UNIT 4

ADVANCED BLOCKCHAIN SECURITY

BY TEJAS MHASKE

CYBER SECURITY TRAINER

A. BLOCKCHAIN SECURITY BASICS

🔑**Key Components of Blockchain Security**

1. **Cryptography**:
   1. Hash functions (**SHA-256, Keccak-256**) ensure data integrity.
   2. Public-private key cryptography (ECDSA) secures transactions.
2. **Consensus Mechanisms**:
   1. Proof-of-Work (**PoW**): Resistant to Sybil attacks but vulnerable to **51% attacks**.
   2. Proof-of-Stake (**PoS**): Energy efficient but has **nothing-at-stake** problems.
3. **Immutability & Transparency**:
   1. **Data is tamper-proof** but may expose sensitive info (privacy issue).

Security Threats

Attack Type	Description	Example
51% Attack	A single entity controls >50% mining power and can alter transactions.	Ethereum Classic (2019)
Sybil Attack	An attacker creates multiple fake identities to manipulate the network.	Peer-to-peer networks
Double Spending	Attacker spends the same coin twice by exploiting block finality.	Bitcoin (theoretical)
Reentrancy Attack	Malicious contract repeatedly calls a vulnerable contract before state updates.	The DAO Hack (2016)

PRIVACY AND ANONYMITY IN BLOCKCHAIN

A. What is Pseudonymity in Blockchain?

- Most public blockchains (e.g., **Bitcoin, Ethereum**) are **pseudonymous**, not anonymous.
- Users **don’t reveal their real identities**, but every transaction is recorded publicly on the blockchain.
- A **public address (wallet address)** is like a "pseudonym"—not directly tied to real-world identity but traceable through activity.

💡 **Example:**

- If **Alice** receives Bitcoin from **Bob**, anyone can see the transaction on the Bitcoin blockchain.
- If Alice later cashes out at a regulated exchange (e.g., Coinbase), the exchange can **link her wallet to her real-world identity**.

PRIVACY AND ANONYMITY IN BLOCKCHAIN

B. True Anonymity in Blockchain

- **Anonymous transactions** hide the sender, receiver, and transaction details.
- Technologies like **Ring Signatures, Zero-Knowledge Proofs (ZKPs), and Coin Mixing** improve anonymity.
- Used by **privacy-focused blockchains** like **Monero (XMR)** and **Zcash (ZEC)**.

Blockchain	Privacy Level	How it Works
Bitcoin (BTC)	❌ No privacy	Transactions are publicly visible. Addresses can be linked to users.
Ethereum (ETH)	❌ No privacy	Smart contracts store transaction history permanently.
Monero (XMR)	✅ High privacy	Uses **Ring Signatures, Stealth Addresses, RingCT** to hide sender/receiver/amount.
Zcash (ZEC)	✅ High privacy	Uses **zk-SNARKs** for private transactions.
Dash (DASH)	🟡 Medium privacy	Uses **CoinJoin** to mix transactions.

PRIVACY AND ANONYMITY IN BLOCKCHAIN

- Blockchain technology provides varying levels of privacy and anonymity, depending on its implementation.
- Privacy ensures that transactional details are only visible to authorized participants, while anonymity conceals the identity of participants.
- Public blockchains like Bitcoin offer pseudonymity, while privacy-focused blockchains like Monero enhance anonymity through cryptographic techniques.

HOW PRIVACY IS COMPROMISED IN PUBLIC BLOCKCHAINS

A. Blockchain Forensics and Deanonymization

Blockchain **transactions are permanent and transparent**, which makes privacy difficult. Forensic companies like **Chainalysis, CipherTrace, Elliptic** specialize in **tracking and de-anonymizing crypto transactions**.

🔍**Deanonymization Techniques(Uncover Identities) Used in Blockchain Forensics**

1. **Wallet Clustering**:
   1. Multiple addresses controlled by the same user are grouped together using transaction history.
   2. Example: If a person **sends funds from multiple addresses to the same exchange**, all addresses can be linked.
2. **IP Address Tracking**:
   1. Bitcoin transactions often **leak IP addresses** if sent from an unprotected network.
   2. Solution: Use **Tor, VPN, or dVPNs (decentralized VPNs)** to hide your IP.
3. **Transaction Graph Analysis**:
   1. Examines transaction flow to **identify patterns** and **link addresses** to real-world identities.
   2. Example: The **Silk Road Bitcoin wallets** were traced using transaction graph analysis.

