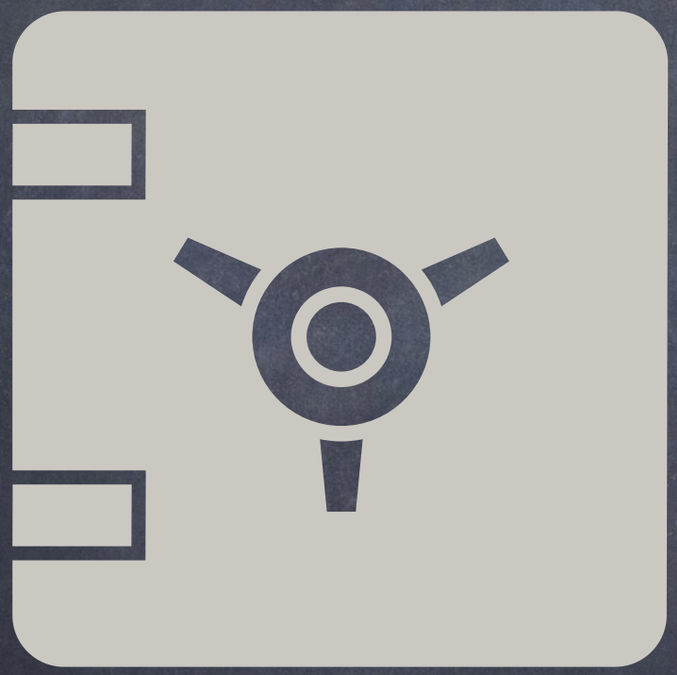
Security Pitfalls & Best Practices 201

Secureum Bootcamp

#102

ERC20 Transfers



ERC20 transfer() & transferFrom()

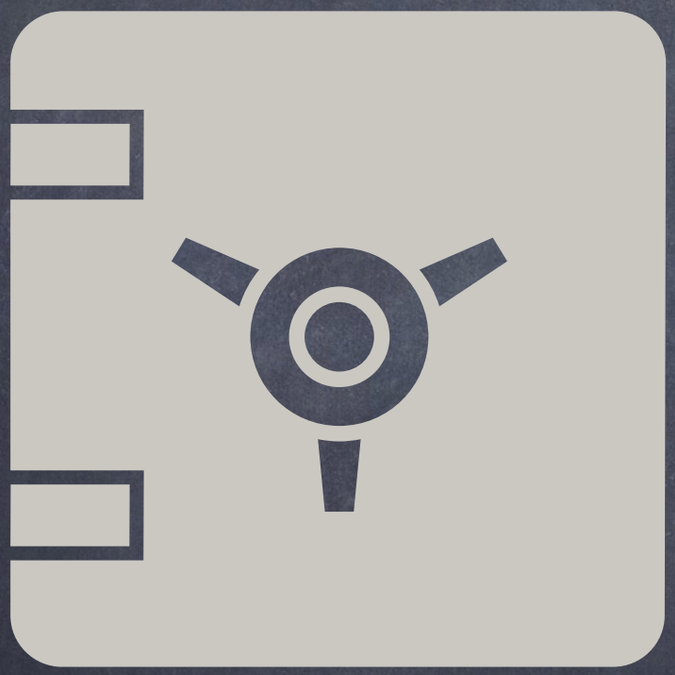
Should Return Boolean

No Boolean Return -> Calls Fail

Check Boolean Return

#103

ERC20
Optional



ERC20
name, symbol & decimals

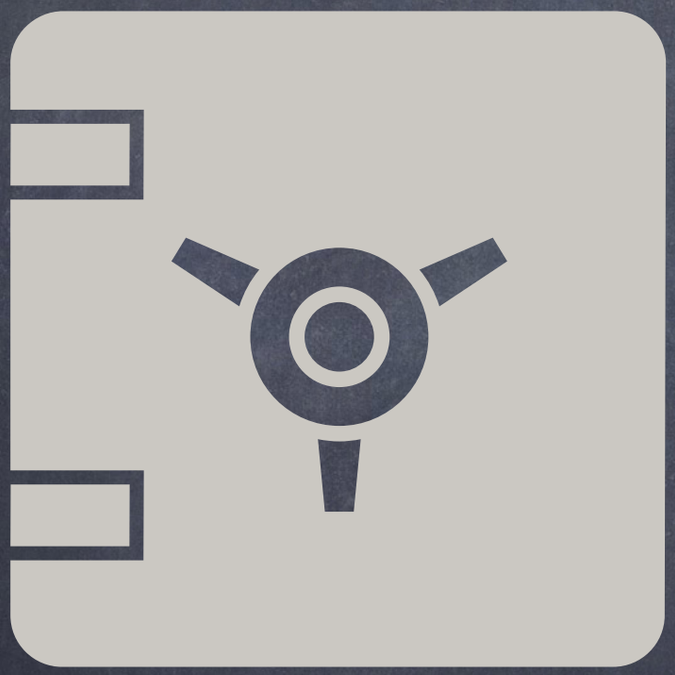
Optional

Used -> Present

Do Not Assume
Check Presence

#104

ERC20
Decimals



ERC20 decimals

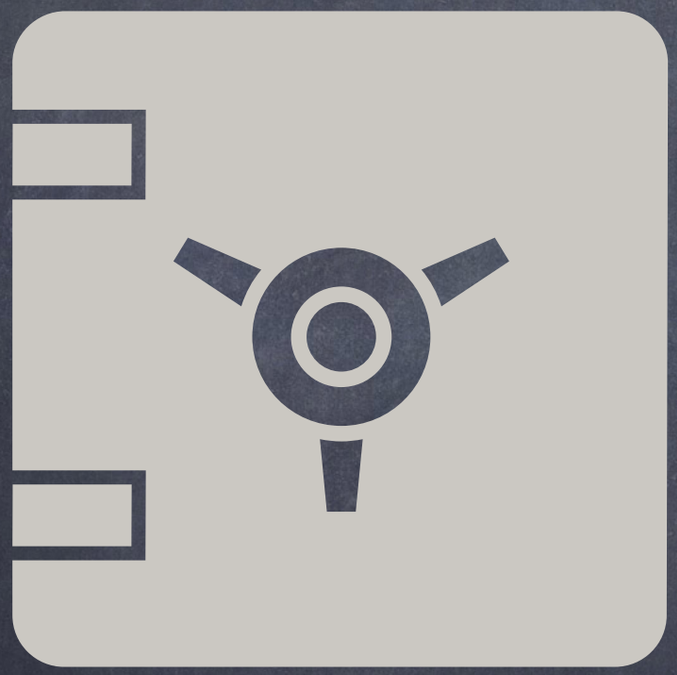
Decimals in Token
Typically 18

Return uint8
uint256 -> Incorrect

Return uint256 -> Check
Value <= 255

#105

ERC20
approve()



ERC20 approve()
Race-condition

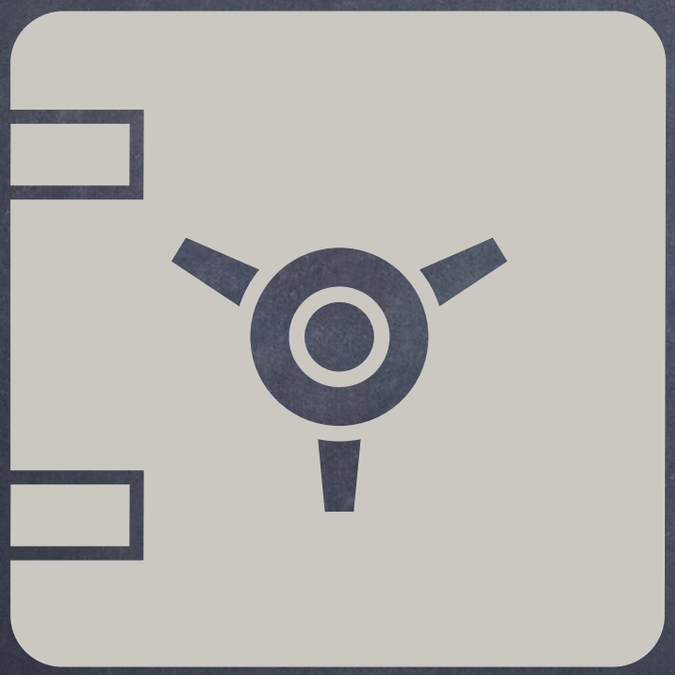
approve(100) -> approve(50)

Allowance Decrease
Front-run -> Spend 150

increaseAllowance()
decreaseAllowance()

