Blockchain for Regeneration Webinar series

University of
Dar es Salaam

Week 1: Introduction to Blockchain Technology

Agenda

- What is blockchain?
- What is a block?
- A brief history and evolution of blockchain.
- Core principles and features of blockchain.
- The different types of blockchain networks.

So, what is blockchain?

Using the official definition by NIST (National Institute of Standards and Technology):

Blockchains are distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper-evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules.

In short...

A blockchain is a public database that is updated and shared across many computers in a network.

Blocks? What are those?

"Block" refers to data and state being stored in consecutive groups known as "blocks"

"Chain" refers to the fact that each block cryptographically references its parent. In other words, blocks get chained together. The data in a block cannot change without changing all subsequent blocks, which would require the consensus of the entire network.

Types of blockchains

- Public
- Private
- Consortium

Public Blockchains:

Public blockchains are open and permissionless, allowing anyone to join the network, participate in the consensus process, and validate transactions.

They are decentralized networks where all the transactions and data are transparent and publicly accessible.

Examples: Bitcoin (BTC), Ethereum (ETH), NEAR, Binance Smart Chain (BNB), and Cardano (ADA).

Private Blockchains

Private blockchains are restricted and permission-ed, allowing only authorized entities or participants to access and interact with the blockchain network.

Participants in a private blockchain are usually known and have specific privileges and roles within the network.

Private blockchains are often used within organizations or consortia to enhance efficiency, privacy, and control over the blockchain network.

Examples: Hyperledger Fabric and Corda.

Consortium Blockchains:

Consortium blockchains are a hybrid between public and private blockchains.

They are governed by a consortium or a group of organizations that collaborate to operate and maintain the blockchain network.
Consortium blockchains provide a balance between openness and control, allowing selected participants to join and participate in the consensus process.

Consortium blockchains are often used for industry-specific use cases or collaborations between multiple organizations.
Examples: R3 Corda Consortium and Enterprise Ethereum Alliance (EEA).

A Brief history and evolution of blockchain

- The Beginning (Late 2000s):
- Bitcoin Boom (Early 2010s):
- Big Companies Join In (Late 2010s):
- Blockchain Beyond Money (Mid-2010s):
- Blockchain Today (Present Time):

The Beginning (Late 2000s):

Imagine a mysterious person named Satoshi Nakamoto who wanted to create a special kind of money on the internet. In 2008, they released a paper explaining how it would work.

In 2009, the first block of this new money system, called Bitcoin, was created. It was like the first page of a digital ledger called the blockchain.

Bitcoin Boom (Early 2010s):

People started to get excited about Bitcoin because it allowed them to send money to each other online without needing a bank. Some even bought pizza with Bitcoin!
But as people got more interested, they realized that the technology behind Bitcoin, called blockchain, could be used for other things too.

Big Companies Join In (Late 2010s):

Big companies saw the potential of blockchain and started using it for their own projects.

They wanted to make their business operations more efficient and secure.

Governments and banks also became interested in blockchain, exploring how it could be used to make financial systems better and create their own digital currencies.

Blockchain Beyond Money (Mid-2010s):

People started to think about how blockchain could be used for things other than money.
They realized that blockchain could be used to make all sorts of transactions secure, like buying and selling things, tracking shipments, and even voting.

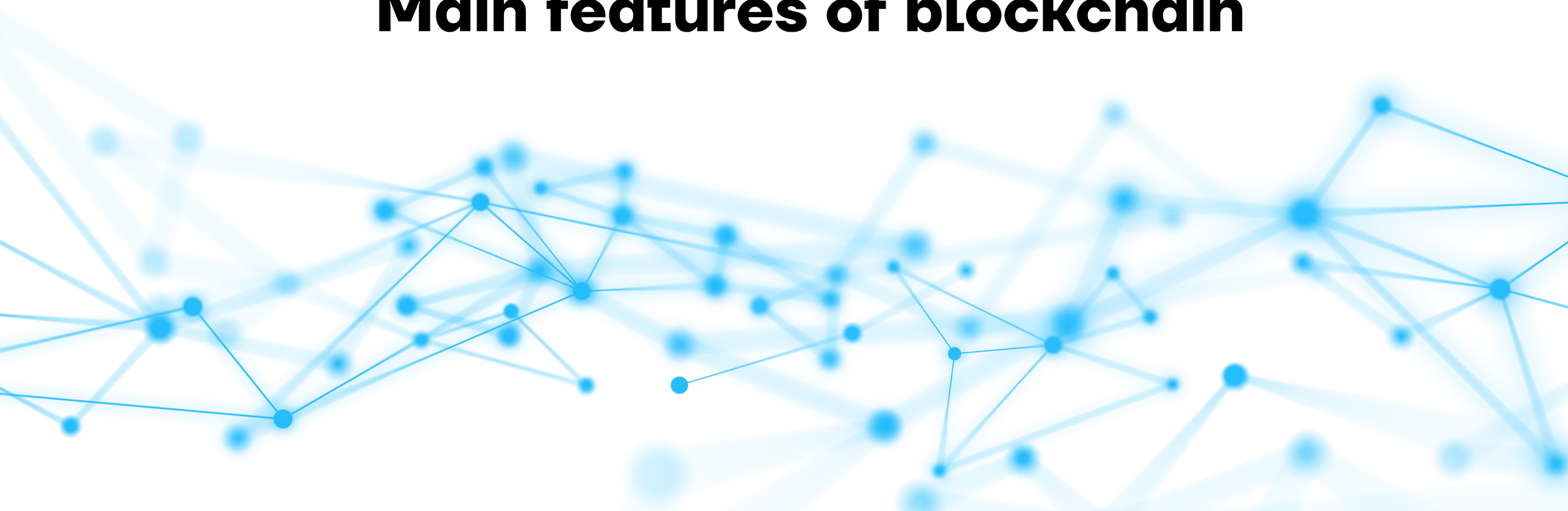
This led to the creation of new blockchain platforms like Ethereum, which allowed people to build smart contracts.

