Apply Fundamentals of Blockchain

Lecturer 3

By: Japhet Moise H.

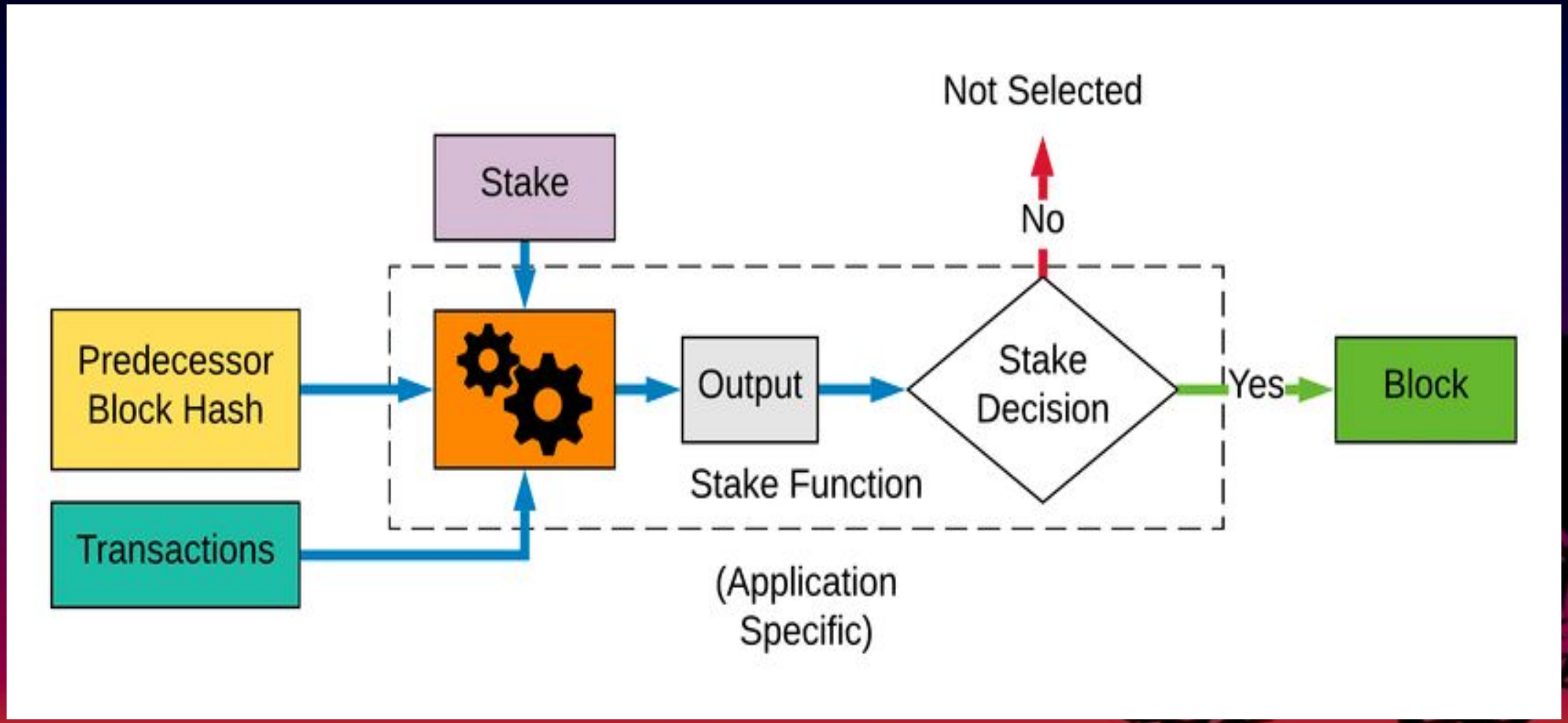
types of Consensus mechanism in blockchain

1. Proof Of Work

- Proof of Work is one of the earliest consensus algorithms, which works based on game theory.
- Many popular blockchains adopted it, including Bitcoin, Litecoin, and Dogecoin. There are high-level computational tasks that miners have to do in discovering new blocks, called mining.

