Blockchain Security

For Beginners (Basics)

Presenter – Sanchay
@ null-meet, Airtel Center, Gurgaon
06 January, 2024

$whoami

-> Co-founder of HackersVilla CyberSecurity

-> Security Consultant/Trainer at MakeIntern

-> Designed trainings for Upgrad and UpgradCampus

-> Trained Employees for KPMG, Cognizant, etc

-> Active part of NULL Delhi Chapter

-> Security Mentor/Speaker at OWASP Delhi

-> Security Mentor at BSides Noida

Sanchay Singh

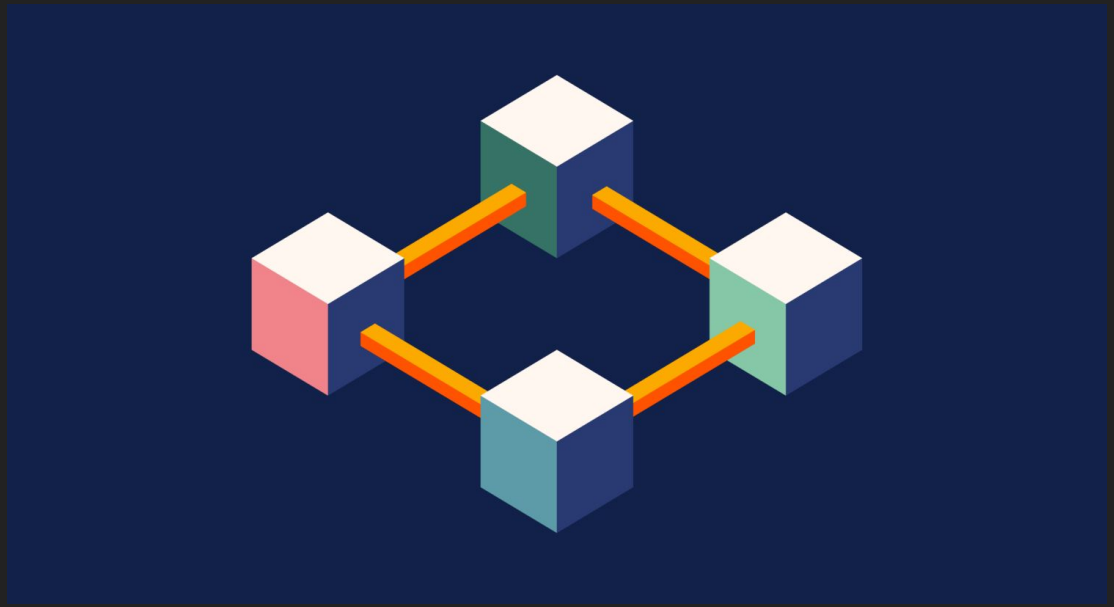
CYBERSECURITY EXPERT | CORPORATE TRAINER | PUBLIC SPEAKER

