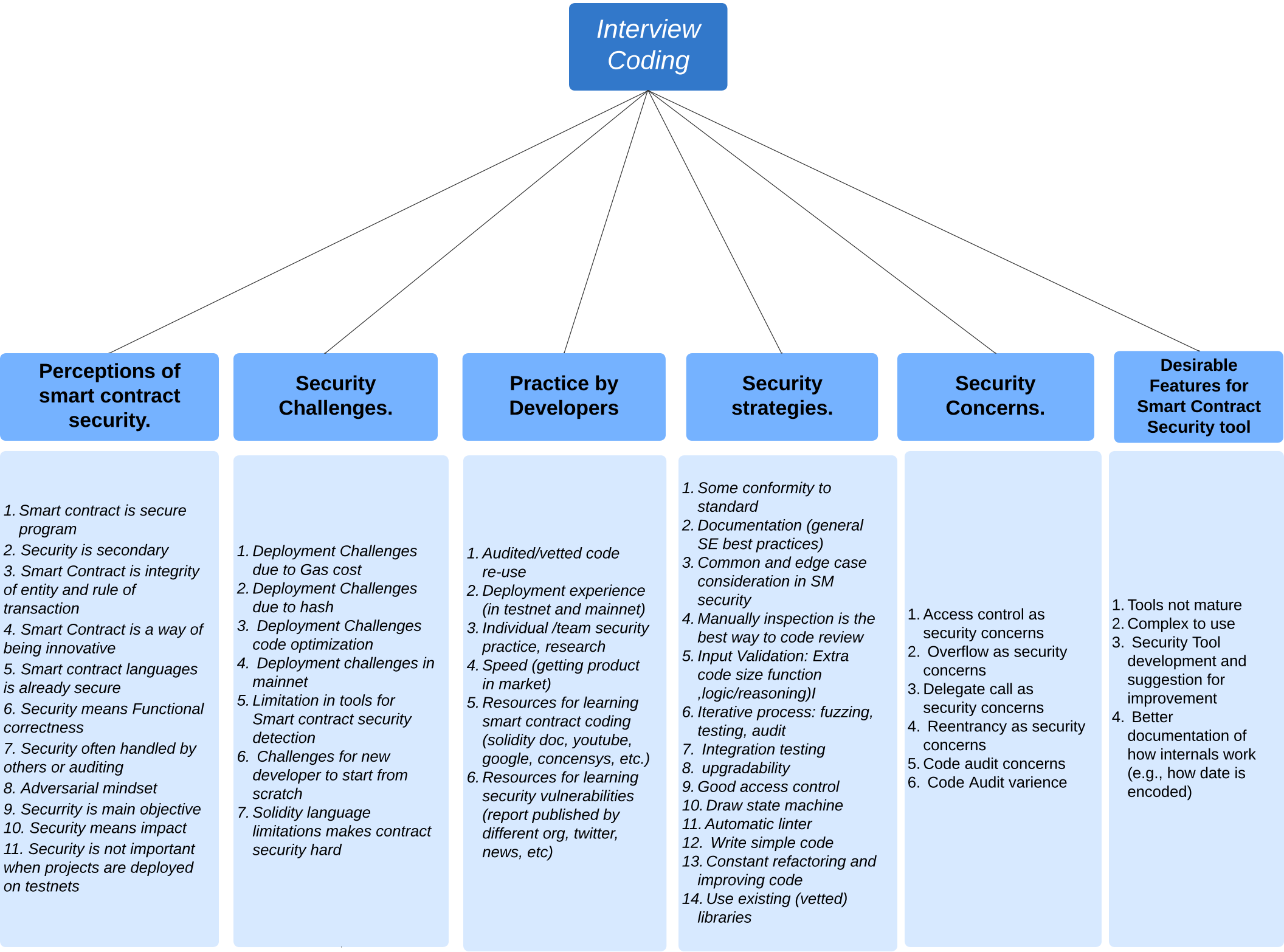
Interview Coding
Perceptions of smart contract security.
1. Smart contract is secure program
2. Security is secondary
3. Smart Contract is integrity of entity and rule of transaction
4. Smart Contract is a way of being innovative
5. Smart contract languages is already secure
6. Security means Functional correctness
7. Security often handled by others or auditing
8. Adversarial mindset
9. Securrity is main objective
10. Security means impact
11. Security is not important when projects are deployed on testnets
Security Challenges.
1. Deployment Challenges due to Gas cost
2. Deployment Challenges due to hash
3. Deployment Challenges code optimization
4. Deployment challenges in mainnet
5. Limitation in tools for Smart contract security detection
6. Challenges for new developer to start from scratch
7. Solidity language limitations makes contract security hard
Practice by Developers
1. Audited/vetted code re-use
2. Deployment experience (in testnet and mainnet)
3. Individual /team security practice, research
4. Speed (getting product in market)
5. Resources for learning smart contract coding (solidity doc, youtube, google, concensys, etc.)
6. Resources for learning security vulnerabilities (report published by different org, twitter, news, etc)
Security strategies.
1. Some conformity to standard
2. Documentation (general SE best practices)
3. Common and edge case consideration in SM security
4. Manually inspection is the best way to code review
5. Input Validation: Extra code size function ,logic/reasoning)I
6. Iterative process: fuzzing, testing, audit
7. Integration testing
8. upgradability
9. Good access control
10. Draw state machine
11. Automatic linter
12. Write simple code
13. Constant refactoring and improving code
14. Use existing (vetted) libraries
Security Concerns.
1. Access control as security concerns
2. Overflow as security concerns
3. Delegate call as security concerns
4. Reentrancy as security concerns
5. Code audit concerns
6. Code Audit varience
Desirable Features for Smart Contract Security tool
1. Tools not mature
2. Complex to use
3. Security Tool development and suggestion for improvement
4. Better documentation of how internals work (e.g., how date is encoded)