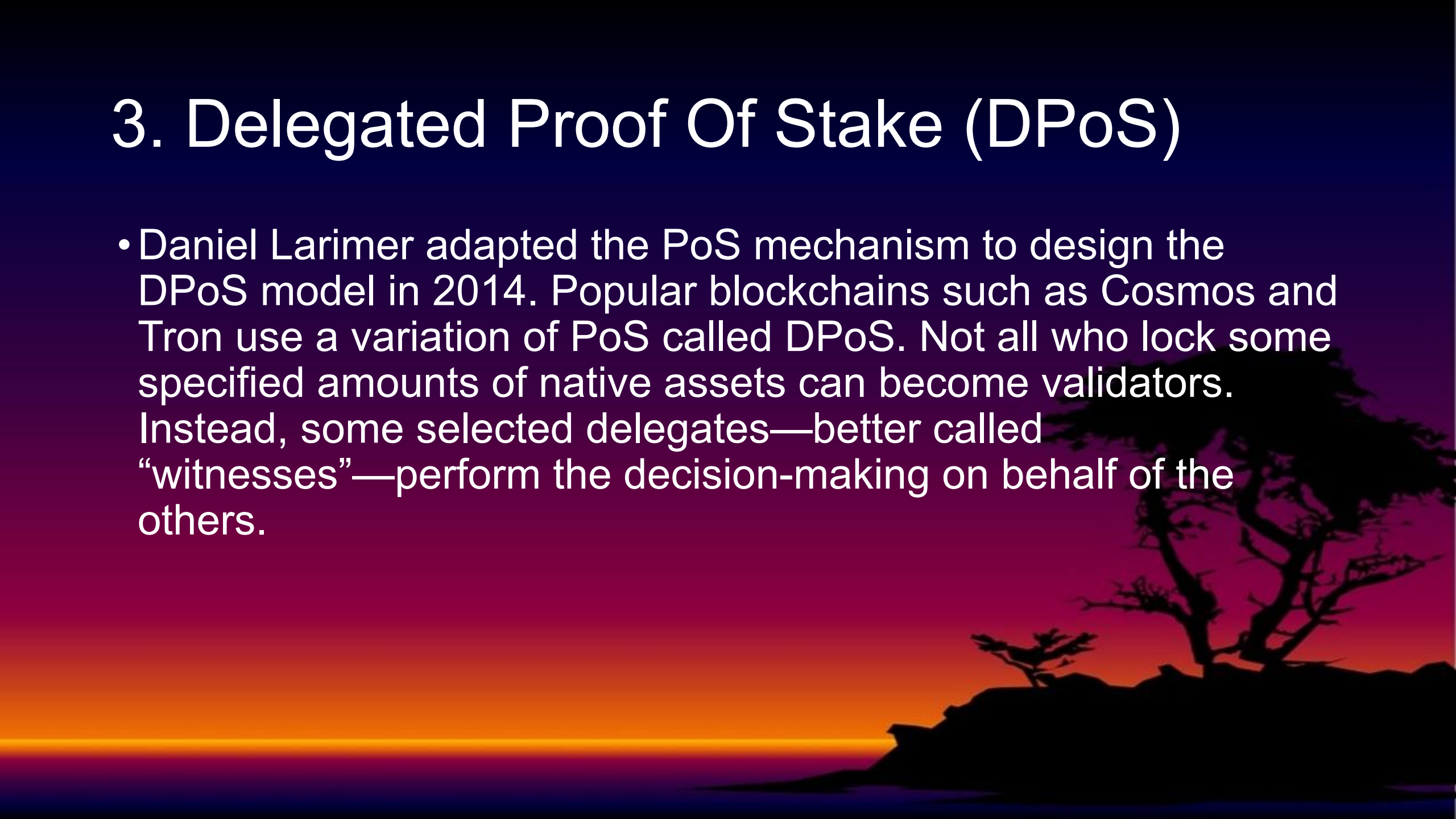
2. Proof Of Stake (PoS)

- Proof of Stake is a consensus algorithm where validators lock up some specified amount of native assets to secure the blockchain. It was developed as a better option for PoW.
- In 2022, Ethereum dropped PoW for PoS because it is more energy-efficient and decentralized.
- Other prominent blockchains, such as Tezos and Cardano, also incorporated PoS into their protocols.


