party**, **trust** is put into **cryptographic algorithms** that prove the **provenance and authenticity of an attestation**.

Blockchain Features | Immutable

- **Cryptography** also plays a part in **another powerful feature** of blockchain technology, **immutability**.

- What makes blockchain **incredibly powerful** is that all the blocks are **linked together**.

- With the use of a **cryptographic technique** called **hashing**, the linked information is forged so that if you go back and try to **change any data on any block anywhere in the shared ledger**, the **link with the other copies is broken** in **a very obvious** and **easy-to-determine** way

Blockchain Features | Immutable

- With **blockchain**, there is **no possibility of changing the data** or **altering the data inside the blockchain**, it is **permanent**.

- In a **traditional database**, a **system administrator oversees** the ledger and **can make changes**.

Blockchain Features | Programable

- Smart contracts are a powerful feature offered by certain blockchains, enabling the **implementation of logic** and **rules** within the system **to automate and enforce agreements**.

- While the Bitcoin blockchain functions as a simple calculator for **recording financial transactions**, other blockchains operate more like computers, allowing for a **wider range of functionalities**.

Blockchain Features | Programable

- Ethereum was the first blockchain to introduce **smart contracts**, which are enforced by the **Ethereum Virtual Machine (EVM)**.

- Through the **EVM**, Ethereum **enables the creation of secure and decentralized digital agreements**, or smart contracts, that can **execute automatically and without the need for intermediaries**.

Blockchain Features | Programable

- **Blockchain smart contracts** allow for the **creation of trustless protocols**.
- This means that **two parties** can **make commitments** via **blockchain**, without having **to know** or **trust** each other.
- They **can be sure** that **if the conditions aren't fulfilled**, the **contract won't be executed**.
- Other than that, the **use of smart contracts** can **remove the need for intermediaries**, **reducing operational costs** significantly.

Cryptography in Blockchain

Cryptography | Cryptography Key Terms

►Cryptography

- Cryptography is a **technique used to secure the communication** between **two parties** from **a third**. The term cryptography is derived from two ancient greek terms, **“*kryptos*”** which means **“hidden”** and **“graphein”** which means **“to write”.**

►Secrets

- The data which we are trying to protect.

►Key

- A piece of data used for encrypting and decrypting the secret.

►Function

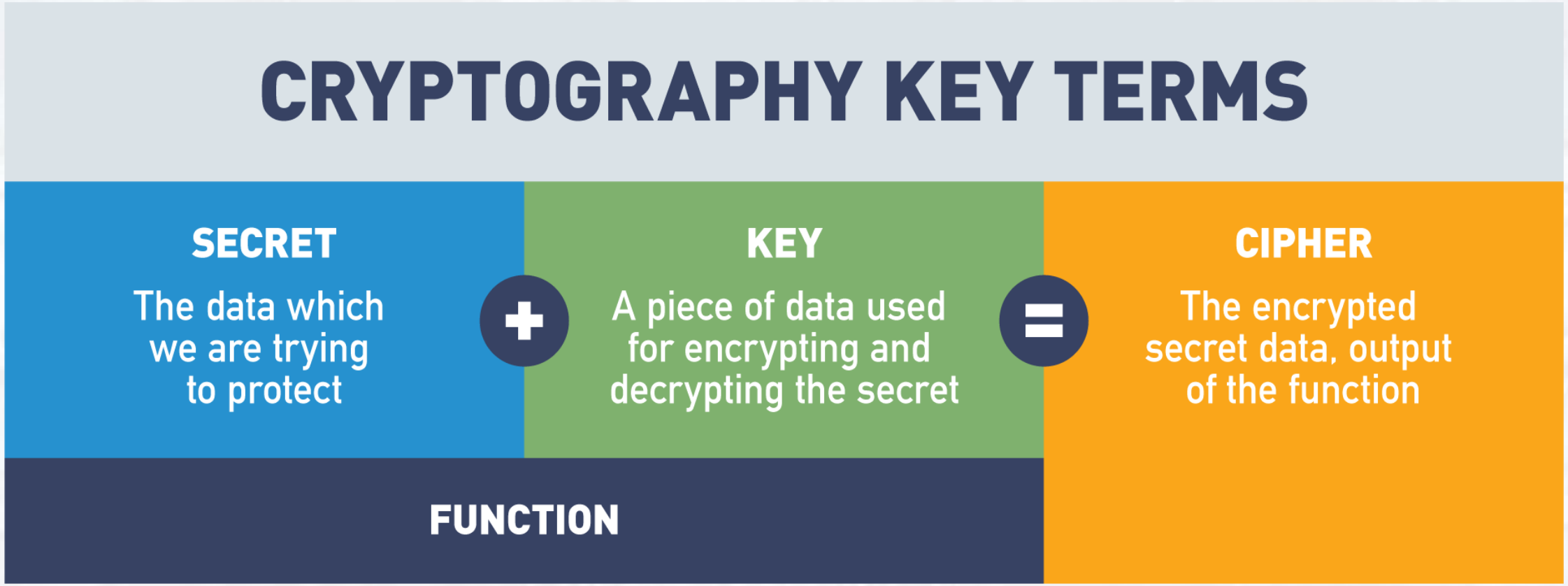
- The process or function used to encrypt the secret.