sanchayofficial

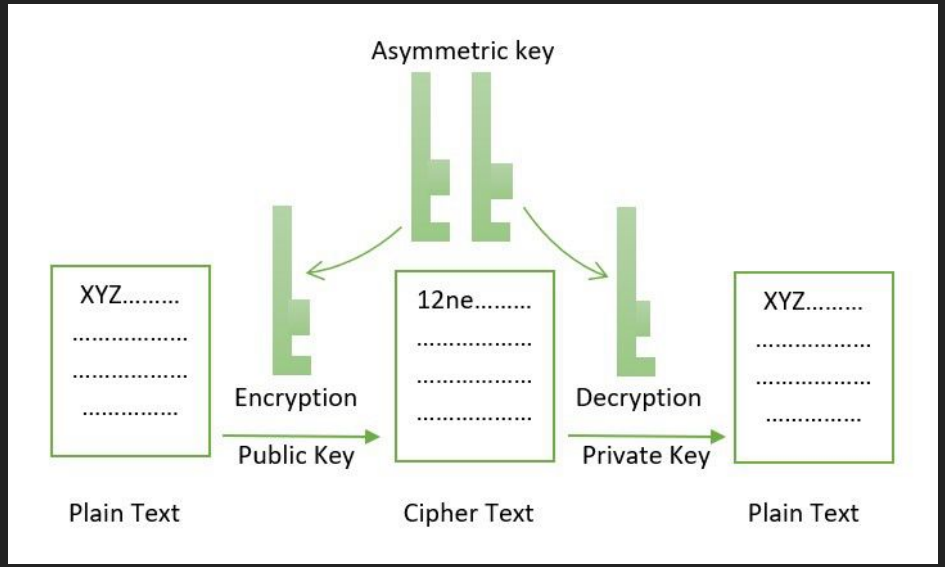
sanchayofficial@gmail.com

Intro to Blockchain

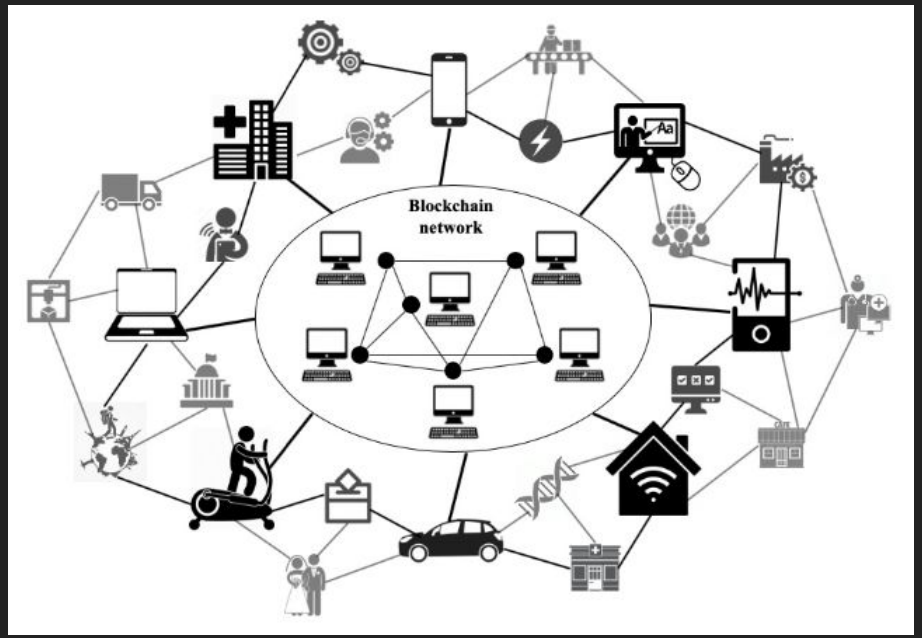
What is Blockchain



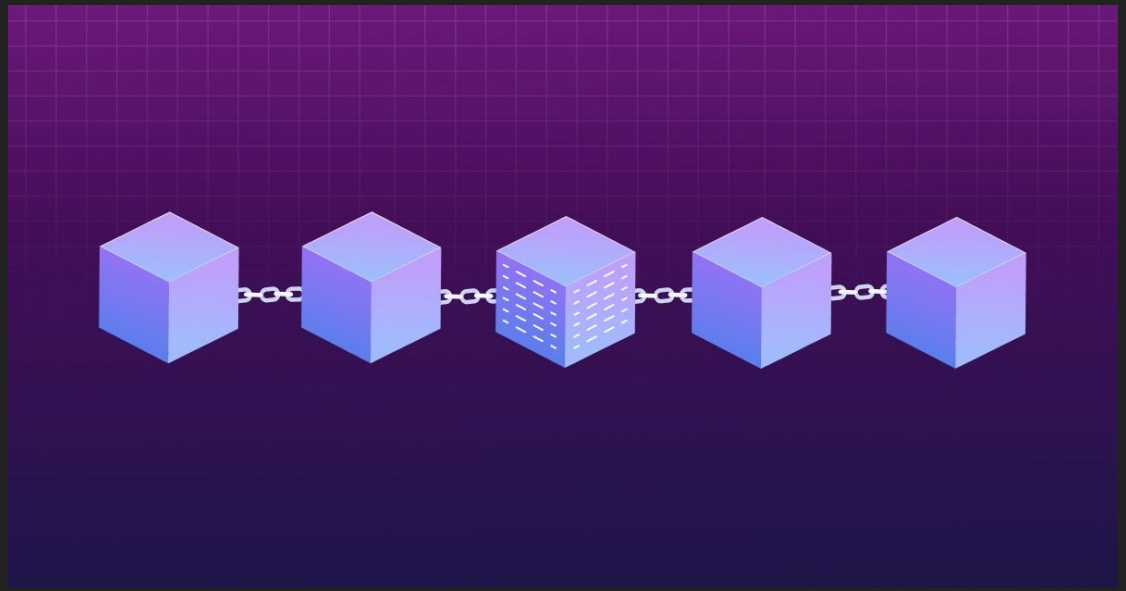
Cryptography



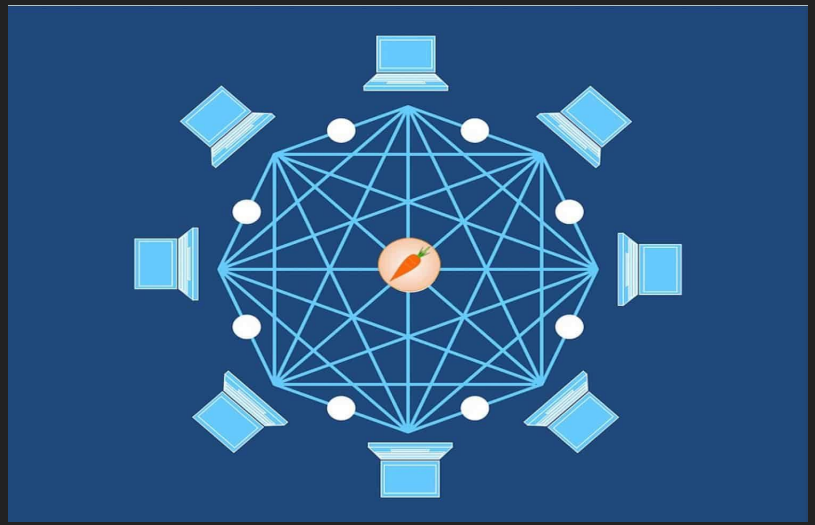
Decentralization



Immutability



Transparency



Importance of Security in Blockchain

Trust in Decentralization

Security is the bedrock of decentralized systems, fostering trust among participants who rely on the integrity of the blockchain.