Smart contracts are like self-executing agreements that work automatically without needing a middleman.

Blockchain Today (Present Time):

Blockchain is becoming more popular and mainstream. It's being used in many different industries, like finance, healthcare, supply chain management, and even in video games.
People are working on making blockchain technology faster and more powerful so that it can handle more transactions and be used by even more people.
Exciting things are happening, and blockchain is still evolving with new ideas and improvements being made all the time!

Main features of blockchain



1.Decentralization

Blockchain operates on a decentralized network of computers, known as nodes.

These nodes maintain a copy of the blockchain ledger and participate in the consensus mechanism to validate and verify transactions, eliminating the need for a central authority.

2.Transparency

The blockchain ledger is a public and distributed database that stores all transactional data.

This transparency allows anyone to view the transactions, ensuring trust and accountability in the system.

3.Security

Blockchain employs cryptographic techniques to secure transactions and data.

Each transaction is digitally signed using private keys, and the integrity of the data is ensured through cryptographic hashes.

The decentralized nature of blockchain also makes it resistant to single points of failure and hacking attempts.

4.Immutability

Once a transaction is recorded on the blockchain, it is nearly impossible to alter or tamper with it. Each block in the chain contains a reference to the previous block, creating a cryptographic link that makes it computationally infeasible to modify past transactions without consensus from the network.

5.Consensus

Blockchain uses a consensus mechanism to agree on the validity of transactions and maintain the integrity of the network.

Different consensus algorithms, such as Proof of Work (PoW) or Proof of Stake (PoS), are employed to ensure agreement among the nodes on the state of the blockchain.

6. Smart Contracts

Blockchain platforms like Ethereum support smart contracts, which are self-executing agreements with predefined rules and conditions.

Smart contracts enable automated and tamper-resistant execution of contractual obligations, eliminating the need for intermediaries in many scenarios.

```
// SPDX-License-Identifier: MIT

pragma solidity ^0.8.0;


contract SimpleVoting {
    struct Candidate {
        uint256 id;
        string name;
        uint256 voteCount;
    }


    mapping(uint256 => Candidate) public candidates;
    mapping(address => bool) public voters;
    uint256 public candidatesCount;


    event votedEvent(uint256 indexed _candidateId);


    constructor() {
        addCandidate("Candidate 1");
        addCandidate("Candidate 2");
    }


    function addCandidate(string memory _name) private {
        candidatesCount++;
        candidates[candidatesCount] = Candidate(candidatesCount, _name, 0);
    }


    function vote(uint256 _candidateId) public {
        require(!voters[msg.sender], "You have already voted.");
        require(_candidateId > 0 && _candidateId <= candidatesCount, "Invalid candidate ID.");


        voters[msg.sender] = true;
        candidates[_candidateId].voteCount++;


        emit votedEvent(_candidateId);
    }
}
```

7. Privacy

While blockchain is inherently transparent, privacy features can be incorporated into certain blockchain implementations.

Techniques like zero-knowledge proofs and private transactions can be used to enhance privacy by concealing the details of transactions or selectively revealing information.

8. Distributed Ledger

Blockchain maintains a distributed ledger that is replicated across all participating nodes.

Each node has a copy of the entire blockchain, ensuring redundancy and resilience.

This distributed nature of the ledger enhances the robustness and availability of the system.

Conclusion

- Blockchain is a decentralized technology that provides transparency, security, and immutability to digital transactions.
- The core principles of blockchain include decentralization, transparency, security, immutability, consensus, smart contracts, privacy, and a distributed ledger.
- Blockchain technology started with the introduction of Bitcoin in 2008 and the creation of the first block, the Genesis Block, in 2009.
- Blockchain is being used in finance, supply chain management, healthcare, gaming, and other sectors.
- The goal is to make blockchain faster, more powerful, and accessible to a broader audience.

University of
Dar es Salaam

UDSM BlockchainClub

CHATAFISHA
www.chatafisha.com

Thank you..