PRIVACY-ENHANCING TECHNOLOGIES IN BLOCKCHAIN

A. **Coin Mixing (CoinJoin, Wasabi, Samourai Wallet)**

- **How It Works**: Combines multiple transactions into one large transaction, **mixing coins** so that inputs and outputs become untraceable.
- **Example**: Wasabi Wallet, Samourai Whirlpool

B. **Ring Signatures (Used in Monero)**

- Allows a **group of users to sign a transaction** so that the real sender is hidden within the group.
- **Example**: Monero (XMR) uses **RingCT (Ring Confidential Transactions)** for complete privacy.

PRIVACY-ENHANCING TECHNOLOGIES IN BLOCKCHAIN

C. Stealth Addresses (Used in Monero, Ethereum Tornado Cash)

- **Each transaction generates a unique one-time address** for the receiver, making it impossible to track the recipient's actual address.

💡 Example:

- Alice sends 10 XMR to Bob.
- Instead of sending to Bob's public address, Monero creates a **random, one-time use address** that only Bob can spend.
- 📌 **Problem**: Transaction scanning takes longer due to extra verification steps.

ZERO KNOWLEDGE PROOFS

- Zero-knowledge proof is an encryption scheme whereby one party (the prover) can prove the truth of specific information to another party (the verifier) without disclosing any additional information.
- Interactive ZKP: The actions associated with the concepts deal with mathematical probability. In interactive ZKP, a prover needs to convince a specific verifier and repeat this process for each verifier. In interactive ZKPs, the prover must complete a series of actions to convince the verifier about a specific fact.
- Non-Interactive ZKP: Non-interactive ZKPs don’t have any voluntary interaction between the verifier and the prover. In non-interactive ZKP, a prover creates proof that anyone can verify, and the verification process can also be moved to a later stage. For a better mechanism of non-interactive ZKPs, they need specific software

ZKP IN BLOCKCHAINS

- Messengers on blockchain
- Next-gen file system controls
- Protection of storage
- Transferring private blockchain transactions
- Data Security

PERMISSIONED BLOCKCHAINS AND ACCESS CONTROL

A. Public vs. Permissioned Blockchains

- **Public Blockchains (Bitcoin, Ethereum)** – Open to all, anonymous, decentralized.
- **Permissioned Blockchains (Hyperledger, Corda)** – Controlled access, identity-based participation.

B. Access Control Models

Model	How it Works	Example Use Case
Role-Based Access Control (RBAC)	Permissions based on job roles.	Corporate blockchains (e.g., supply chain tracking)
Identity-Based Encryption (IBE)	Uses unique identity attributes (email, ID) as public keys.	Healthcare record management
Multi-Party Authentication	Requires multiple signers for transactions.	Enterprise blockchain security

SECURITY AUDITING AND TESTING

A. Smart Contract Audits

- **Common Smart Contract Vulnerabilities**:
  - **Reentrancy** (DAO hack)
  - **Integer Overflows** (Parity wallet bug)
  - **Front-Running** (MEV attacks on Ethereum)

🛠**Tools for Smart Contract Auditing**:

✅ **Slither** – Static analysis for Solidity
✅ **MythX** – Cloud-based vulnerability scanner
✅ **OpenZeppelin** – Secure contract libraries

B. Network Security Audits

- **Sybil-resistant consensus protocols**
- **Node monitoring** (checking Byzantine behavior)

REGULATORY COMPLIANCE IN BLOCKCHAIN

Key Global Regulations

Regulation	Region	Key Concern
GDPR	Europe	Right to be forgotten vs. blockchain immutability
SEC/CFTC Rules	USA	Crypto as securities (e.g., Ripple case)
FATF Travel Rule	Global	KYC/AML enforcement on exchanges

Case Studies: Notable Security Incidents

Incident	Year	Cause	Loss
Mt. Gox Hack	2014	Private key theft	850,000 BTC
The DAO Hack	2016	Reentrancy bug	$60M
Poly Network Hack	2021	Cross-chain vulnerability	$600M
Ronin Bridge Hack	2022	Private key compromise	$620M

FUTURE TRENDS AND INNOVATIONS IN BLOCKCHAIN SECURITY

A. AI & Machine Learning for Threat Detection

- AI-based anomaly detection to identify suspicious blockchain transactions.

B. Post-Quantum Cryptography

- Quantum computers could break ECDSA – moving towards **Lattice-based encryption**.

C. Zero-Knowledge Proofs & Confidential Smart Contracts

- **zk-Rollups** enable private transactions on Ethereum.
- **Secret Network** allows private computation on-chain.

धन्यवाद