#106

ERC777 Hooks



ERC777 Hooks

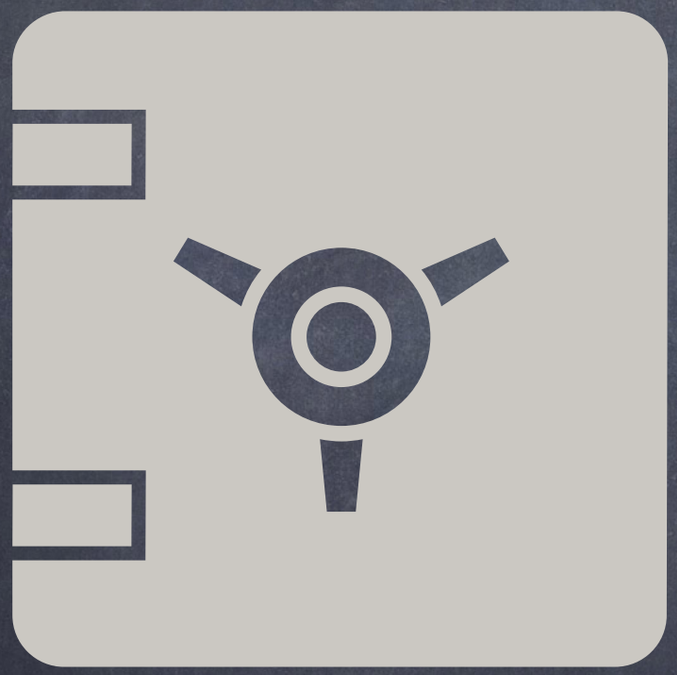
send/transfer/mint/burn/ operatorSend

External Calls -> Reentrancy

Check Hooks -> External Calls

#107

Token Deflation



ERC20 Token Deflation

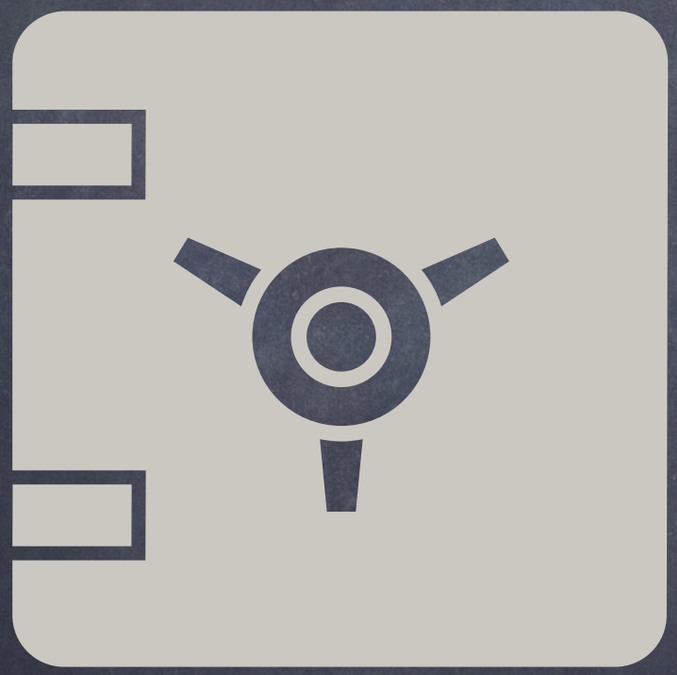
transfer/transferFrom -> Token Fee

Fee -> Deflation
Received < Sent

Check Deflation
Unexpected Behaviour

#108

Token Inflation



ERC20 Token Inflation

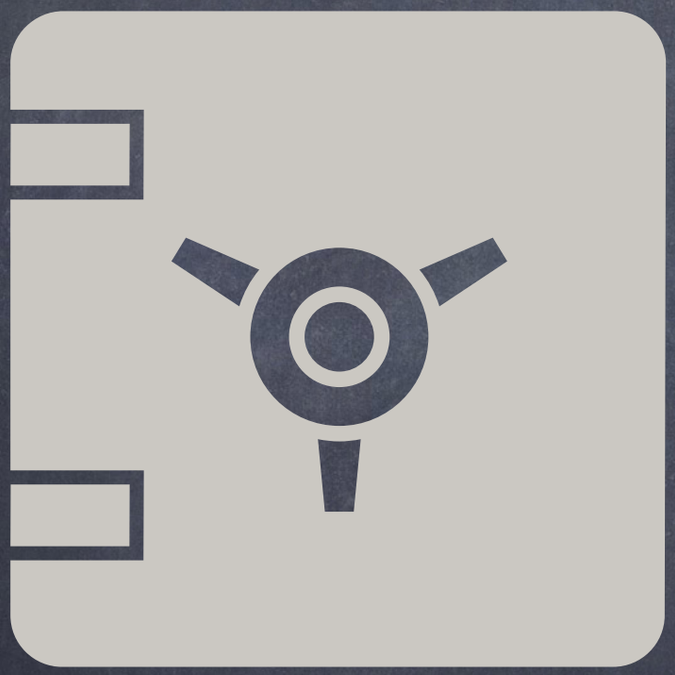
transfer/transferFrom -> Token Interest

Interest -> Inflation
Received > Sent

Check Inflation
Trapped in Contract

#109

Token Complexity



ERC20 Token Contract

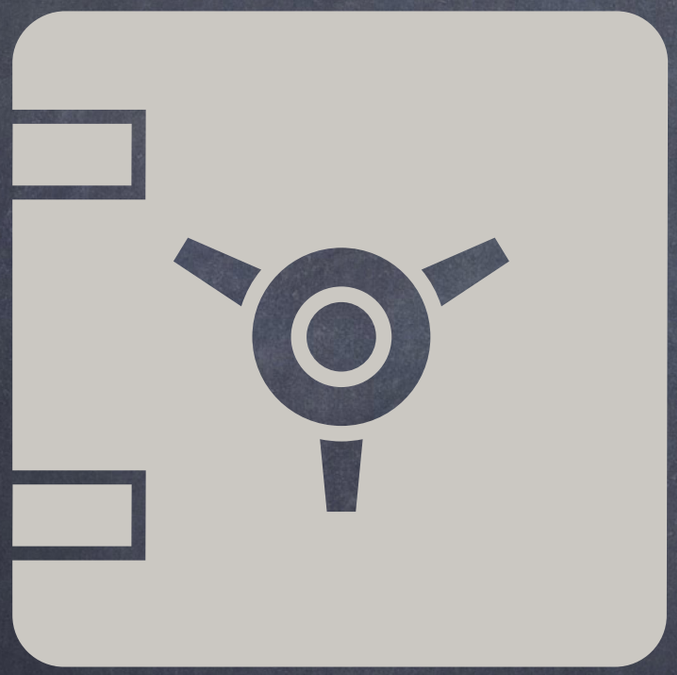
Well-defined Spec
Simple Contract

Complexity -> Bugs

Avoid Unnecessary Complexity

#110

Token Functions



ERC20 Token Contract

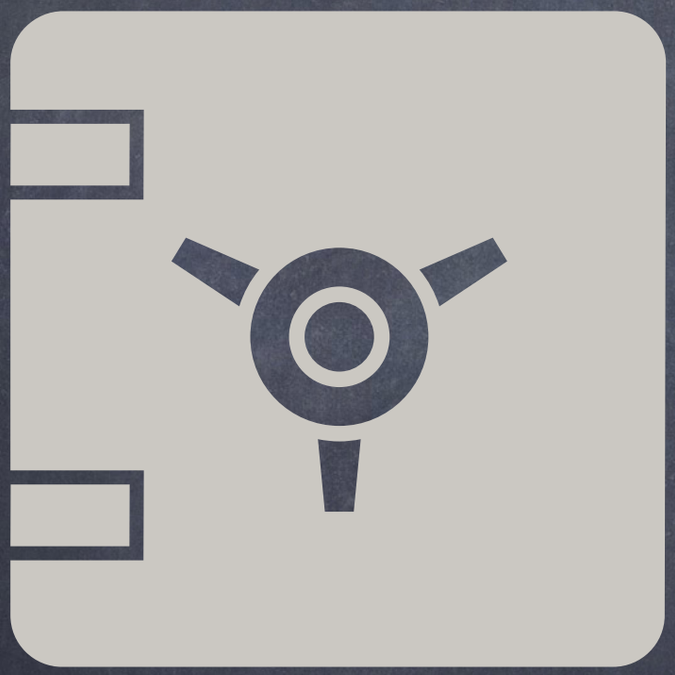
Token Functions
Non-token Functions

No/Few Non-token Functions
Complexity -> Bugs

Avoid Unnecessary Complexity

#111

Token Address



ERC20 Token Address

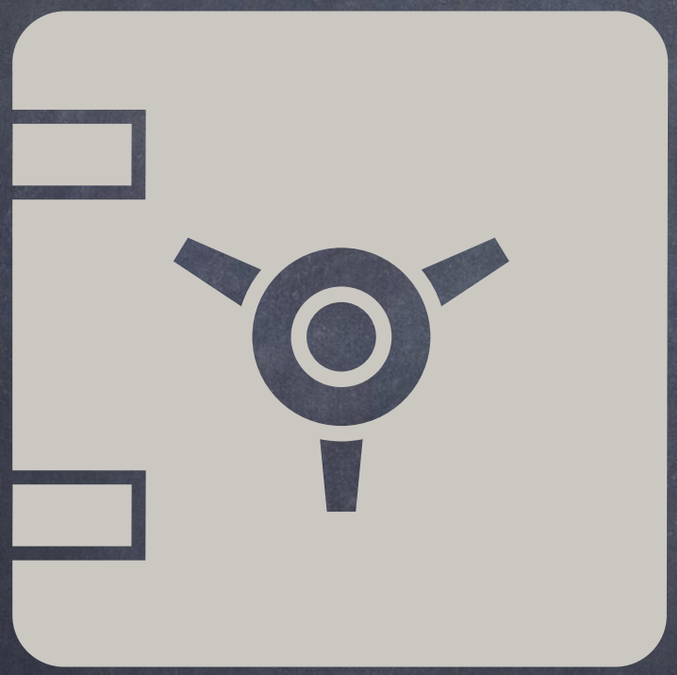
Only One Address

Multiple Addresses -> Multiple Balances -> Bugs