Not Selected
Stake
No
Predecessor Block Hash
Output
Stake Decision
Yes
Block
Stake Function
Transactions
(Application Specific)

3. Delegated Proof Of Stake (DPoS)

- Daniel Larimer adapted the PoS mechanism to design the DPoS model in 2014. Popular blockchains such as Cosmos and Tron use a variation of PoS called DPoS. Not all who lock some specified amounts of native assets can become validators. Instead, some selected delegates—better called “witnesses”—perform the decision-making on behalf of the others.



Proof Of Weight (PoWeight)

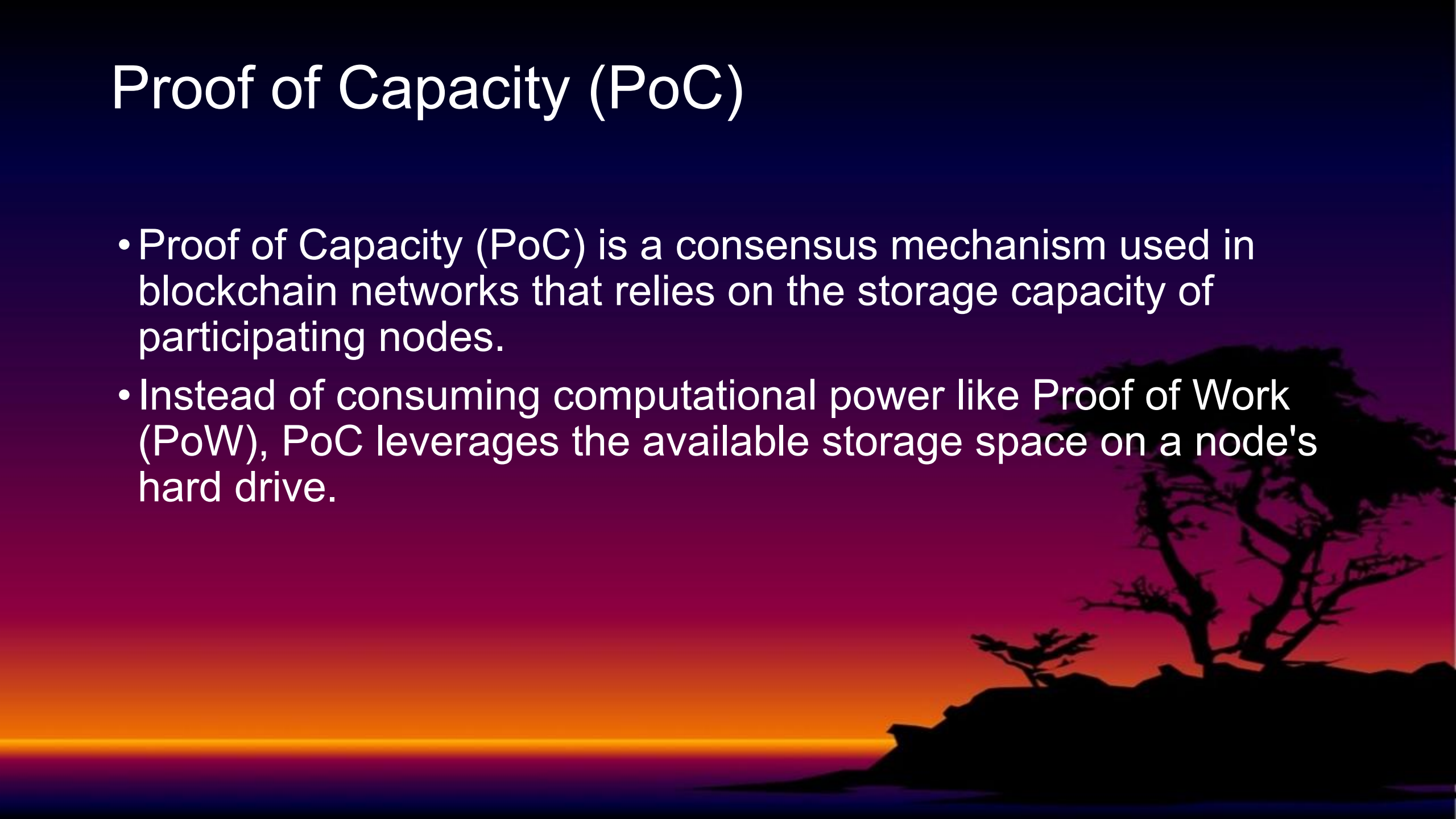
- Proof of Weight (PoWeight) is a consensus mechanism designed to address the energy consumption and centralization concerns associated with Proof of Work (PoW).
- Unlike PoW, which relies on computational power, PoWeight focuses on the weight or stake a participant has in the network.

