Brief Note Blockchain Consensus Algorithms

Raghava Mukkamala

Here is the list of some of the major blockchain consensus protocols, along with their practical blockchain applications:

1. Proof of Work (PoW)

- **Description**: PoW requires miners to solve complex mathematical puzzles to validate transactions and create new blocks. The first miner to solve the puzzle gets to append the block and is rewarded with cryptocurrency.
- **Practical Blockchain Applications**:
  - **Bitcoin (BTC)**: The original blockchain that introduced PoW. It remains one of the most secure and decentralized networks.
  - **Ethereum (ETH)**: Initially used PoW before transitioning to Proof of Stake (PoS) with Ethereum 2.0.
  - **Litecoin (LTC)**: A faster and lighter version of Bitcoin, also using PoW.
  - **Monero (XMR)**: Privacy-focused cryptocurrency that also uses PoW.
  - **Zcash (ZEC)**: A privacy coin that employs PoW.

2. Proof of Stake (PoS)

- **Description**: PoS selects validators based on the number of coins they hold and are willing to “stake” as collateral. Validators confirm transactions and create blocks, and they are rewarded with new coins or transaction fees.
- **Practical Blockchain Applications**:
  - **Ethereum 2.0**: Transitioned from PoW to PoS in 2022 to enhance scalability and energy efficiency.
  - **Cardano (ADA)**: Uses a PoS algorithm called Ouroboros to offer scalability and sustainability.
  - **Polkadot (DOT)**: Uses PoS to secure a heterogeneous multichain.
  - **Tezos (XTZ)**: Implements a liquid PoS mechanism, where participants can delegate staking rights without transferring ownership.
  - **Cosmos (ATOM)**: Uses a PoS consensus algorithm to allow multiple blockchain interactions.

3. Delegated Proof of Stake (DPoS)

- **Description**: In DPoS, users vote for a small number of delegates to validate transactions and create new blocks. This improves efficiency and speeds up block creation.
- **Practical Blockchain Applications**:
  - **EOS (EOS)**: Uses DPoS to offer a highly scalable platform for decentralized applications (dApps).
  - **Tron (TRX)**: Also uses DPoS to offer fast and scalable transactions, primarily for content distribution platforms.
  - **Steem (STEEM)**: A social media platform with a DPoS mechanism.
  - **BitShares (BTS)**: A decentralized exchange platform using DPoS for faster consensus.

4. Practical Byzantine Fault Tolerance (PBFT)

- **Description**: PBFT ensures consensus even when some nodes in the network are faulty or malicious. Nodes must communicate to agree on the next block, requiring a two-thirds majority.
- **Practical Blockchain Applications**:
  - **Hyperledger Fabric**: A permissioned blockchain platform for enterprises that uses PBFT for finality.
  - **Zilliqa (ZIL)**: Uses PBFT for consensus within shards of its network, ensuring high throughput.
  - **Stellar (XLM)**: Uses a variant of PBFT called the Stellar Consensus Protocol (SCP) for fast and scalable payment settlements.

5. Proof of Authority (PoA)

- **Description**: PoA relies on a small group of trusted validators who are authorized to validate blocks. It is typically used in private or consortium blockchains.
- **Practical Blockchain Applications**:
  - **VeChain (VET)**: Uses PoA for supply chain management and enterprise-level applications.
  - **Ethereum (Testnet)**: PoA is used in Ethereum’s Rinkeby and Kovan testnets.
  - **Microsoft Azure**: Uses PoA for blockchain applications in enterprise environments.

6. Proof of Burn (PoB)

- **Description**: In PoB, miners “burn” coins by sending them to an address where they are permanently destroyed. This gives them the right to create new blocks, and the amount burned represents their stake in the network.
- **Practical Blockchain Applications**:
  - **Slimcoin**: Uses PoB to incentivize long-term investment.

    - **Counterparty (XCP)**: Originally used PoB to distribute tokens by burning Bitcoin.

7. Proof of Elapsed Time (PoET)

- **Description**: PoET is an energy-efficient consensus mechanism that uses trusted execution environments (like Intel SGX) to ensure that nodes “wait” for a randomly assigned period before creating new blocks.
- **Practical Blockchain Applications**:
    - **Hyperledger Sawtooth**: A modular blockchain platform that uses PoET for efficient consensus in permissioned environments.

8. Directed Acyclic Graph (DAG)

- **Description**: DAGs represent a different structure where transactions are confirmed by referring to previous transactions. There are no blocks, and validation is done simultaneously, increasing speed and scalability.
- **Practical Blockchain Applications**:
    - **IOTA (MIOTA)**: Uses the Tangle, a DAG-based system, for machine-to-machine transactions and IoT applications.
    - **Hedera Hashgraph (HBAR)**: Uses a DAG-based consensus algorithm for high-throughput decentralized applications.
    - **Nano (NANO)**: Uses a block-lattice structure (a form of DAG) for feeless, scalable transactions.

9. Proof of Capacity (PoC) / Proof of Space (PoSpace)

- **Description**: In PoC, miners allocate hard drive space to solve cryptographic puzzles. The more space you allocate, the higher the chances of solving the puzzle and creating a new block.
- **Practical Blockchain Applications**:
    - **Chia (XCH)**: Uses PoSpace for mining, aiming to be a more eco-friendly alternative to PoW.
    - **Burstcoin (BURST)**: Uses PoC for mining through allocated hard disk space.

10. Proof of Activity (PoA)

- **Description**: PoA is a hybrid consensus combining PoW and PoS. Mining starts with PoW, but instead of finalizing a block, the system switches to PoS to sign the block. This aims to balance security and energy efficiency.
- **Practical Blockchain Applications**:
    - **Decred (DCR)**: Uses a hybrid PoW/PoS consensus model to provide more decentralized governance and security.

11. Proof of Importance (PoI)

- **Description**: PoI measures the “importance” of a participant based on their coin holdings, transaction activity, and network interaction to validate transactions and create new blocks.
- **Practical Blockchain Applications**:
  - **NEM (XEM)**: Uses PoI to determine who can add blocks to the chain, factoring in reputation and activity, not just stake.

12. Proof of History (PoH)

- **Description**: PoH is used to timestamp transactions and prove the passage of time between events. This is typically used alongside other consensus mechanisms to ensure scalability and performance.
- **Practical Blockchain Applications**:
  - **Solana (SOL)**: Combines PoH with PoS to achieve high throughput and scalability, making it ideal for decentralized finance (DeFi) and dApp platforms.