Single Address

#112

Token
Upgradeable



ERC20 Token
Upgradeability

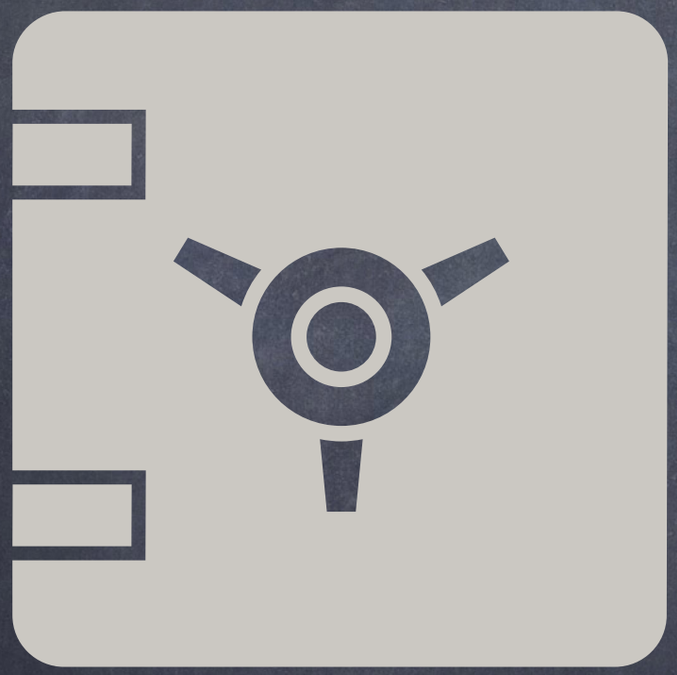
Upgradeable ->
Functionality Change

ERC20 Token Functions
Mint/Burn/Transfer Rules

Token Not Upgradeable

#113

Token Mint



ERC20 Token Minting

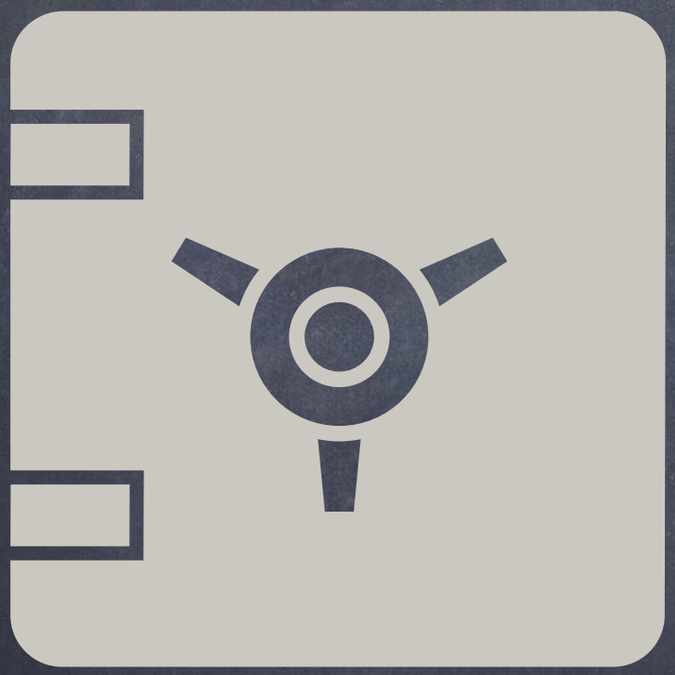
Owner -> Capabilities

Malicious Owner ->
Infinite Minting

Owner Minting
Misuse or Abuse

#114

Token Pause



ERC20 Token Pausing
Guarded Launch

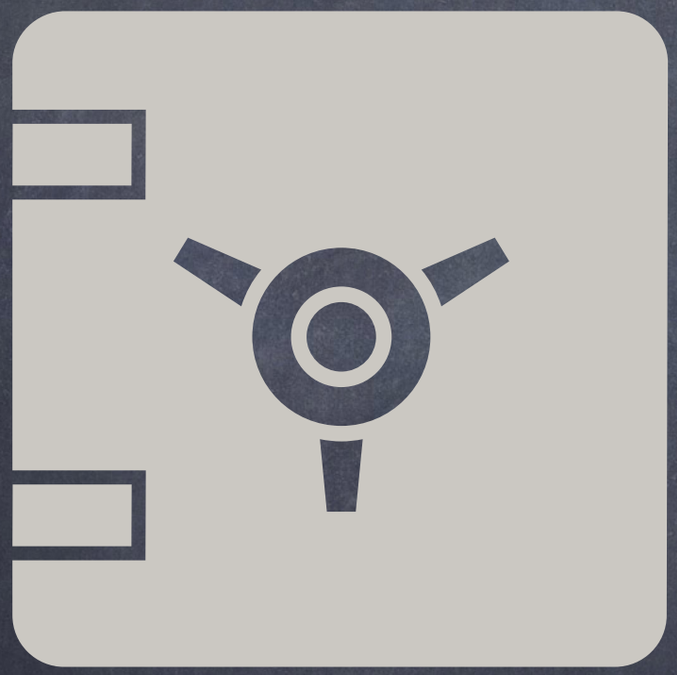
Owner -> Malicious or
Compromised

Pause Contract -> Trap
Funds

Not Pausable
Risk Awareness

#115

Token Blacklist



ERC20 Token Blacklist

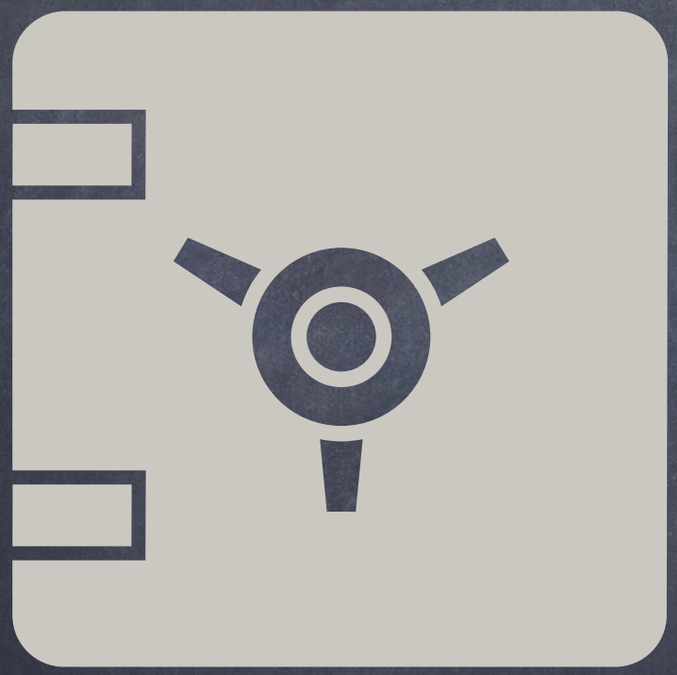
Owner -> Malicious or Compromised

Blacklist Contract -> Trap Funds

Cannot Blacklist
Risk Awareness

#116

Token Team



ERC20 Token Team

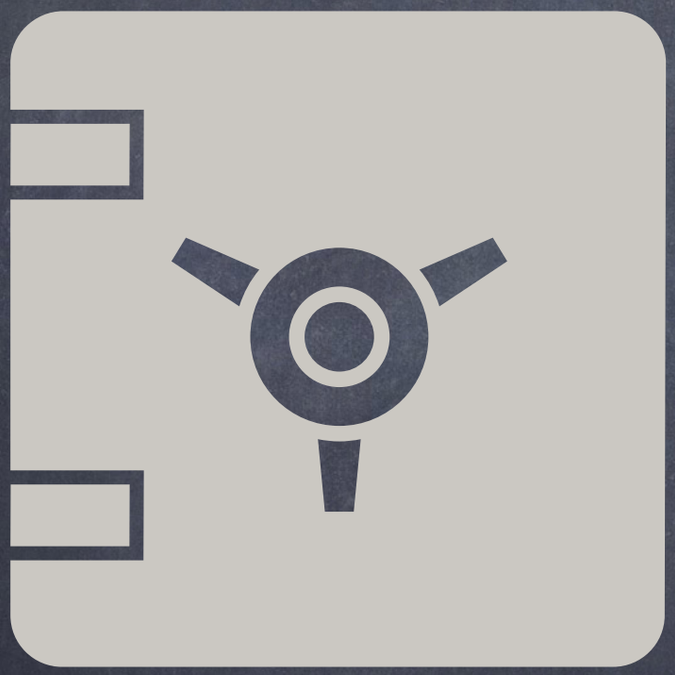
Team -> Public or Anonymous

Anonymous Team
Reputation & Risk

Team/Legal Risk
Risk Awareness

#117

Token Ownership



ERC20 Token Ownership

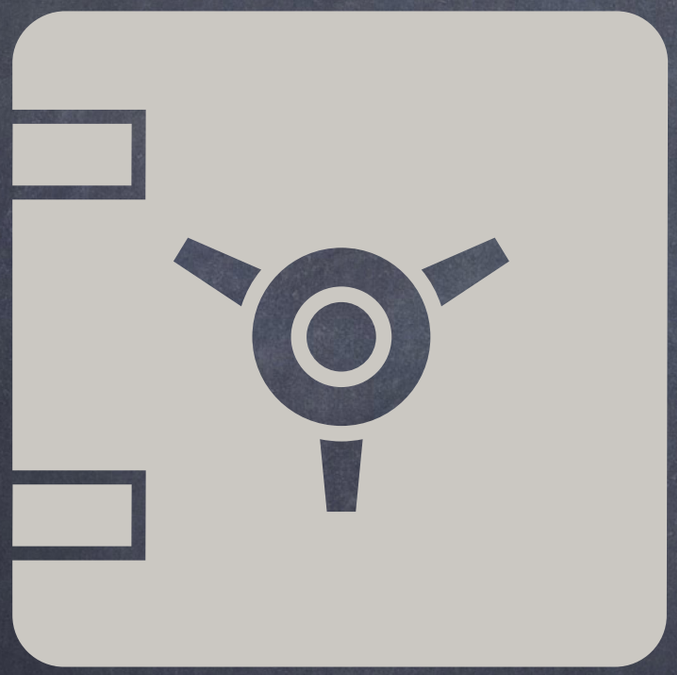
Who Owns?
How Much?