Cryptography | Cryptography Key Terms

- **Cipher**
  - The encrypted secret data, the digital secret, the output of the mathematical function or a cryptographic algorithm
- **Encryption**
  - This is the process from plain text (ordinary text) to cipher text (random sequence of bits)
- **Decryption**
  - Encryption is the reverse process of converting ciphertext into plain text

Cryptography | Cryptography Key Terms

The Secret and the Key are passed into the Function to create the Cipher



Cryptography | Cryptographic Functions

- **Simple example function:**
  - **Secret = "*Blockchain technology is transformative*"**
  - **Function = Swap each letter in the secret with a new letter according to the Key**
  - ***Key* = *"+2"***
  - **Cipher = *"Dnqemejckp vgejpqnqia ku vtcpuhqtocvkxg"***

Cryptography | Cryptographic Functions

- In the 1970s, cryptologists Whitfield Diffie and Martin Hellman invented "**Asymmetric Key Encryption**".
- This concept is used by **HTTPS**, the popular protocol for **accessing secure web servers,** as well as the **secure element within a token**.
- Asymmetric Key Encryption uses separate **encryption and decryption keys**, instead of a **shared key**, to keep information private.
- This groundbreaking invention has revolutionized online security by enabling secure and private communication over the internet.

Cryptography | Cryptographic Functions

- **Asymmetric Key Encryption** enables sending secret messages without knowing the **receiver's identity**.
- The **private key**, which is essential for secure authentication and identity protection, is never shared.
- As a result, there is no need to share secrets with others.

Cryptography | Types of Cryptography in Blockchain

Four main ways Blockchain leverages Cryptography

1. **Public Key Cryptography**

   This encryption method uses a pair of keys: an encryption key, and a decryption key, named public key and private key, respectively. The key pair generated by this algorithm consists of a private key and a unique public key that is generated using the same algorithm

2. **Merkle Trees**

   A data storage technique that compresses or packs data for storing blockchains with a tamper-free component built in. Merkle trees are built upon hashing principles in that each hash becomes a part of the next hash to build a tamper resistant data storage model

Cryptography | Types of Cryptography in Blockchain

Four main ways Blockchain leverages Cryptography

3. Hash Functions

This type of encryption doesn't make use of keys. It uses a cipher to generate a hash value of a fixed length. The function converts plain text (no matter the size) into a hash of fixed size. It is nearly impossible for the contents of plain text to be recovered from the cipher text.

Think of it like trying to recreate a human from a fingerprint, a fingerprint uniquely represents a human no matter the size of the human and you can't reverse engineer a fingerprint to recreate the human

4. Zero-Knowledge Proofs

Zero-Knowledge Proofs is an innovative technique for safeguarding digital secrets. It enables individuals to prove that they possess knowledge of a secret without having to disclose it.

Cryptography | Public Key Cryptography

- **Identity** in the blockchain is based on **public key cryptography**

- A **person's address** on the **blockchain** is their **public key**

- **Transactions on** the blockchain include **their public key** and are **digitally signed with the sender's private key**:
  - A **digital signature verifies** that **someone in possession of the private key authorized** the **transaction**
  - Digit**al signatures** can be **easily verified** using the **corresponding public key**, which is **included in the transaction**

Cryptography | Public Key Cryptography

Public key cryptography is how identity is handled on the blockchain.
A user's address on the blockchain is their public key.

