Polkadot Script Outline:

Topics/Notes.

- Chain Fibers
- Decoupling the consensus algorithm with the state change mechanism
- Problems of previous attempts at POS migration and side chains, such as COSMOS, casper,
- The tangle's approach to scalability
- WHAT is polkadot? A scalable, heterogeneous multi-chain ecosystem
    - Relay chain, parachain
- It is a blockchain of all the blockchains, running parallel "parachains"
- Roles of Validators, Collators, Nominators and Fishermen.
- The design of polkadot. Minimal, Simple, General, Robust.
- Consensus algorithm
- Nominated Proof of Stake
- Possible ATTACKS
    - Short Range Attack (Where validator
    - tries to validate both branches of a fork)
    - Long Range "nothing at stake" Attack (Where the attacker rewrites the entire history of the blockchain from the beginning)
    - This is stopped by the latch checkpoint (snapshot?)
- Blocks must be both intrinsically validated and extrinsically validated
- Interchain Communication
- Merkle Trees (Ingress and Egress)
- Polkadot and Ethereum
    - Interoperability
    - Polkadot TO Ethereum (break in contract, costs, majority validator vote)

        - Ethereum TO Polkadot (break out contract, checking the logs either by running a standard ethereum node, or bitcoin's SPV proofs. Bond system)
- Polkadot and Bitcoin
    - 2 way peg
    - Break out address
    - Bitcoin maximum multisig (3) problem
    - Virtual parachain
- Polkadot main 3 levels
    - Relay Chain Operation
        - Used for accounting only, cannot deploy contracts on it.
        - Layer of smart contracts, EVM. Simple and only for keeping track.
    - Staking Contract
        - Maintains validators
            - Who they are, who can be avail to validate, etc
            - Allows new validators to enter and old ones to exit
        - 80% staked, 20% left for liquidity. Reverse auction available.
    - Nominating
        - Approval-voting system.
        - Nominate the validator of choice, and stake your bond with them.
        - Reward-Punish relationship based on validator responsibility.
    - Punishable behavior of validators:
        - Being unable to provide consensus of a block
        - Signing validity to an invalid block

        - Validating multiple competing forks
    - Fisherman:
        - They look for misbehavior, and get rewarded for reporting it.
        - Like fishing, it's mostly a hit or miss ratio and takes work.
    - Token Burn (Punishment)
    - Parachain Registry:
        - Database containing info of each chain. 2 types of data:
        - Static Info - classifies the types of blockchains, AKA the chain index.
        - Dynamic Info - Transaction Routing Info (think routing numbers on checks?)
    - Voting to remove or suspend parachains
- Sealing Relay Blocks
    - Sealing refers to the standardization of chain info, think ERC 20 standards etc. For a POW chain, sealing would be mining.
    - Consensus creating state machine.
        - Both the parachain and relay chain are brought together to a single consensus algorithm
        - When consensus is reached, the block is "sealed" with a stamp, where the proof is put into the block header.
- Validators sign blocks based on 2 pieces of info: Availability and Validity.
    - Availability: Does the validator have all the info so they can validate the next block? Are they available to do the job? 1 for yes, 0 for not yet known. Must vote the same moving onward (back their candidate each time).

        - Validity: Is the block valid and are all transactions present and accounted for? 1 for valid, -1 for invalid, 0 for not yet known
- Voting must have:
    - At least ⅔ positive and 0 negative
    - Over ⅓ of yes towards the egress queue info
- What if there's a tie? Then it's either a mistakenly forked parachain, or there's a problem with the chain itself, and therefore may be suspended.
- Improvements for sealing relay blocks
- Validators validate the blocks, while collators keep the actual data in secondary sources to ensure the data avail and speed isn't compromised.
- Latency: like tetris. When you hit the 4 lines, boom. All of them are finalized
- Public participation: micro-complaints system, where the public can police the validators. Fishermen role outside of the network.
- Collator preferences: Weighted blocks
- Overweight blocks: making blocks ultra difficult (like factoring a large prime number)
- Validators must publish their own block history (track record) before they can publish new blocks, to prevent overweight blocks from forming.
- Collator insurance: validators can put into the next block a transaction for the "offender". If it misbehaves, it will transfer funds out of the block to the validator for grievance lol
- Collator can appeal this in front of a jury with random validators as well. Checks and balances.
- Interchain routing: FIFO. Collators collect outgoing info from parachains, Validators collect info for entering info to the relaychain, aka the accounting system.
- External data

SOURCES

https://polkadot.network/PolkaDotPaper.pdf

https://polkadot.network/Polkadot-lightpaper.pdf

https://www.youtube.com/channel/UCB7PbjuZLEba_znc7mEGNgw

https://wiki.polkadot.network/docs/en/

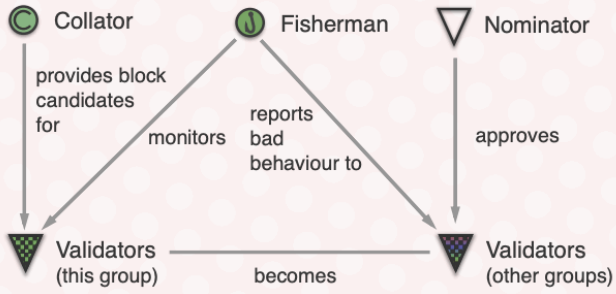

FIGURE 1. The interaction between the four roles of Polkadot.