Ownership -> Few + Lot

Centralization Risk
Risk Awareness

#118

Token Supply



ERC20 Token Supply

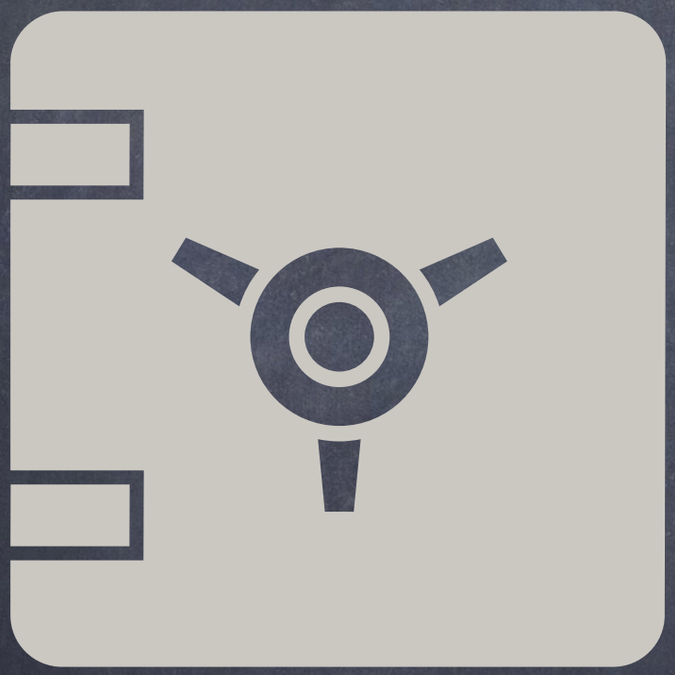
Token Supply -> Low or High

Low Supply -> Ownership & Liquidity & Volatility

Manipulation Risk
Risk Awareness

#119

Token Listing



ERC20 Token Listing

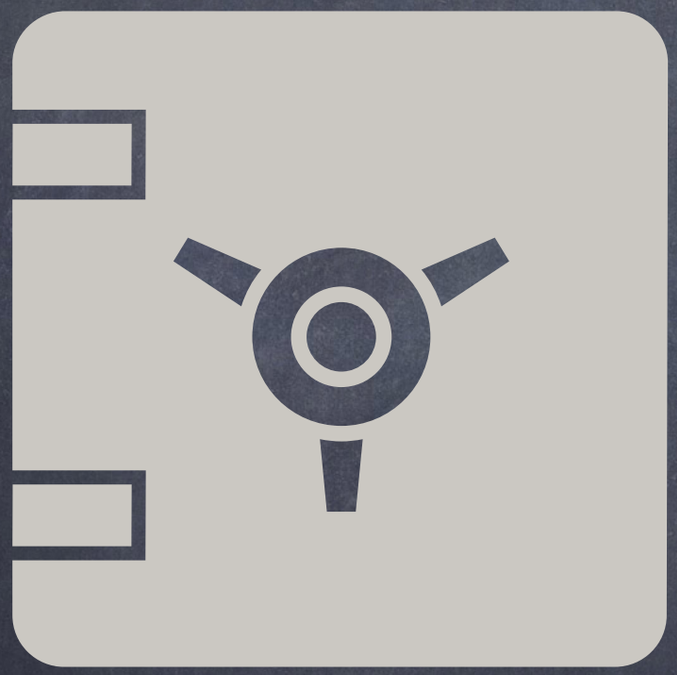
CEX Vs DEX

Few CEXs -> Down/Hacked -> Liquidity/Volatility

Centralization Risk
Risk Awareness

#120

Token Balance



ERC20 Token Balance

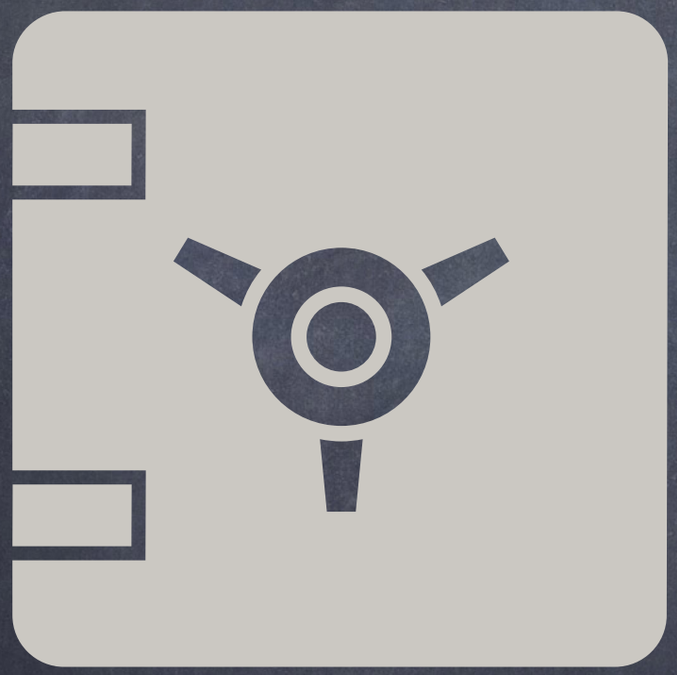
Logic -> Balance

Flash Loans or Whales

Manipulation Risk
Risk Awareness

#121

Token Minting



ERC20 Token
Flash Minting

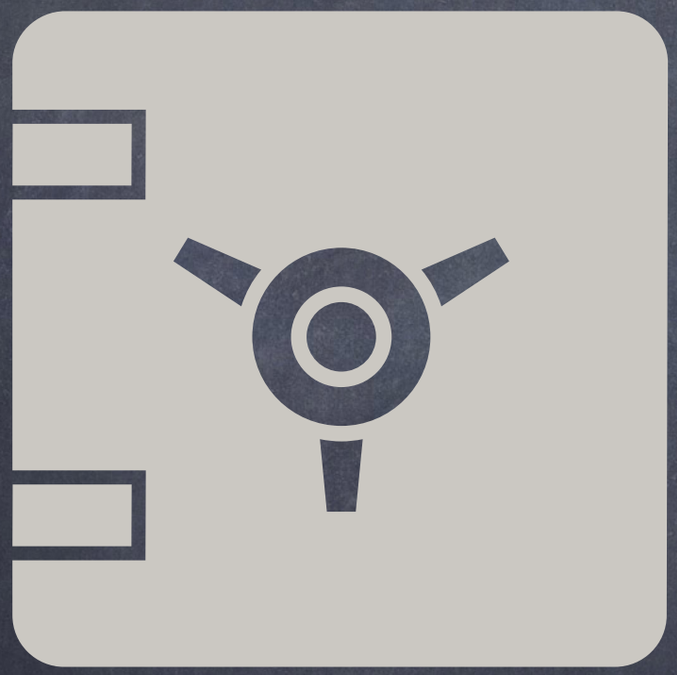
Flash Minting
Vs Flash Loans

Overflows or Balance/
Supply Assumptions

Manipulation Risk
Risk Awareness

#122

ERC 1400
Addresses



ERC1400 Permissioned
Addresses

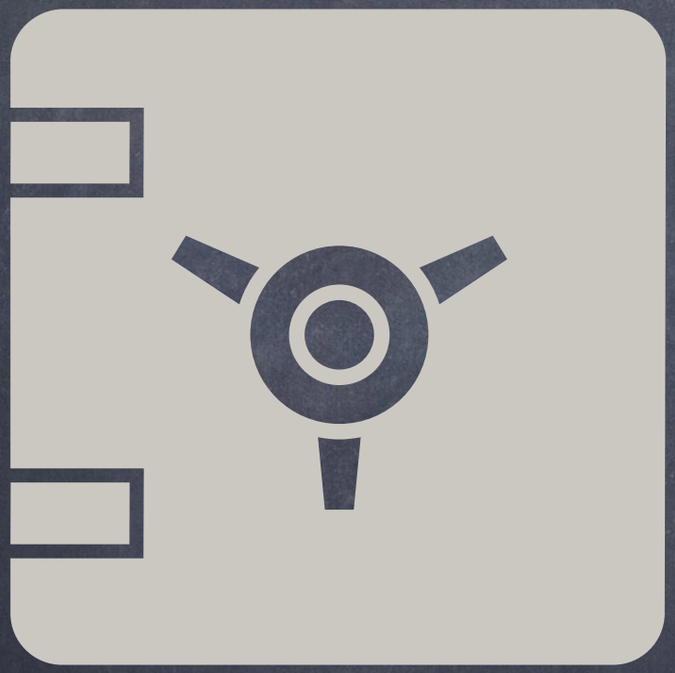
PolyMath
Security Tokens

Block -> Transfers
To/From Addresses

DoS Risk
Risk Awareness

#123

ERC 1400 Transfers



ERC1400 Forced Transfers

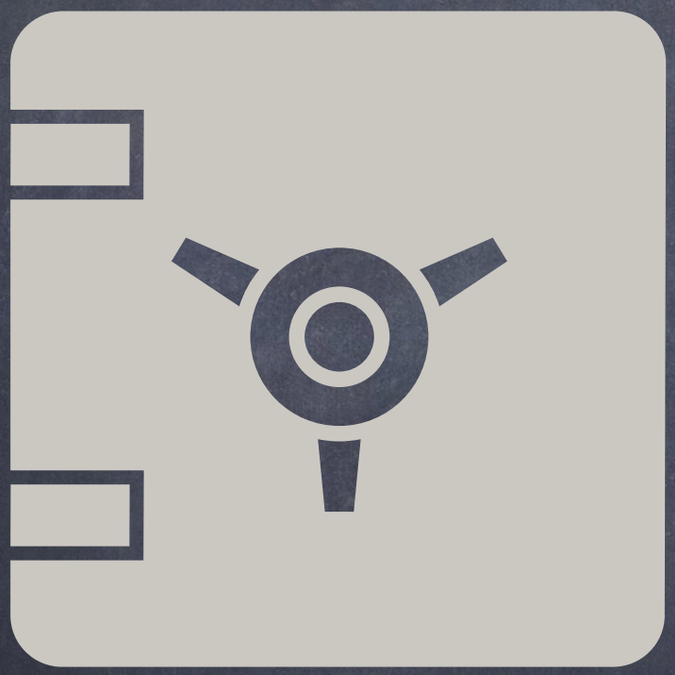
Trusted Actors

Unbounded Transfers

Transfer Risk
Risk Awareness

#124

ERC 1644
Transfers



ERC1644 Forced
Transfers

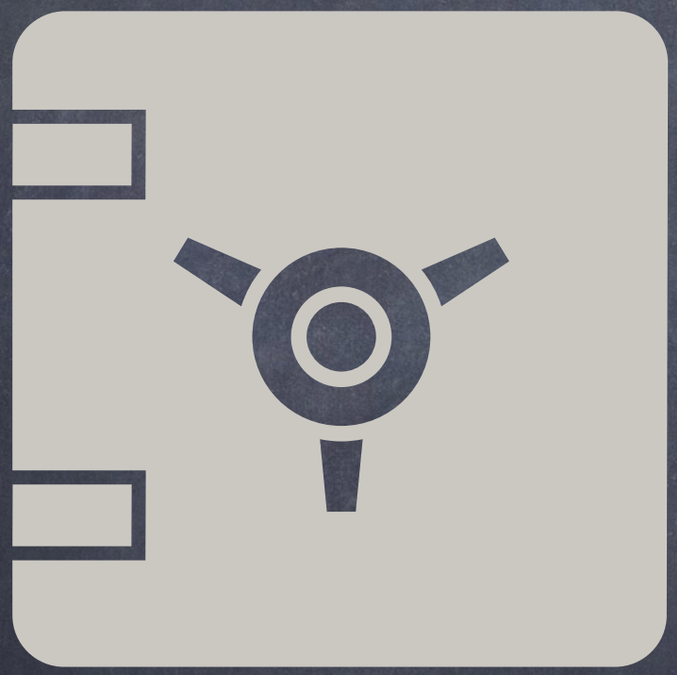
Controller Role
Part of ERC 1400

Controller -> Arbitrary
Transfers -> Steal Funds

Controller Risk
Risk Awareness

#125

ERC 621
totalSupply



ERC 621 totalSupply
Control

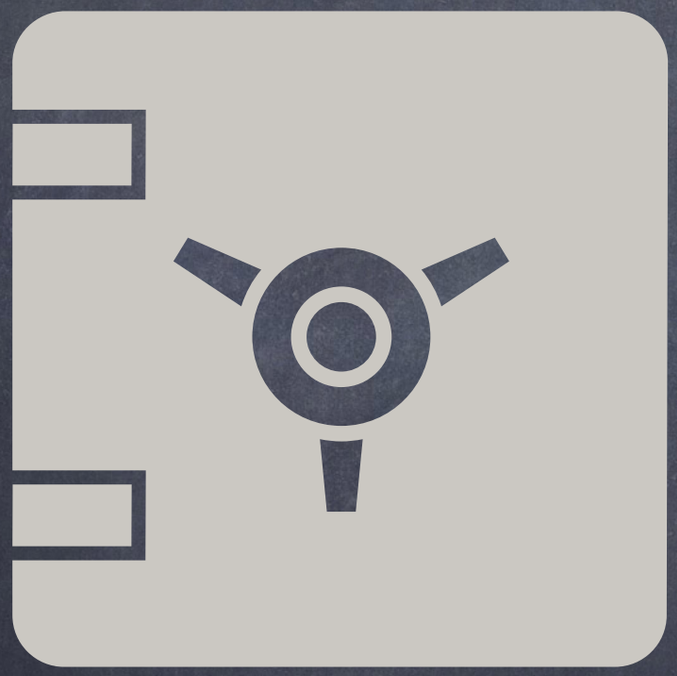
Trusted Actors -> Change
totalSupply

increaseSupply &
decreaseSupply

Token Supply Risk
Risk Awareness

#126

ERC 884
Reissue



ERC 884
Cancel & Reissue

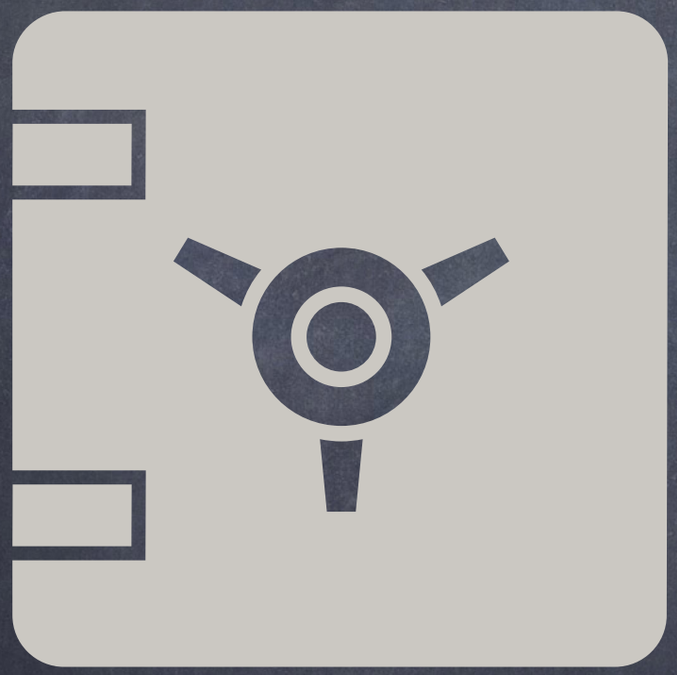
Token Implementers
Cancel Address

Move Tokens -> New
Address

Token Holding Risk
Risk Awareness

#127

ERC 884 Whitelisting



ERC 884 Whitelisting Addresses

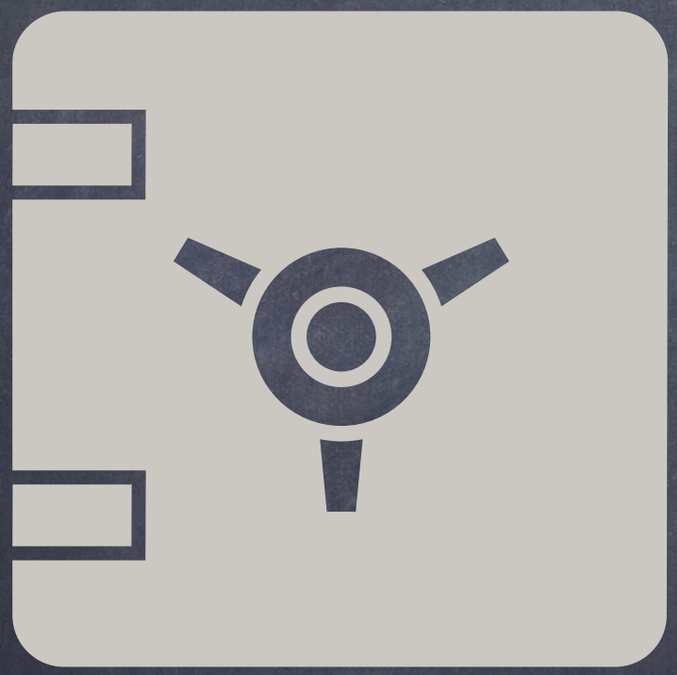
Addresses -> Whitelisted

Token Transfer -> Only To Whitelisted Addresses

Token Transfer Risk Risk Awareness

#128

Asset Limits



Guarded Launch
Asset Limits

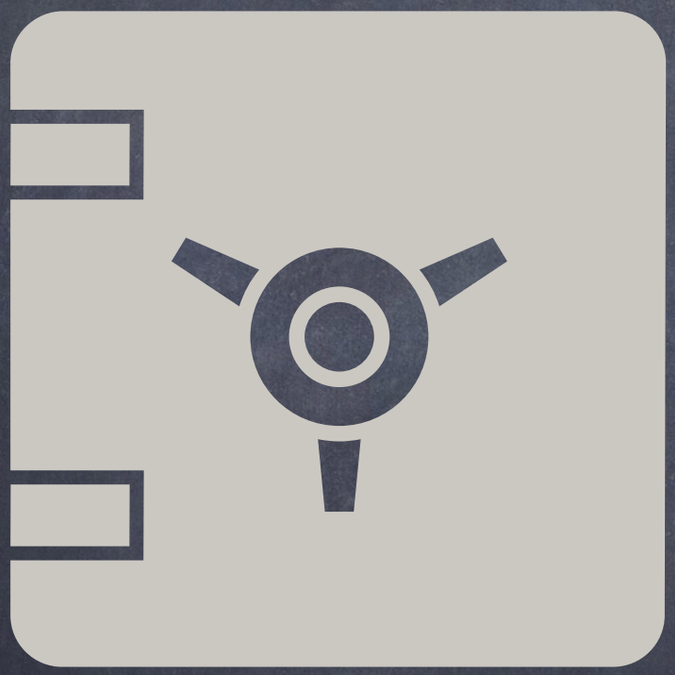
Launch -> Low #Assets
Over Time -> Increase

