Blockchain Technology

Consensus Mechanism & Advanced Blockchain Feature Homework

Name: Vannchannida ANG
Class: FDE-C6 (Afternoon)

Write an essay about:

1. Why Consensus Exists

2. Safety, Liveness, Finality

3. Consensus in P2P Network (visual topology)

4. Common Attack Models

Standard databases rely on a central authority to validate data, which unfortunately creates a single point of failure. Blockchain moves away from this by sharing the ledger across a decentralized network. To ensure accuracy across so many different nodes, it uses consensus mechanisms. This process actually allows the entire network to agree on a single right information, this means to confirm which transactions are valid and in what order, without ever needing a central coordinator.

The consensus protocols are designed to achieve 3 keys technical goals, including safety, liveness and finality. It is known that no 2 honest nodes will finalize conflicting blocks. This ensures the ledger remains consistent across the network. Additionally, the system continues to produce new blocks and process transactions by avoiding deadlocks. As for the finality, once a block is confirmed, it can't be reversed. In Proof of Work (PoW), finality is probabilistic, while in Byzantine Fault Tolerance (BFT) systems, it's deterministic and immediate. These kinds of properties ensure that the blockchain remains reliable, available and tamper-resistant even in the case of a fault or malicious actors.

Furthermore, in a P2P blockchain network, nodes are interconnected in a mesh-like topology. Unlike the centralized systems with a hierarchy, P2P networks distribute authority. Consensus protocols help manage how these nodes communicate and agree. We can see this in different forms. Like as for Blockchain, they uses a "longest chain" rule, where the network follows the path with the most proven effort. In contrast, BFT-based systems like the Hyperledger Fabric use a more democratic voting process to verify the data. While this decentralized setup makes the network more tough to take down, however it requires rules to prevent disagreements and keep the data consistent.

For instance, we've seen the 2020 Ethereum Classic breaches proved that 51% attacks can lead to massive losses through double spending. Meanwhile, Bitcoin defends against Sybil attacks by tying network influence to real-world energy costs, making it too expensive to fake a majority. As we move to the Proof of Stake, the early model struggled with the "Nothing at Sake" flaw, but modern networks like Ethereum 2.0 now use the slashing method to keep validators honest. Similarly, Cosmo uses checkpoints to prevent a long-range attacks that target old security keys. Ultimately, these aren't just theoretical risks, but they are the catalysts that drive the next generation of blockchain security.

In conclusion, consensus is the foundation process that enables trust agreements in decentralized networks. As it balances safety, liveness, and finality while defending against attacks. From PoW's energy-intensive security to PoS's stake based effiency and BFT's deterministic finality, each consensus model offers trade offs suited to different use cases. By understanding these kind of mechanism, it’s really important for designing secure and resilient blockchain systems in the evolving digital economy.