THIS HAS SEVERAL USEFUL PROPERTIES:

1. Users don't need to reveal their real identity on the blockchain but can positively identify themselves since determining their private key requires solving a hard problem
2. Anyone can send a user an encrypted message since they have easy access to their public key
3. Users can verify the validity of their transactions using digital signatures

Cryptography | Public Key Cryptography

Identity: RSA Public Key Cryptography

ANYONE CAN VERIFY THE SIGNATURE USING A SIMPLE THREE-STEP PROCESS

1. Condense the attached message using the same method as the message writer
2. Raise the attached signature to the user's public key
3. Verify that the results of the previous two steps are identical

Cryptography | Public Key Cryptography

Identity: Specific Identity Implementations

- **Ethereum** is a **public blockchain** that **anyone can participate in.**
  - *A user's identity is an address based on their public key*
- **Hyperledger** is an **example of an enterprise blockchain** where **participants must be granted access to engage in the blockchain**
  - *Identity is managed by X.509 certificates. Certificates are only shared with parties involved in the transaction*
- **Public key cryptography** uses a **pair of a public key and a private key to perform different task**
- **Public keys** are widely **distributed,** while **private keys** are **kept secret**

Cryptography | Public Key Cryptography

Identity: Specific Identity Implementations

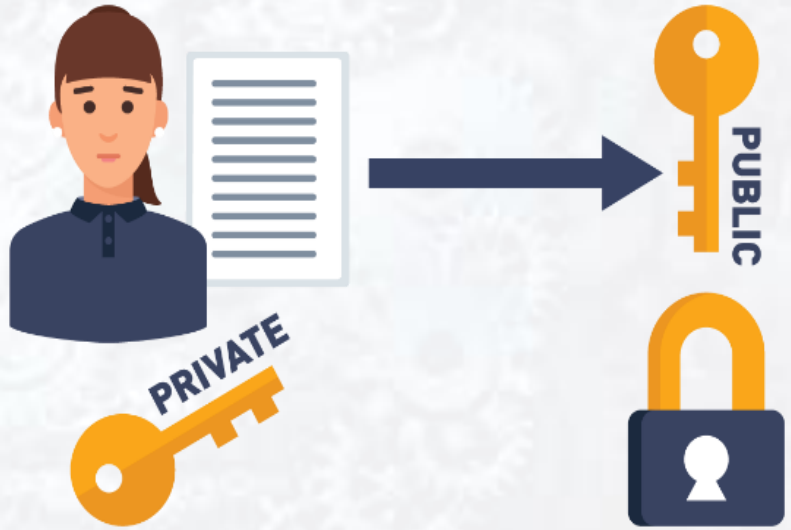
- Using a **person's public key,** it is possible to **encrypt a message** so that **only the person** with the **private key** can **decrypt and read it**
- Using a **private key, a digital signature** can be **created** so that **anyone with** the corresponding **public key** can **verify** that the **message was created by the owner** of the **private key and** was not **modified since**