Launch Time
Higher Risk -> Exploits

Risk Mitigation
Gradually Increase Asset Limits

#129

Asset Types



Guarded Launch
Asset Types

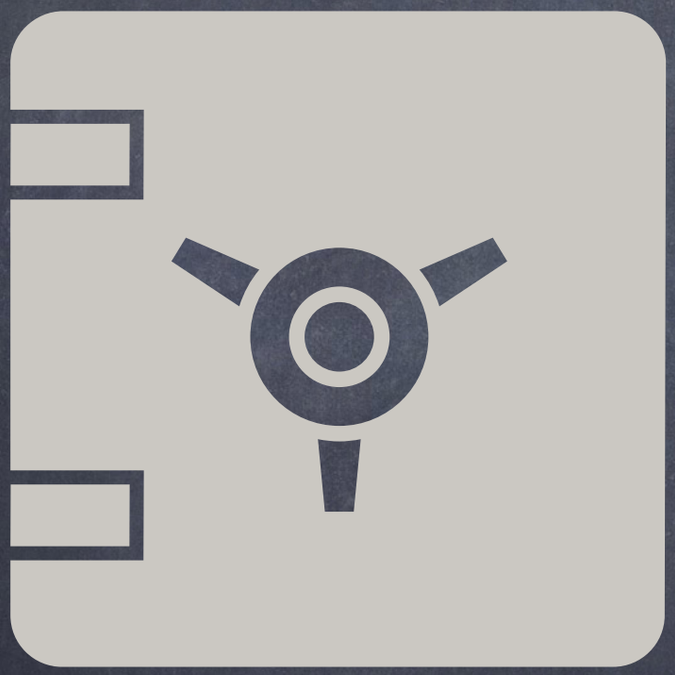
Launch -> Few Types
Over Time -> Increase

First -> Known Assets
Later -> Others

Risk Mitigation
Gradually Increase Asset Types

#130

User Limits



Guarded Launch
User Limits

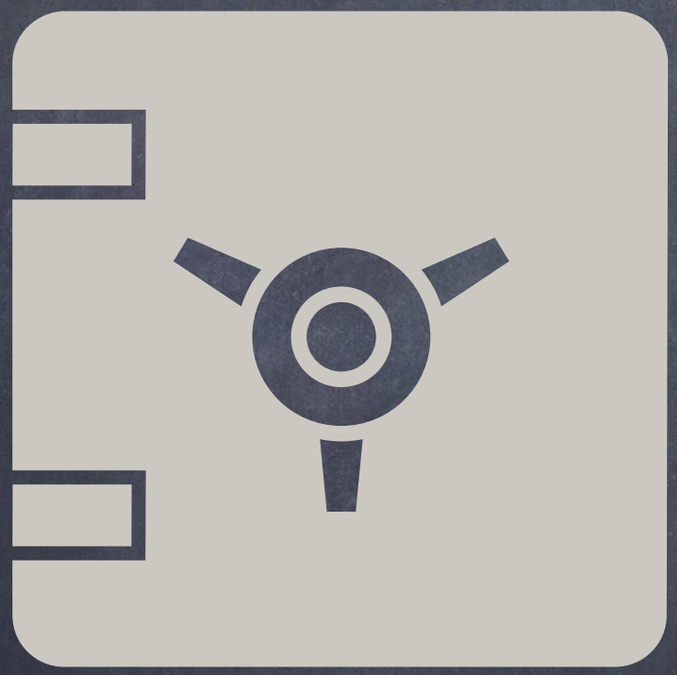
Launch -> Few/Trusted Users
Over Time -> Increase

Launch Time
Higher Risk -> Exploits

Risk Mitigation
Gradually Increase Users

#131

Usage Limits



Guarded Launch
Usage Limits

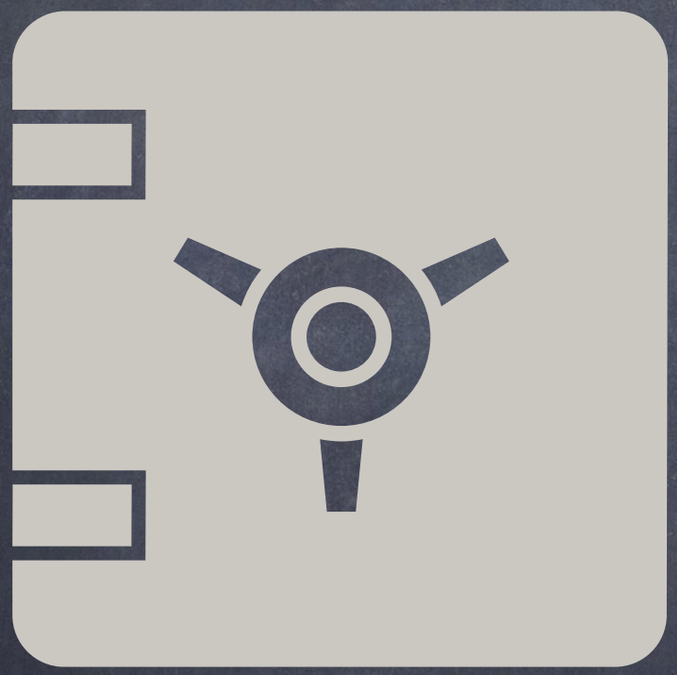
Launch -> Limited Usage
Over Time -> Increase

Tx Size, Tx Volume, Daily Limit, Rate Limiting

Risk Mitigation
Gradually Increase Usage

#132

Composability
Limits



Guarded Launch
Composability Limits

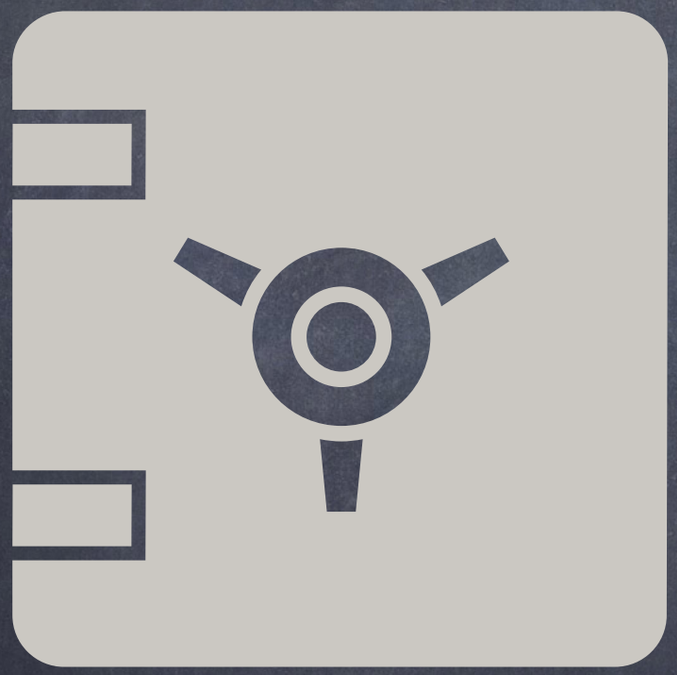
Launch -> Limited
Composability
Over Time -> Increase

First -> Known Protocols
Later -> Others

Risk Mitigation
Gradually Increase

#133

Escrow



Guarded Launch
Escrowed Funds

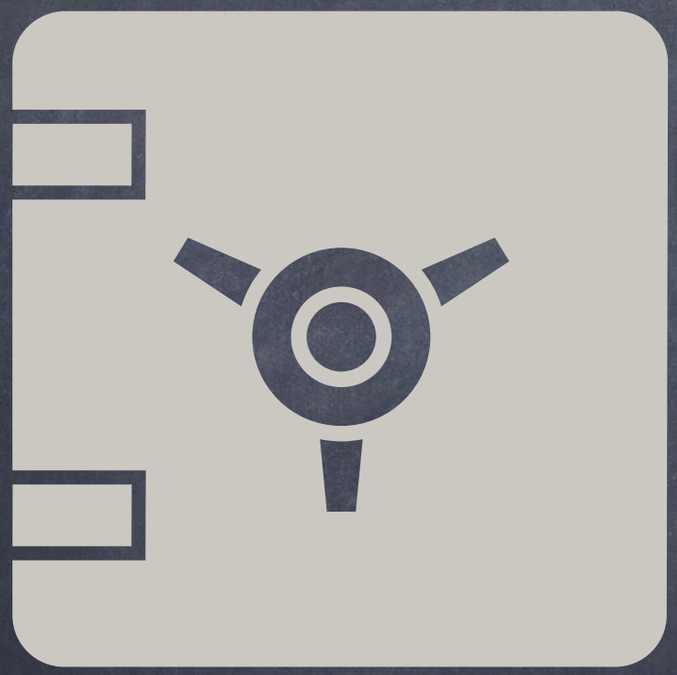
High-value Tx -> Escrow
Timelock/Gov -> Revert

