Learning module 3: Consensus Mechanisms

Description

One of the central problems in the design of a blockchain system is the choice of the mechanism used by the nodes of the network to reach consensus on the state of the system in a decentralized manner, that is without resorting to having central trusted party.

Learning Module 3 explores the current mechanisms that handle the agreement among all the nodes that participate in a blockchain system. The most widely used consensus mechanisms will be discussed, with equal emphasis on the technical and business aspects of the topic.

At the beginning of the module, the need of a consensus mechanism in a distributed database setting is presented and solutions for permissioned systems are discussed. The role of Game Theory in the design of consensus mechanism is presented. A classification of the different consensus mechanisms that have been implemented in practice or proposed in theory within the two broad categories of Proof of Work (PoW) mechanisms and Proof of Stake (PoS) mechanisms is given and potential attacks on such mechanisms are described. Subsequently, a mapping of the different mechanisms to the trade-off between incentives to maintain the blockchain and security against malicious attacks that can compromise the blockchain's integrity, with special consideration of the position that each particular mechanism occupies in the centralization-decentralization space is presented. The final part of the module presents a set of practical case studies.

Participants who complete this module will be able to grasp the advantages and disadvantages of any consensus protocol in the context of any specific business model based on a distributed ledger as well as its limitations in terms of accuracy, cost efficiency, degree of decentralization, scalability, throughput rate and network sustainability.

Dependencies

This learning module has the following prerequisites:

- P2P database design (LM1)
- Encryption techniques (LM2)

Learning Objectives

- To explain the need for a consensus mechanism in a blockchain-based system.
- To present consensus mechanisms used in permissioned blockchain setups.
- To discuss the role of Game Theory in the design of a consensus mechanism.
- To present Proof-of-Concept (PoX) consensus protocols more widely used in blockchain systems
- To discuss possible attacks on distributed consensus protocols.
- To introduce and describe incentive structures used in distributed consensus protocols.
- To present attacks on consensus protocols related to incentives structures.
- To discuss costs of commonly used distributed consensus protocols.
- To discuss performance and scalability properties of widely used distributed consensus protocols.

- To present solutions to scalability issues based on alternatives to distributed consensus protocols used blockchain-based systems.
- To present use cases of different distributed consensus mechanisms in different blockchain systems.

Learning Outcomes

- **Understand** the role of consensus in DLTs and Blockchain systems.
- **Understand** the workings of PoX-type distributed consensus protocols.
- **Understand** possible attacks of distributed consensus protocols.
- **Compare** costs, performance, scalability and security between consensus protocols by analyzing their design specifications.
- **Appraise** the desired characteristics of a consensus protocol for a specific business model.

Syllabus

1. Introduction
   1.1. The need for consensus mechanisms
   1.2. Permissioned blockchains: Consensus through Byzantine-Fault Tolerant (BFT) voting mechanisms
2. The role of Game Theory in consensus
3. Proof-of-Concept (PoX) Protocols
   3.1. The concept of probabilistic consensus and its properties
   3.2. Cryptographic puzzle lotteries and their required properties
   3.3. Main protocols: Proof-of-Work, Proof-of-Stake, Delegated Proof-of-Stake, Proof-of-Authority
   3.4. A taxonomy of potential attacks: Sybil attacks, race attacks, Finney attacks, 51% attacks
4. Incentives
   4.1. Basic theory: sunk costs, principal-agent problems and incentive compatibility
   4.2. Incentive compatibility in PoX protocols: tokens, mining pools and mining cartels
   4.3. Markets in tokens
   4.4. Vulnerabilities of PoX protocols: selfish mining, block withholding, lie-in-wait mining pools, pool hopping
5. Costs
   5.1. The costly nature of PoX protocols
   5.2. Proof-of-Stake (PoS) protocols and the tragedy of the commons problem
   5.3. Security issues in PoS protocols: Nothing-at-stake attacks, grinding attacks
6. Performance
   6.1. The limited performance of permissionless blockchains
   6.2. Hybrid protocols
   6.3. Blockchain interoperability
   6.4. Non-linear blockchain networks: Greedy Heaviest-Observed Sub-Tree (GHOST) protocol
   6.5. Direct Acyclic Graph (DAG)-based protocols
7. Examples
   7.1. Hyperledger Fabric (BFT)
   7.2. Bitcoin (PoW)

7.3. Primecoin (PoUS)
7.4. Filecoin (UPoW)
7.5. SpaceMint (PoSP)
7.6. Bytecent (PoH)
7.7. Peercoin (PoS)
7.8. Algorand (Hybrid protocols)
7.9. Teechain on Bitcoin (Side-chain networks)
7.10. Ethereum Casper implementation (GHOST)