Cryptography | Public Key Cryptography

Identity: Specific Identity Implementations

Digital Signatures and Key Pairs

Step 1



Cryptography | Public Key Cryptography

Identity: Specific Identity Implementations

Digital Signatures and Key Pairs

Step 2

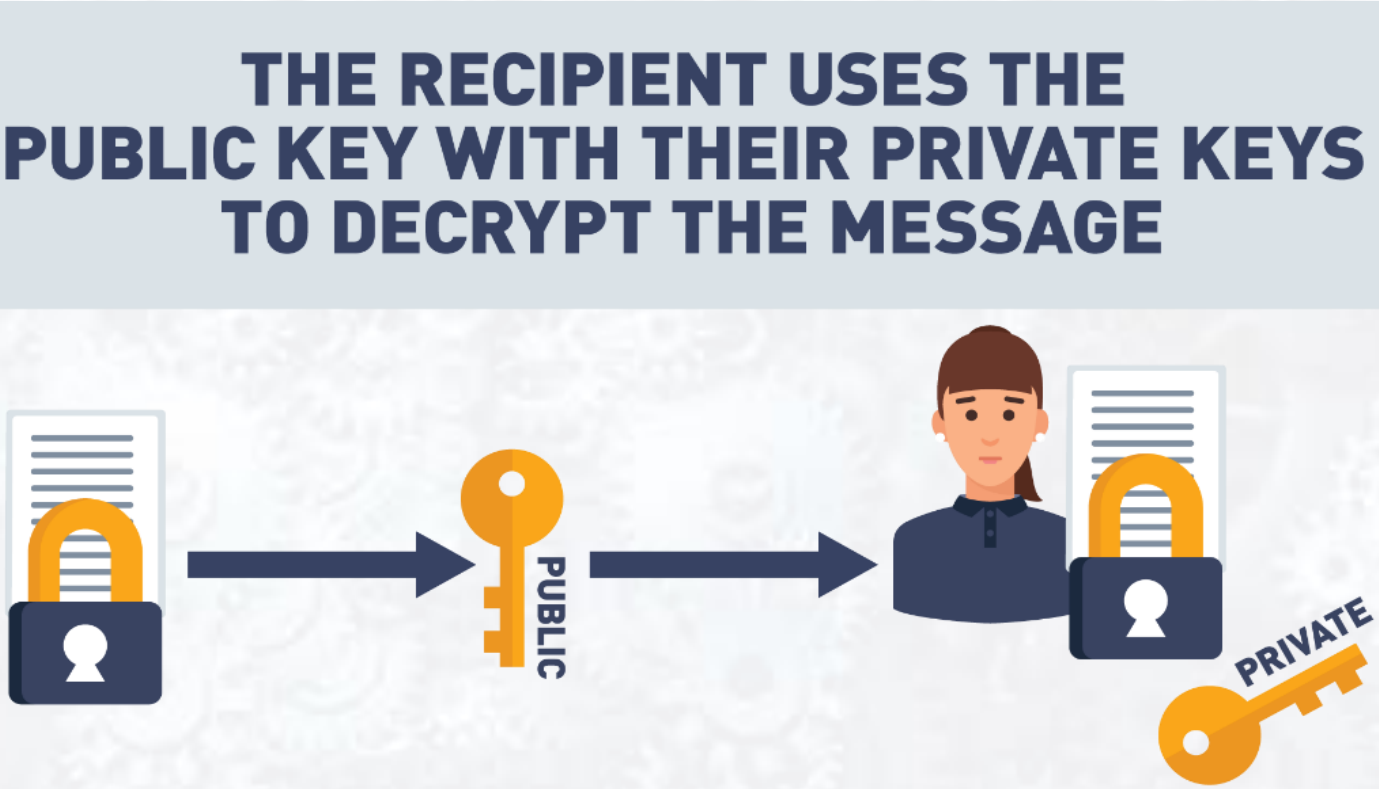
THE SENDER ENCRYPTS MESSAGE USING THE KEY PAIRS. AND SENDS IT.

Cryptography | Public Key Cryptography

Identity: Specific Identity Implementations

Digital Signatures and Key Pairs

Step 3



Cryptography | Hash Functions in Blockchain

- When using blockchain, the need to trust a central authority to verify the accuracy of data is removed and replaced by trust in a cryptographic hashing function
- With data integrity guaranteed by algorithms, trust becomes part of the system
- Blockchain provides users with data integrity in a trustless environment
- This is accomplished using cryptography in a way that moves the burden of trust from data processors to cryptographic algorithms

Cryptography | Hash Functions in Blockchain

- Hash functions are featured heavily in blockchain. A hash function is a mathematical equation with four important properties:

1. Hash functions can take anything as input and create an output with a fixed size. This makes it possible to condense anything into a piece of data of a fixed size and is how messages are condensed for digital signatures

2. It's easy to calculate a hash, but hard to determine a hash input from the output. The best option is to keep trying inputs until one produces the desired output