First -> Escrow
Later -> No Escrow

Risk Mitigation
Initially Escrow

#134

Circuit Breaker



Guarded Launch
Circuit Breaker

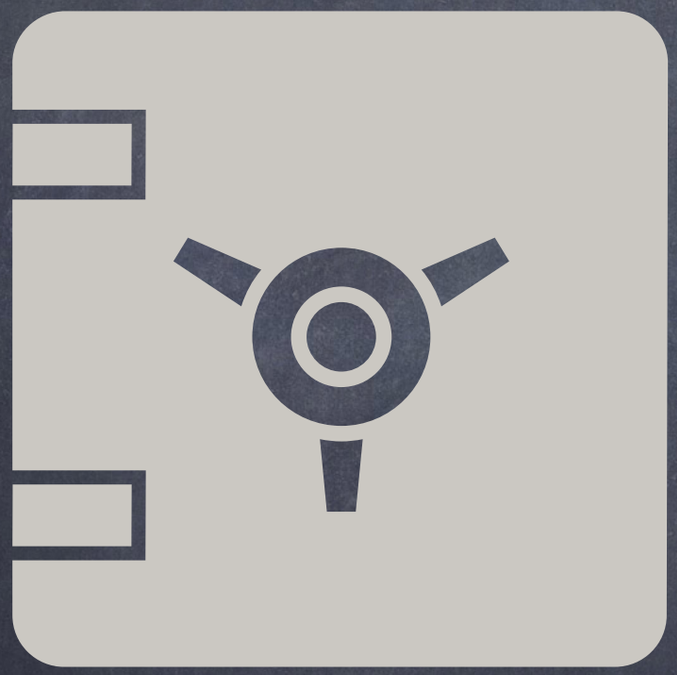
Emergency -> Pause
Recover -> Unpause

First -> Pause/Unpause
Later -> No Circuit Breaker

Risk Mitigation
Initially Pause/Unpause

#135

Emergency
Shutdown



Guarded Launch
Emergency Shutdown

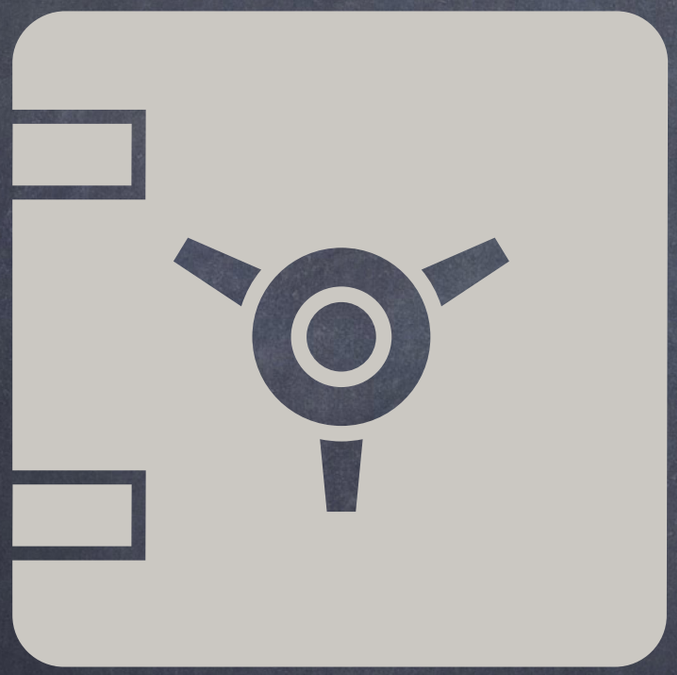
Emergency -> Shutdown
Reset -> Restart

First -> Capability
Later -> Remove

Risk Mitigation
Emergency Shutdown

#136

System Specification



Requirements -> Specification

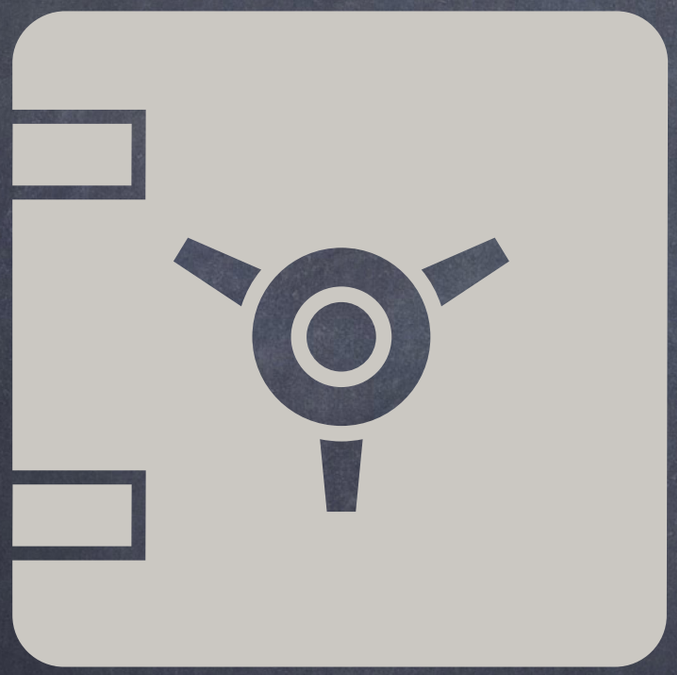
Why & How
Spec <-> Requirements

No Spec -> No Baseline

Requirements -> Design
Specify -> Evaluate

#137

System Documentation



Implementation -> Documentation

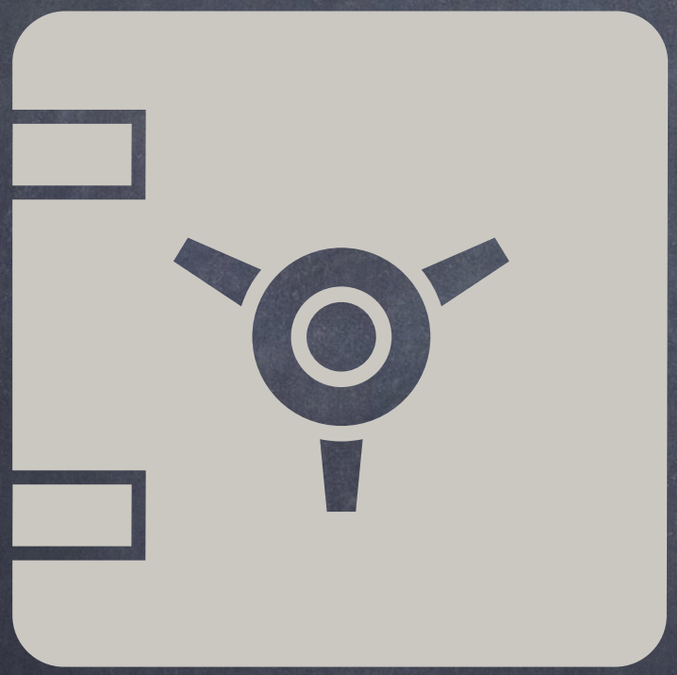
What & How
Implement <-> Document

Assets/Actors/Actions
Trust/Threat Model

Specify -> Implement ->
Document -> Evaluate

#138

Function Parameters



Function Parameters
Input Validation

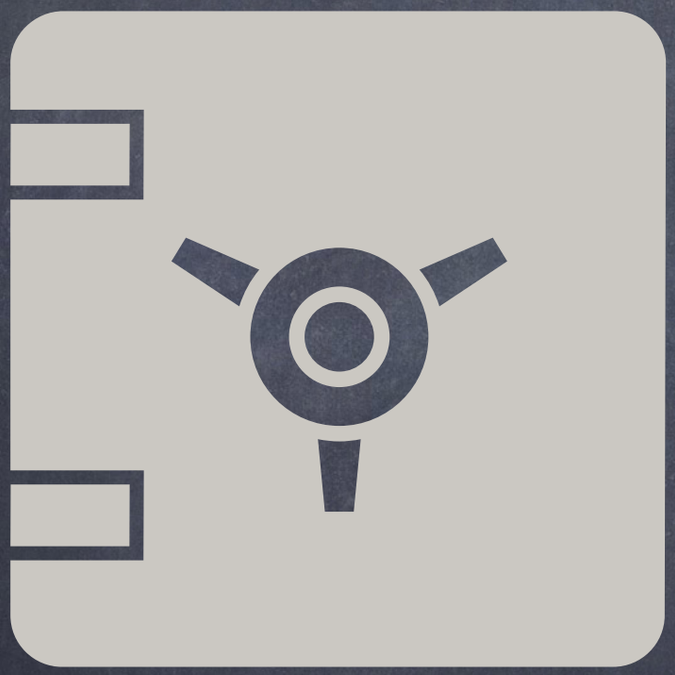
Public/External Functions
Taint Analysis

Sanity/Threshold Check
Address -> Zero

Malicious/Accidental
Incorrect/Invalid Values

#139

Function Arguments



Function Arguments
Call Sites

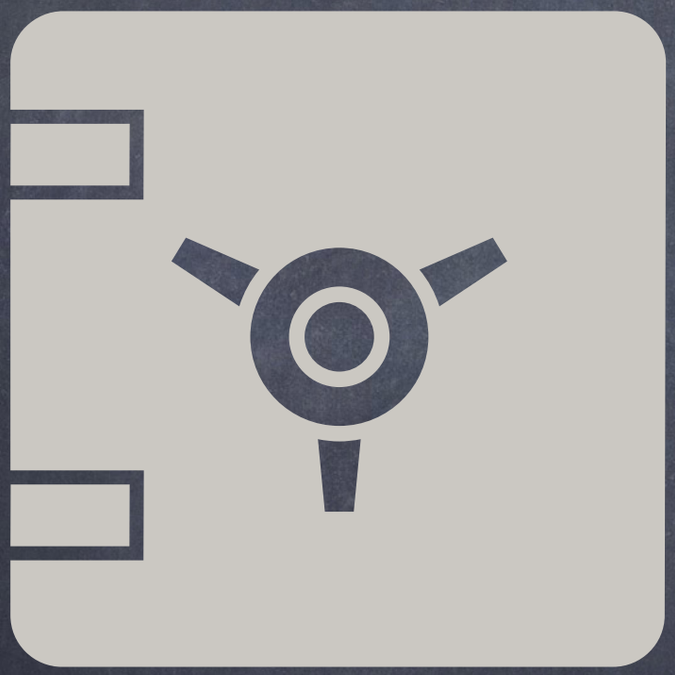
Arguments Vs Parameters
Callers Vs Callees