Digital Asset Protection

There’s a critical need to protect digital assets, as blockchain often involves the transfer and storage of valuable tokens or data.

Immutable Ledger, Not Invincible

While the blockchain ledger is immutable, vulnerabilities in security can still compromise the overall system.

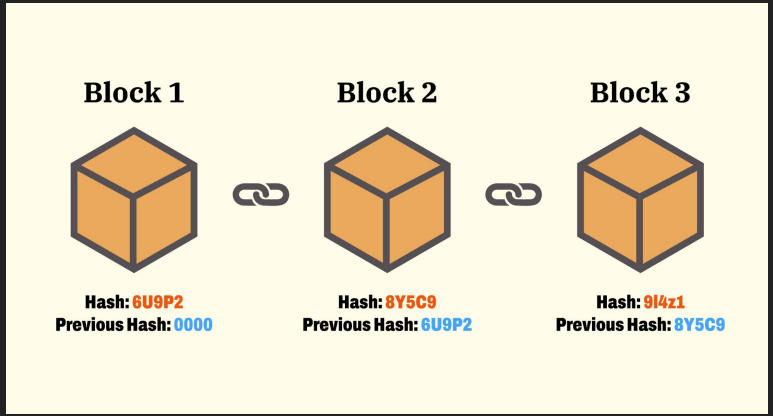
Blockchain as a Target

As blockchain technology gains prominence, it becomes an attractive target for malicious actors, requiring heightened security measures.