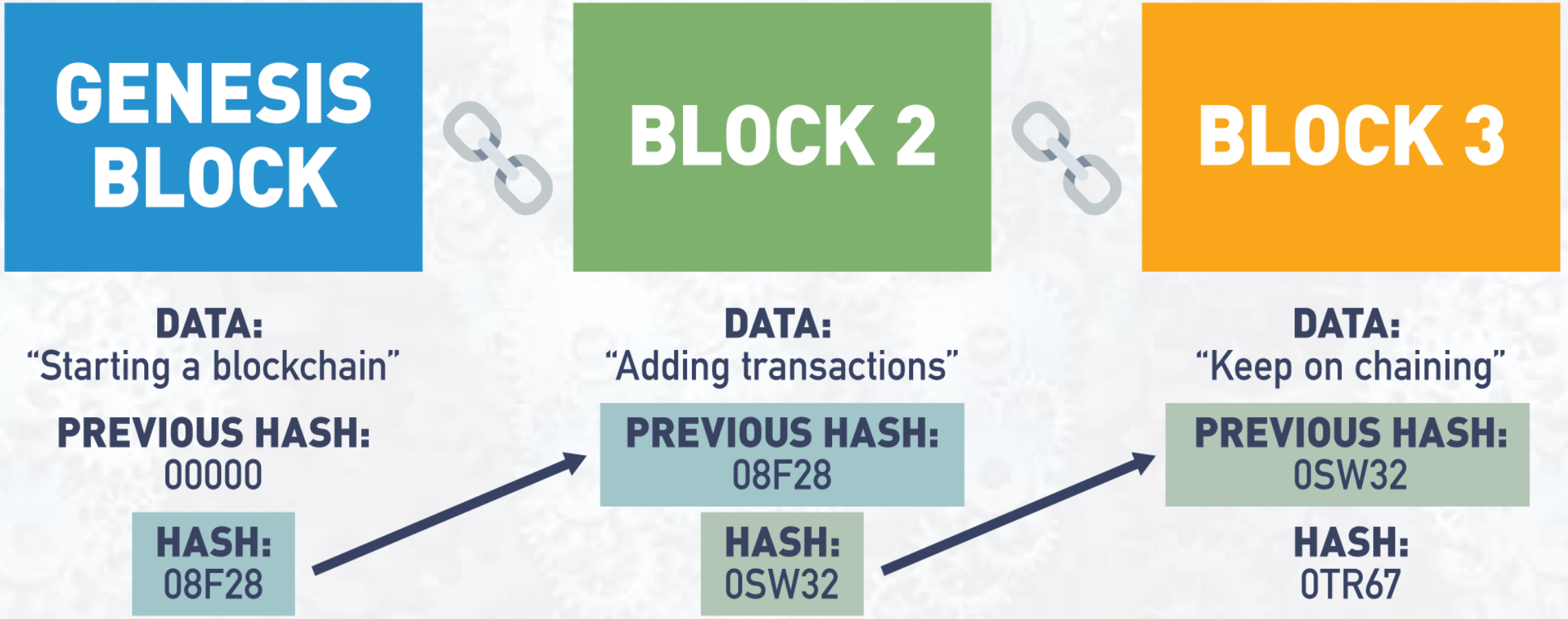
Cryptography | Hash Functions in Blockchain

- Hash functions are featured heavily in blockchain. A hash function is a mathematical equation with four important properties:

3. Inputs that differ by a single bit produce hashes that differ by half of their bits on average. This prevents someone from finding a desired hash input using a “hill climbing”

4. It is infeasible to find two inputs that produce the same output when hashed. Since a hash can take any input and produce a fixed output, it makes sense that multiple different inputs will create the same output. A good hash function will make it so that you have to try a large number of inputs before finding two that produce the same output

Cryptography | Hash Functions in Blockchain



Cryptography | Hash Functions in Blockchain

► ***Lab 1: Hashing***

- Next, let's engage with an interactive lab.
- This lab is an actual hands-on demonstration of taking data and creating a hash output. Enjoy!