Arguments -> Validity/
Order

Check Function Calls
Valid/Orderly Arguments

#140

Function Visibility



Public -> External -> Internal -> Private

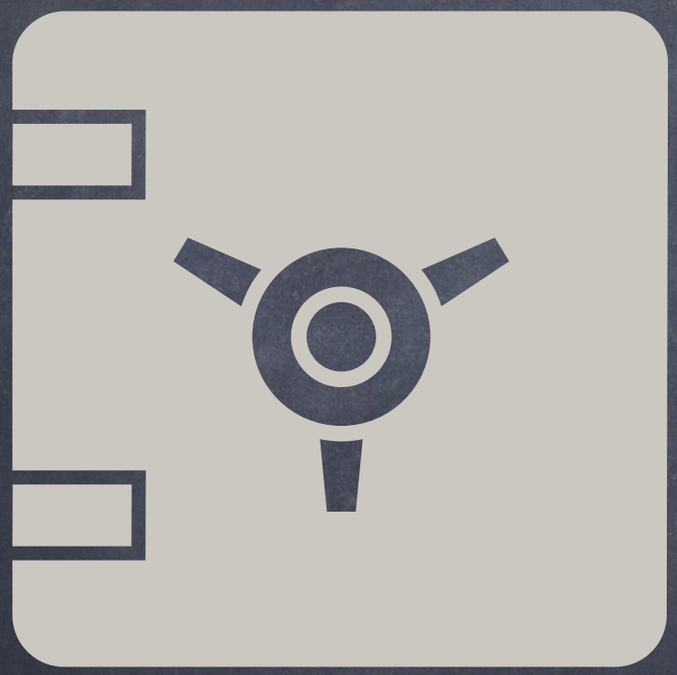
Strictest Visibility

Public/External -> Anyone

Use <-> Abuse
Byzantine Threat Model

#141

Function Modifers



Modifiers -> Access Control & Validation

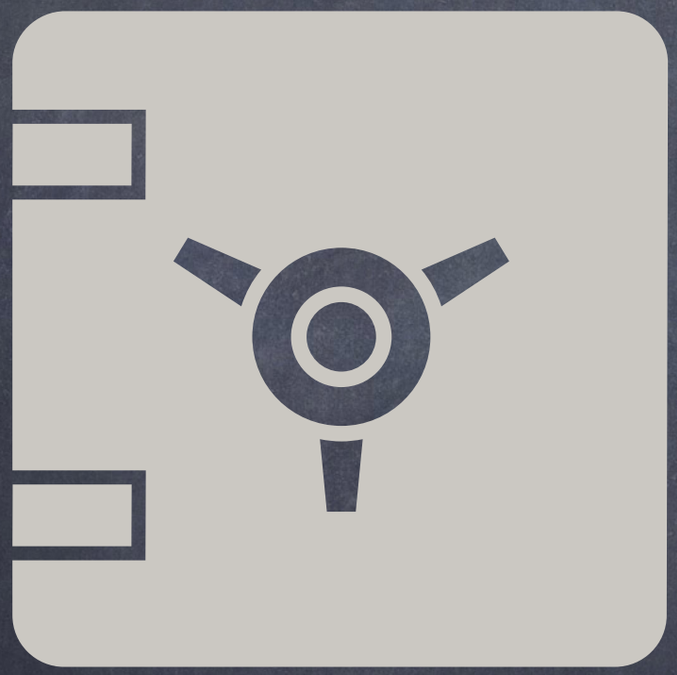
Modifiers: Missing/ Incorrect/Order

Control -> Authorize
Data -> Validate

Ensure Correct Modifiers

#142

Function
Returns



Function Call -> Return
Return Values

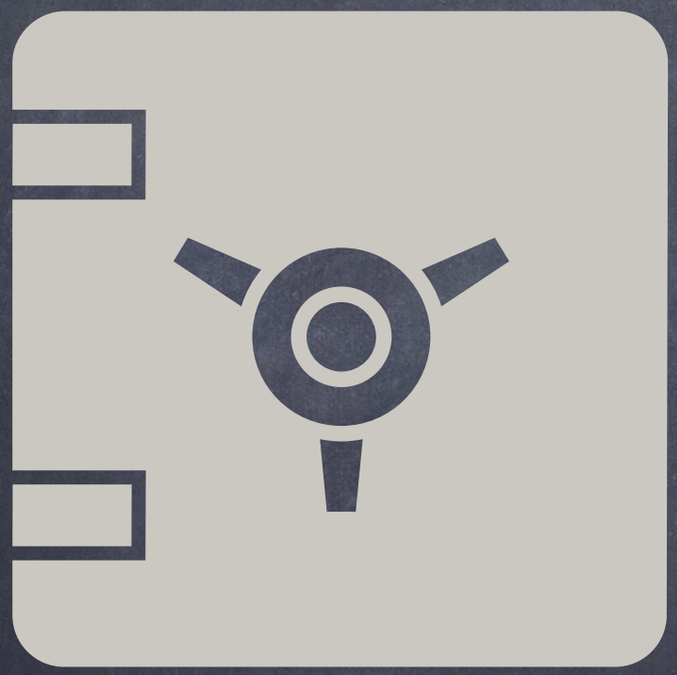
Return Values
Correct & All Paths

Call Sites -> Use/Ignore

Return Values
Error Checking/Handling

#143

Function
Timeliness



Function Calls
Timeliness -> When

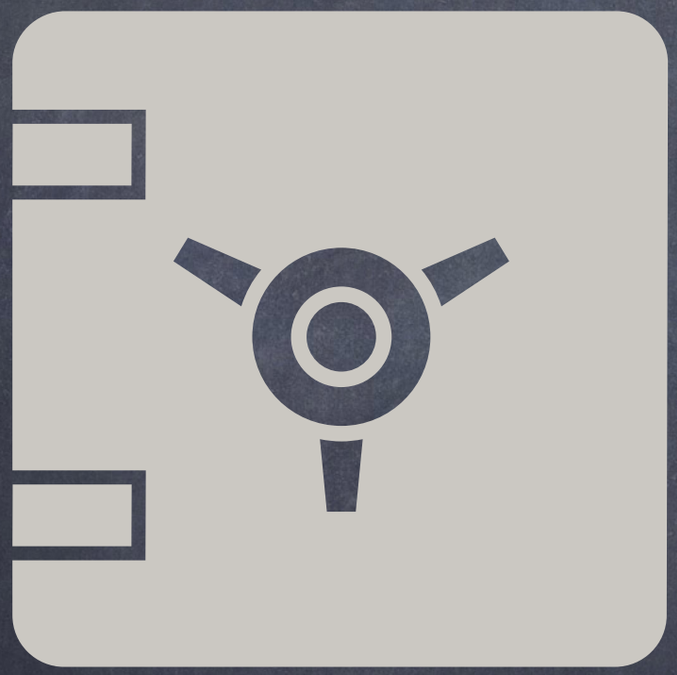
Public/External
Called Anytime

State Transitions
Assumptions on When

When -> Arbitrary
Robust Handling

#144

Function
Repetitiveness



Function Calls
Repetitiveness -> How Many

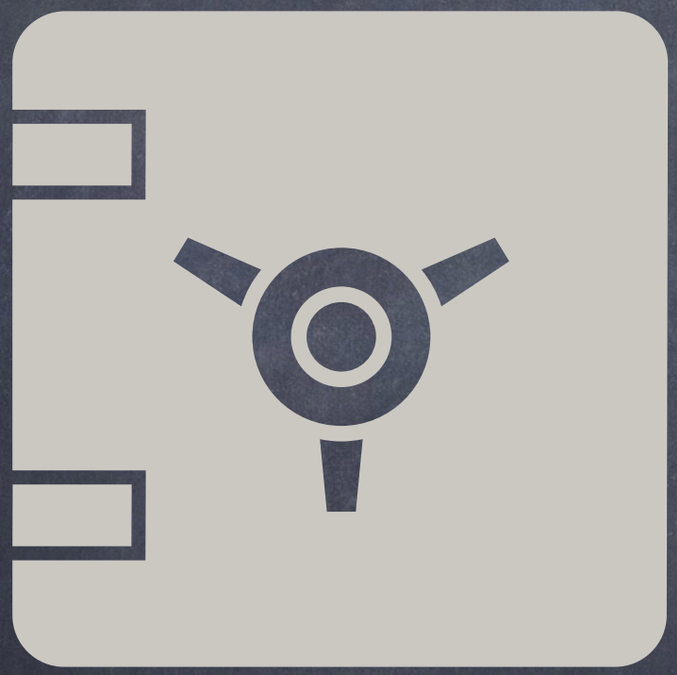
Public/External
Called Any #Times

State Transitions
Assumptions on #Calls

How Many -> Arbitrary
Robust Handling

#145

Function
Order



Function Calls
Order -> Which+When

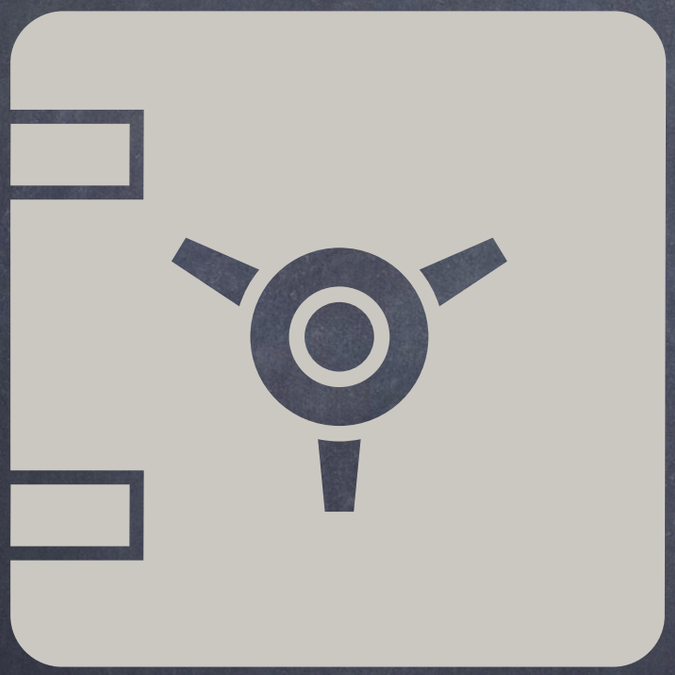
Public/External
Called Any Order

State Transitions
Assumptions on Order

Order -> Arbitrary
Robust Handling

#146

Function
Inputs



Function Calls
Inputs -> What

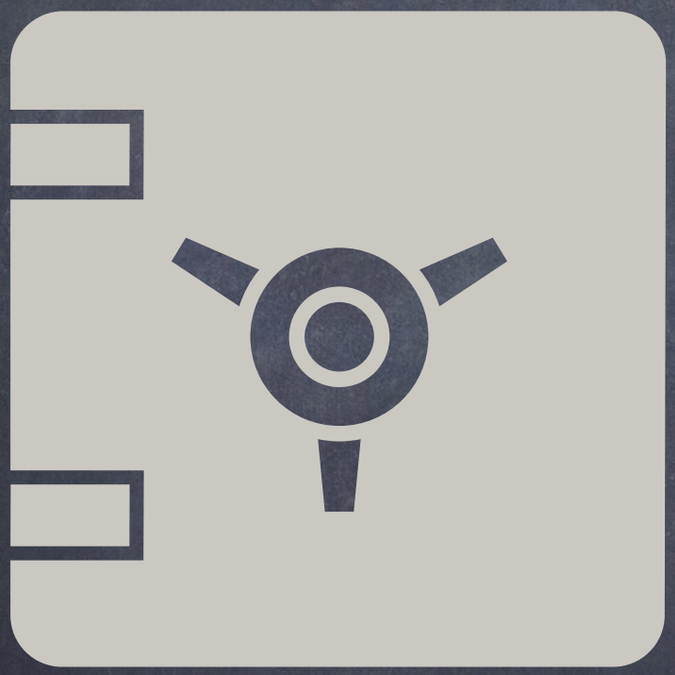
Public/External
Called w/ Any Inputs

Assumptions on Validity

Inputs -> Arbitrary
Input Validation

#147

Conditionals



Conditionals -> Control Flow

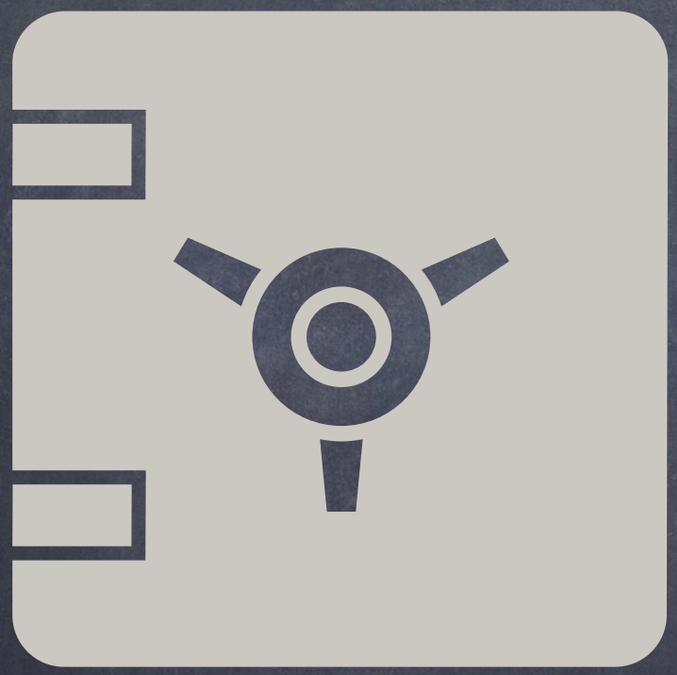
if/else/for/while/do
break/continue/return

Predicates & Expressions
Variables & Operators

E.g. || Instead of &&
Check Conditionals

#148

Access Control Spec



Access Control -> Assets/ Actors/Actions

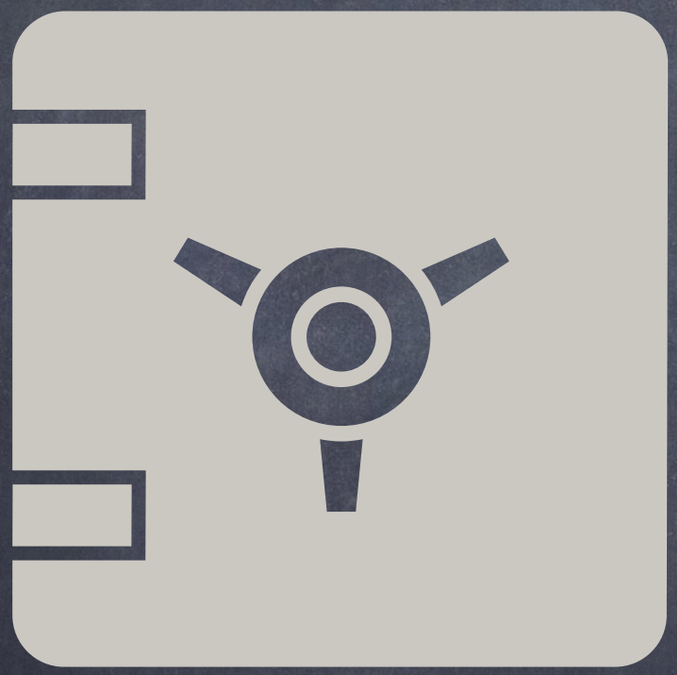
Spec: Who/What/Why/ When/How-Much

Trust/Threat Model & Assumptions

Spec -> Implement -> Enforce -> Evaluate

#149

Access Control
Implementation



Access Control
Spec -> Implement

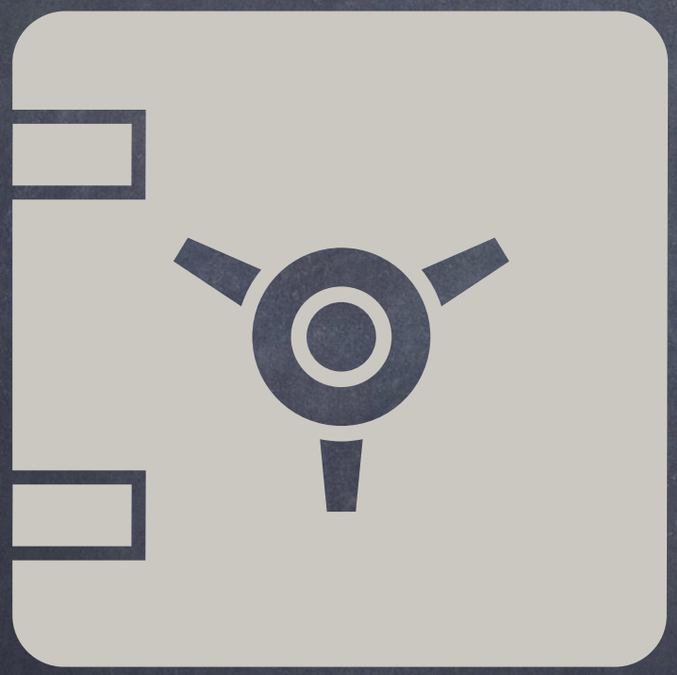
Implement/Enforce
Actors -> Assets

No Missing Actors/Assets/
Flows/Conditions

Spec -> Implement ->
Enforce -> Evaluate

#150

Access Control Modifiers



Access Control Modifiers -> Enforce

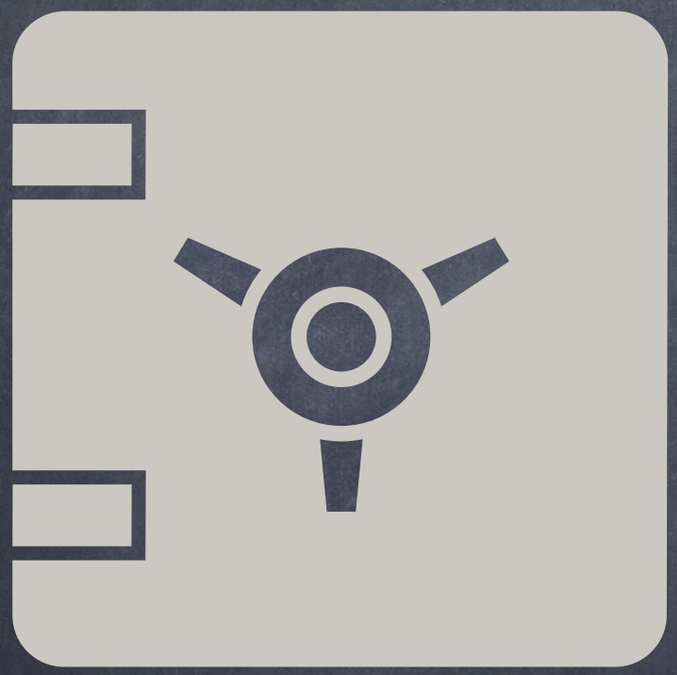
Modifiers -> Encapsulate Repetitive Checks