Blockchain Components

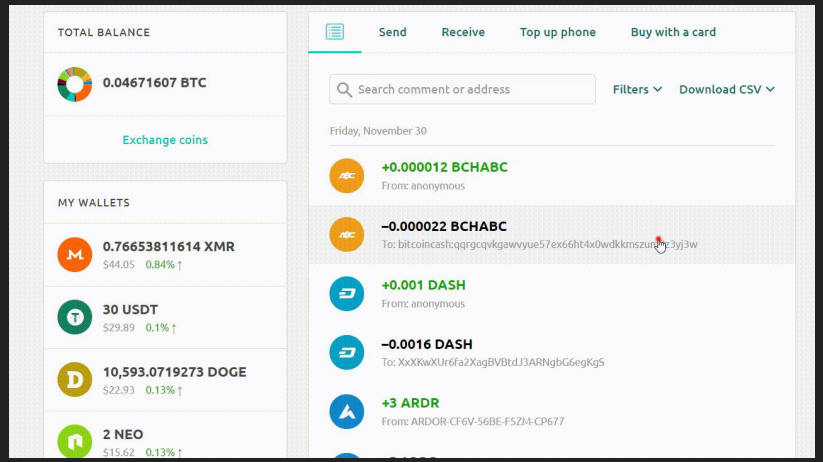
Blocks

The basic units of data storage in a blockchain. Each block contains a list of transactions and a reference to the previous block.



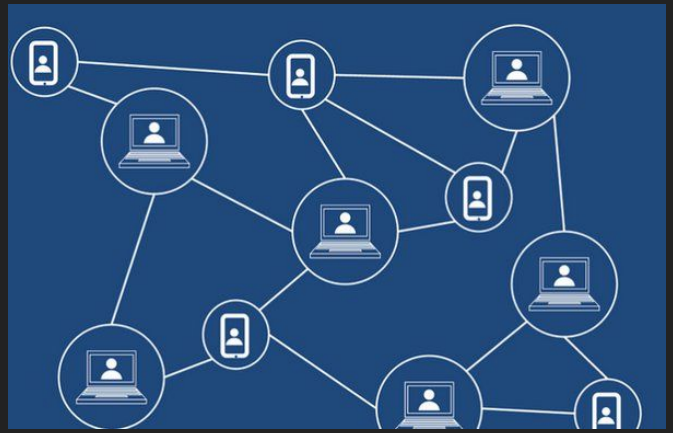
Transactions

Represents the transfer of assets or information between participants in the network. Transactions are bundled into blocks for validation.



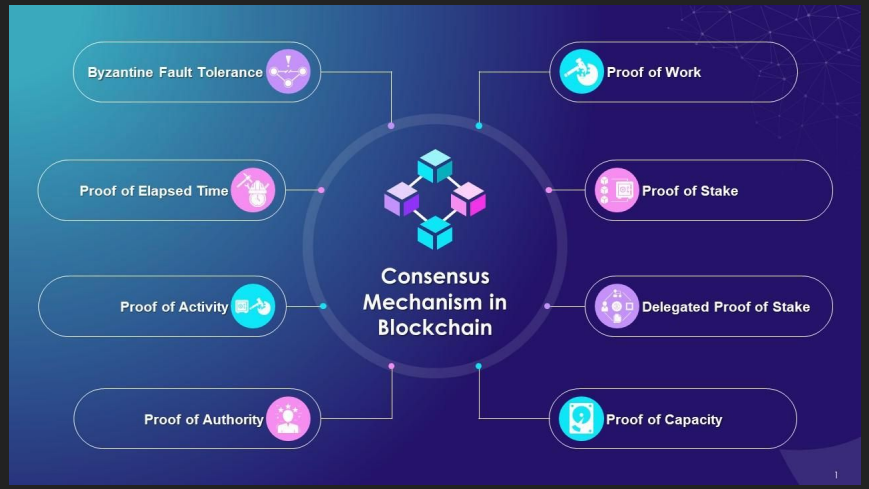
Nodes

Individual computers or devices participating in the blockchain network. Nodes maintain a copy of the entire blockchain, contributing to decentralization.