Key principles of PoWeight

- **Weight-based validation:** Participants with a higher stake in the network have a greater chance of validating blocks.
- **Weight calculation:** The weight of a participant is typically determined by the amount of cryptocurrency they hold or the resources they contribute to the network.
- **Economic incentives:** Participants are incentivized to maintain honest behavior and contribute to the network's security.

Proof of Capacity (PoC)

- Proof of Capacity (PoC) is a consensus mechanism used in blockchain networks that relies on the storage capacity of participating nodes.
- Instead of consuming computational power like Proof of Work (PoW), PoC leverages the available storage space on a node's hard drive.



Proof of Authority (PoA)

- Proof of Authority (PoA) is a consensus mechanism and algorithm used in blockchains to verify transactions and create new blocks. It's based on identity and reputation, and uses a small group of trusted validators to reach consensus.
- PoA can improve transaction throughput and energy efficiency, and is considered an improvement on the traditional proof of stake (PoS) mechanism.
- However, it can also be criticized for being more centralized than other consensus mechanisms, and for sacrificing decentralization.

Attacks and vulnerabilities of blockchain

- **51% Attacks:**
- Control of the Network: An attacker gains control of more than 50% of the network's computing power.
- **Double-Spending Attacks:**
- Duplicate Transactions: A malicious actor attempts to spend the same cryptocurrency twice.
- **Sybil Attacks:**
- Fake Identities: An attacker creates multiple fake identities to gain control or influence over the network.
- **Smart Contract Vulnerabilities:**
- Coding Errors: Bugs or flaws in smart contract code can be exploited.