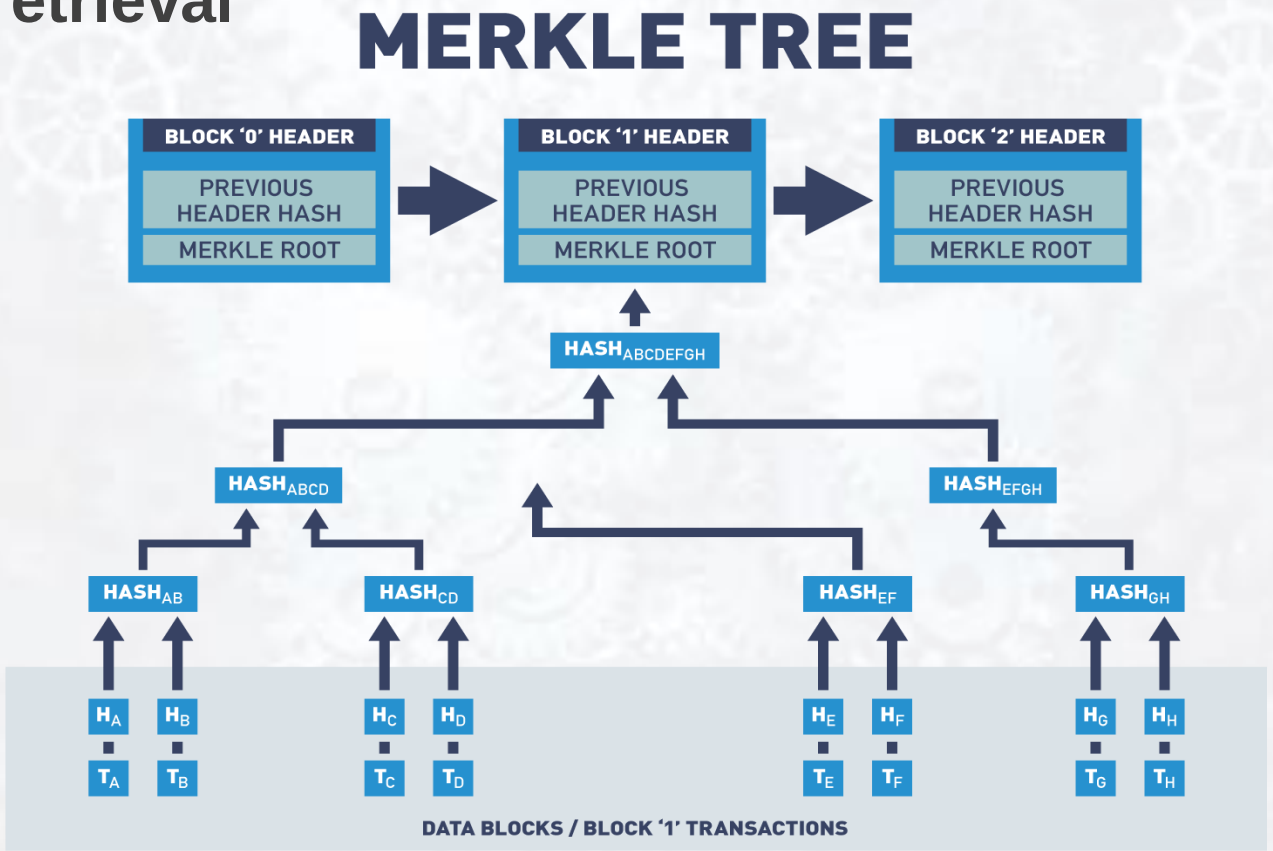
► ***Start Lab***

Cryptography | Merkle Tree in Blockchain

- **A special type of data storage structure based on hash functions is called a Merkle tree:**
  - It is structured as a binary tree; the leaves contain the values to be stored and each internal node is the hash of its two children.
  - It provides efficient lookups and protection against forgery since verifying a transaction is included in the tree. Can be accomplished by sending only the transaction, the hash contained in each node between the transaction leaf node and the root, and the hash values used to create each hash sent
  - Looking up a transaction in a Merkle tree with three levels includes sending two transactions (the desired one and the other child of its parent) and three hashes (the transaction's parent, the root, and the root's other child)

Cryptography | Merkle Tree in Blockchain

Merkle trees are a data structure that allows authenticated storage with efficient data retrieval



Cryptography | Zero-Knowledge Proof (ZKP)

- Zero-knowledge proofs **provide authentication without the need to share private information online**.
- This cryptographic technique enables a **prover to demonstrate the truth of a statement** to a **verifier** without **disclosing any further information**.
- With Zero-knowledge proofs, only the necessary information is revealed, ensuring the privacy and security of sensitive data.
- Zero-knowledge proofs are a powerful tool for securing online transactions and interactions, as they reduce the risk of identity theft and other forms of cybercrime.

Cryptography | Zero-Knowledge Proof (ZKP)

- Let's review an example
  - Let's say there are two toy cars, identical in shape and size, except, one is ***red*** and one is ***blue***
  - Jerry, who is color-blind, holds the toy cars behind his back
  - Jerry then shows one of the cars to Sam
  - Jerry then hides that car behind his back and shows Sam the other car. Sam can consistently detect the switch because the cars are different colors, but he never has to reveal the color of the cars to Jerry in order to prove the secret

Cryptography | Ethereum vs. Hyperledger Fabric

- **Public key cryptography** securely **manages digital identities** in blockchains, allowing verification of digital signatures without revealing sensitive information.
- **Ethereum** and **Hyperledger Fabric** verify identities and data integrity in transactions and blocks using digital signatures.
- Users sign transactions or blocks with their private key and share their public key with the network for verification, ensuring data access and modification only by the corresponding private key owner.
- Public key cryptography ensures secure and transparent blockchain networks for Ethereum and Hyperledger Fabric, protecting user privacy and preventing unauthorized data access or modification.