Consensus Mechanism

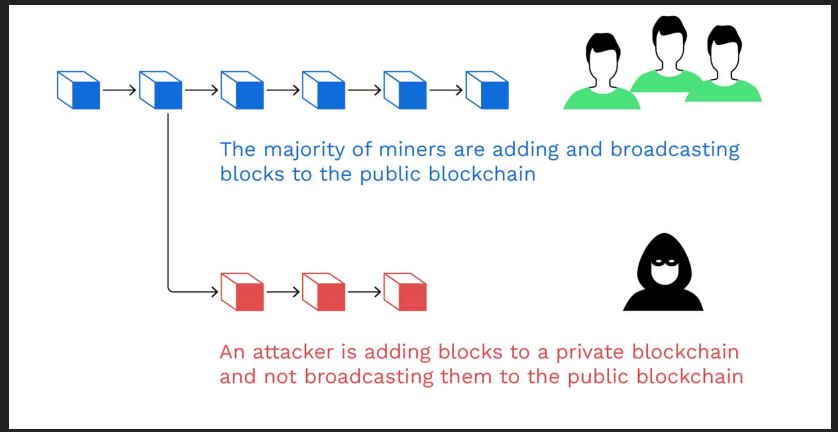
Consensus Mechanisms ensure agreement among nodes on the validity of transactions and the order in which they are added to the blockchain.



Blockchain Security Risks

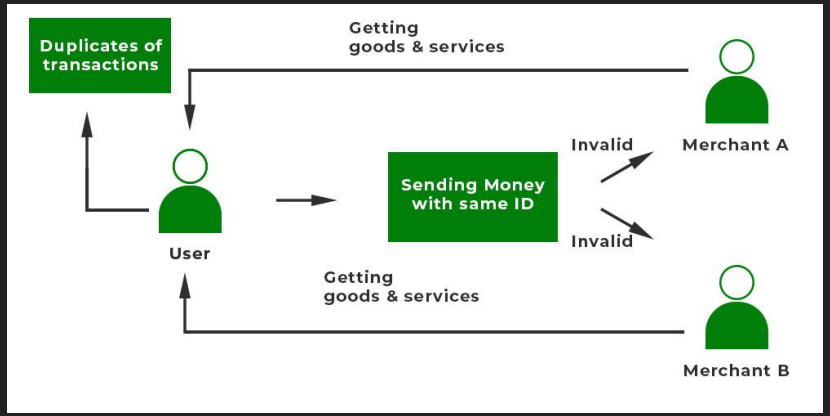
51% Attack

An attacker gains control of the majority of the network's computing power, compromising the integrity of the blockchain.



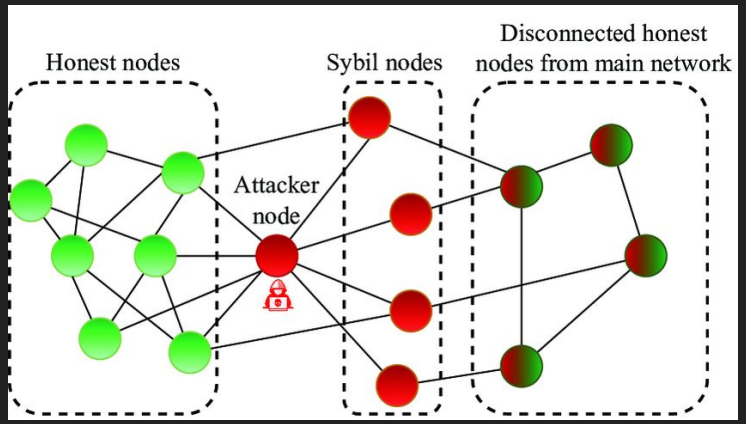
Double-spending attacks

An actor attempts to spend the same cryptocurrency more than once by exploiting a time gap in the confirmation process.



Sybil Attack

Scenarios where a single adversary controls multiple nodes to manipulate the network, leading to potential disruptions.