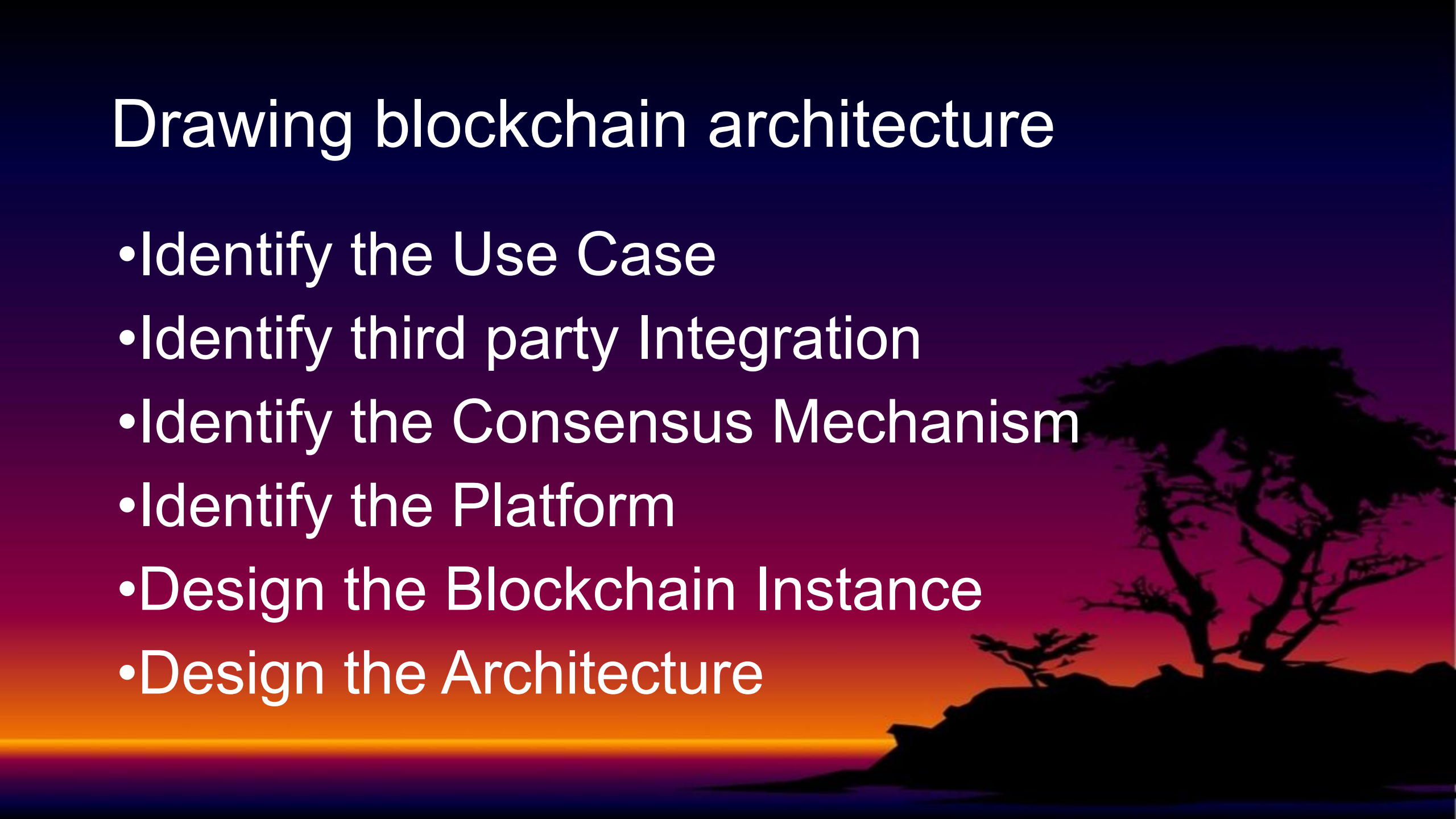
- **Quantum Computing Threats:**
- Cryptographic Breakdown: Quantum computers could potentially break current cryptographic algorithms used in blockchain.
- **Side-Channel Attacks:**
- Information Leakage: Attackers can extract sensitive information from a node's physical behavior or side channels.
- **Phishing and Social Engineering:**
- User Deception: Attackers trick users into revealing their private keys or other sensitive information.

Mitigating Risks:

- **Strong Consensus Mechanisms:** Choose consensus mechanisms that are resistant to attacks.
- **Secure Code Audits:** Conduct thorough audits of smart contracts to identify vulnerabilities.
- **Regular Updates:** Keep software and hardware up-to-date with security patches.
- **User Education:** Educate users about security best practices and common threats.
- **Diversification:** Consider using multiple blockchains or protocols to reduce risk.

Drawing blockchain architecture

- Identify the Use Case
- Identify third party Integration
- Identify the Consensus Mechanism
- Identify the Platform
- Design the Blockchain Instance
- Design the Architecture



Thank you!!!