Cryptography | Ethereum vs. Hyperledger Fabric

- **Public key cryptography** is a method used in blockchain for **managing user identities** while **preserving anonymity**.
- **Ethereum** uses **an address** related to the **user's public key** to identify users, providing identity verification without revealing real-world identities.
- **Hyperledger Fabric** identifies users **via X.509 certificates** that include **information about the user**, including their **public key**.
- Both **Ethereum** and **Hyperledger Fabric** use public key cryptography to **ensure secure** and **private identity management** in their blockchain networks.

Cryptography | Ethereum vs. Hyperledger Fabric

- **Hash functions** are essential in blockchain technology and are primarily used to chain blocks together.
- Chaining blocks together in **Ethereum** and **Hyperledger Fabric** involves including the hash of the previous block in each block, **creating a cohesive chain of blocks**.
- Hash functions are also used to ensure the **integrity of data in each block**, as any alteration of the data would result in a different hash value.
- By using hash functions to chain blocks together and maintain data integrity, blockchain technology can provide a secure and transparent method for storing and sharing data.

Cryptography | Ethereum vs. Hyperledger Fabric

- **Zero-knowledge proofs** are a powerful tool for **increasing privacy** and **security** in various blockchain applications.
- Ethereum is currently working on **a layer 2 solution** that uses Zero-knowledge proofs to **store large amounts of data securely** and **only prove the validity** of the batch of information to the **mainnet**.
- Hyperledger Fabric also supports Zero-knowledge proofs through its pluggable **cryptographic library**, which enables **enhanced privacy measures** for **confidential transactions** and **identity verification**.
- By using Zero-knowledge proofs, these blockchain platforms can ensure that **sensitive data** and **user information remain private** while **maintaining the transparency** and **trustworthiness** of the blockchain network.

Cryptography | Ethereum vs. Hyperledger Fabric

- **Merkle trees** are an effective way to **store large amounts of data** and **ensure the integrity of that data** in a secure and efficient manner.
- **Ethereum** and **Hyperledger Fabric** are smart contract platforms that use a variant of the Merkle tree called **the Patricia tree** to store the current state of their virtual machines.
- The Patricia tree **stores key-value pairs** in a tree structure that allows for **efficient data retrieval** and **reduces the amount of storage** required for the state data.
- By using Merkle trees, Ethereum and Hyperledger Fabric can maintain a secure and tamper-proof record of all state changes made to their respective blockchains, ensuring the overall integrity and consistency of the system.

Cryptography | Ethereum vs. Hyperledger Fabric

CRYPTOGRAPHY	HYPERLEDGER	ETHEREUM
Public Key Cryptography	Membership Service Providers define and issue certificate authority to entities to issue X.509 digital certificates that contain public keys and defines the users' rights.	Based on ECDSA (Elliptic Curve Digital Signature Algorithm) any user can generate a public key from a private key.
Hash Functions	Hyperledger Fabric and Ethereum link blocks together by including the hash of the previous block into the hash of the current block creating a cohesive unbreakable chain.	
Zero-Knowledge Proofs	Hyperledger offers ZKP cryptographic functions in the Ursa Library to prove the existence of a transaction without revealing the details.	Ethereum uses ZKP technology to reduce computing and storage resources needed to validate blocks. It accomplishes this by reducing the data stored by only proving block is valid without sharing all the data.
Merkle Tree Structure	Ethereum and Hyperledger Fabric are smart contract platforms that use a particular type of Merkle tree called the Patricia tree to store the current state of their virtual machine.	

Introduction to Ethereum | Summary

►In this session, we discussed:

- The history of the Internet and how blockchain technology relies on Internet technology as the foundation for building the future of the blockchain evolution
- Blockchain concepts and characteristics: distributed ledger, peer to peer, transparent, consensus, encryption, immutability, programmable.
- Public-key cryptography and public/private key pairs to support privacy, authenticity and security
- Hashing functions, zero-knowledge proofs (ZKPs) and Merkle tree data structures and how they are used to secure the blockchain


THANK
YOU