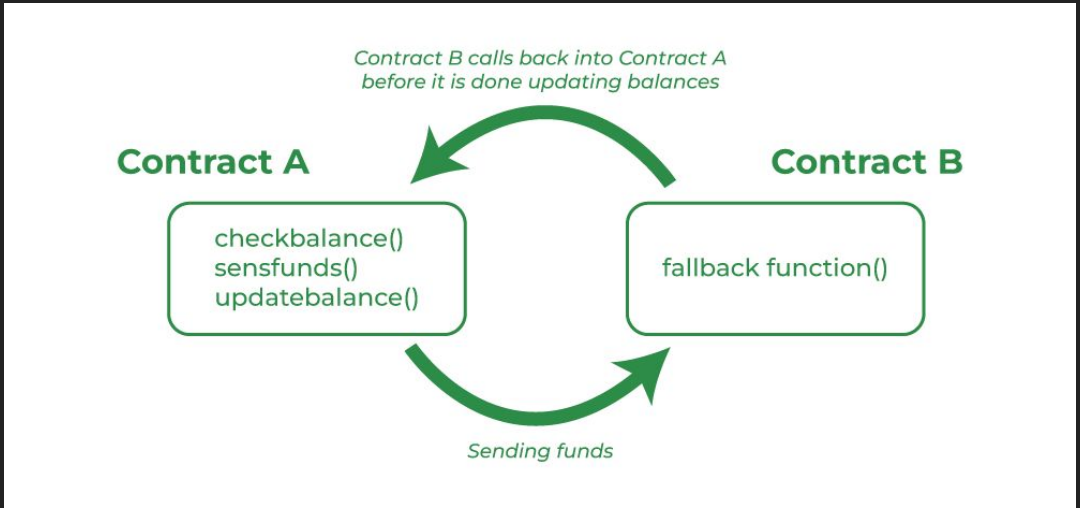
Social Engineering in Decentralized Applications

Vulnerability of decentralized applications (DApps) to social engineering attacks, where users are manipulated to disclose sensitive information.

Smart Contract Vulnerabilities

Reentrancy Attacks

An attacker exploits the recursive nature of smart contracts to repeatedly call a function before the previous execution is complete.

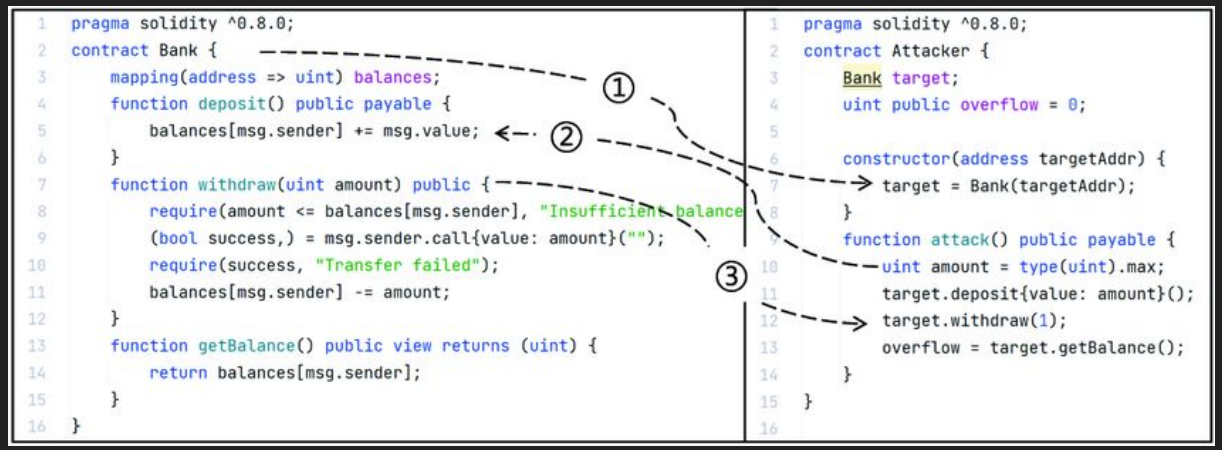


Insecure External Calls

Risks associated with external calls to other contracts or interfaces, emphasizing the need for secure coding practices to prevent unauthorized access.

Integer Overflow/Underflow

Improper handling of numeric values can lead to unexpected behavior, potentially allowing attackers to manipulate calculations within the smart contract.



Let me show you a Demo


BLOCKCHAIN
SECURITY SUMMIT 2022
IN PARTNERSHIP WITH
// HALBORN

Best Practices

1. Use of **Strong Cryptographic** Techniques
2. Regular Security Audits and Testing
3. Ensuring Secure Coding Practices
4. Importance of Consensus Mechanisms in Security
5. Secure Key Management and Storage

Thank You

Want to Practice
Blockchain Vulnerabilities?

https://pastebin.com/gWy0wwS8