

Smart Contract Issues [WIP]

Ref: [Blockchain Based Smart Contracts : A Systematic Mapping Study](#) (Maher Alharby and Aad van Moorsel)

Smart contract issues

Codifying issues

- Difficulty of writing correct smart contracts
- Inability to modify or terminate smart contracts
- Lack of support to identify under-optimised smart contracts
- Complexity of programming languages

Security issues

- Transaction-ordering dependency vulnerability
- Timestamp dependency vulnerability
- Mishandled exception vulnerability
- Re-entrancy vulnerability
- Criminal smart contract activities
- Lack of trustworthy data feeds 'Oracles'

Privacy issues

- Lack of transactional privacy
- Use of 'Hawk' tool
- Lack of data feeds privacy

Performance issues

Sequential execution of smart contracts