Functions <-> Modifiers
Modularity Vs Auditability

Present & Valid & Correct

#151

Modifiers
Implementation



Modifiers
Incorrect Implementation

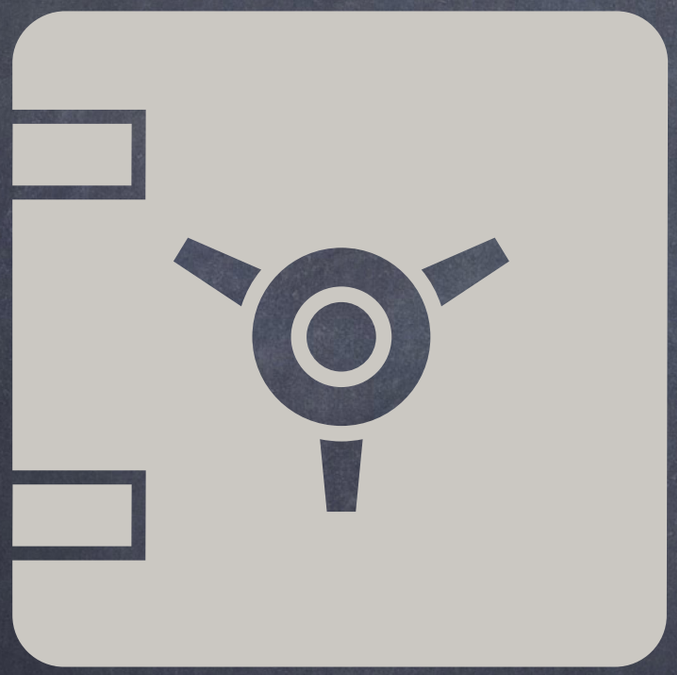
Roles & Privileges

Correct Checks & Roles &
Composition

Ensure Correct
Implementation

#152

Modifiers
Usage



Modifiers
Incorrect Use

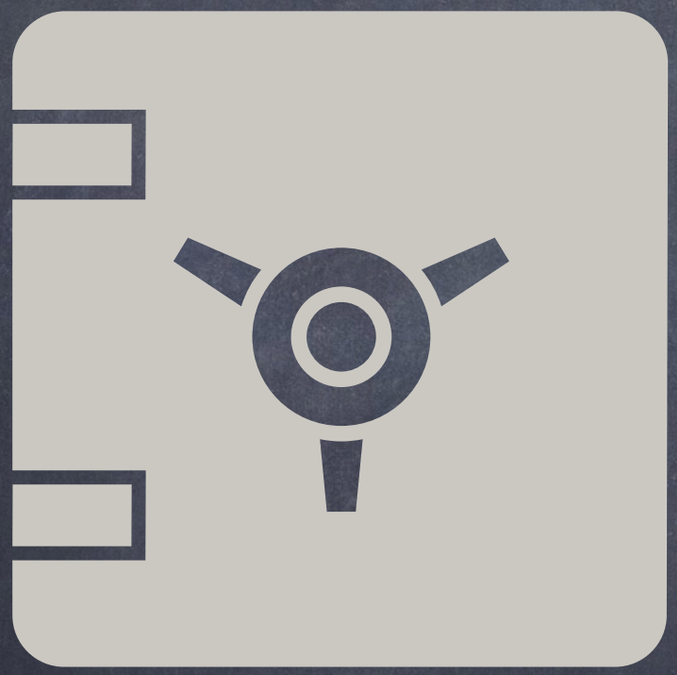
Modifiers -> Which/Why/
How/What/When/Where

Correct Functions &
Modifiers & Parameters

Ensure Correct Usage

#153

Access Control
Changes



Access Control
Correct Changes

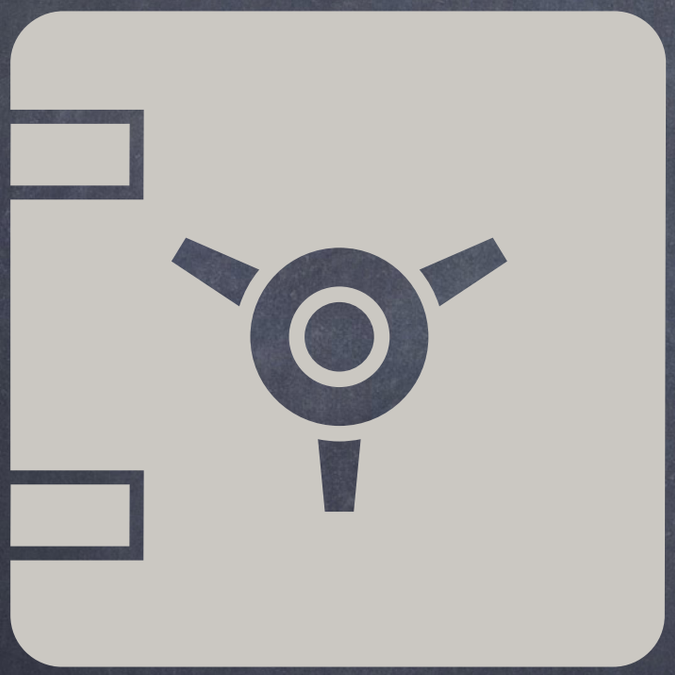
Change -> Assets/Actors/
Actions

Risk: Wrong/Timeliness
Impact: Loss/Lock Funds

Validate/Two-step/Log
Ensure Correct Changes

#154

Comments



Code Comments
Documentation

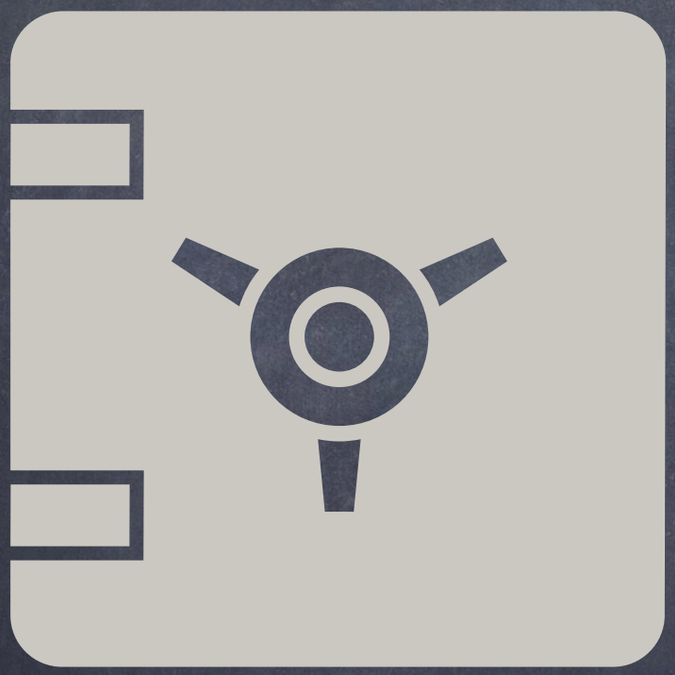
Inline & Natspec
Details & Relevance

Readability &
Maintainability

Sync: Code <-> Comment
Sufficient Comments

#155

Testing



Software Testing
Validation

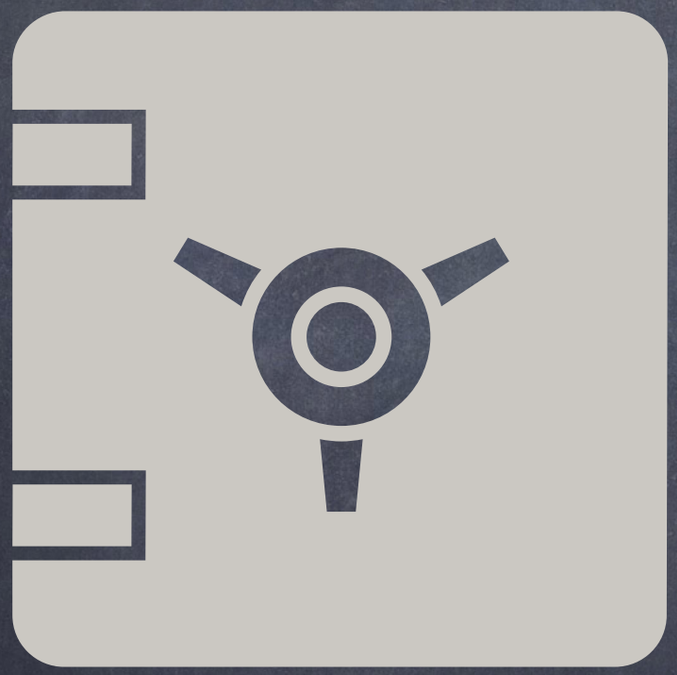
Unit/Functional/
Integration/Regression/E2E

Smoke/Stress/Perf/Security
Testnet Vs Mainnet

Test Vs Production
Sufficient Testing

#156

Unused



Unused Constructs

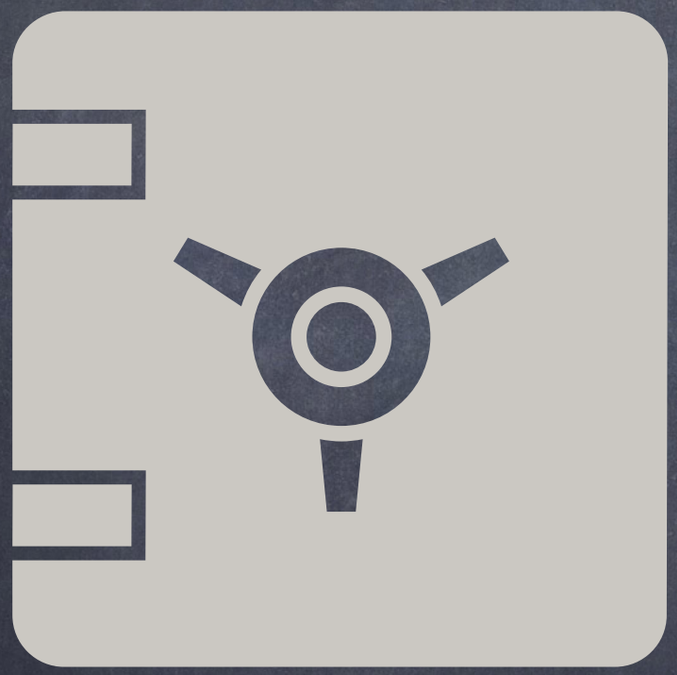
Imports/Contracts/Functions/
Variables/Events/Returns

Reduce Gas
Improve Auditability/
Maintainability

Missing Logic & Assumptions
Remove/Use Unused Constructs

#157

Redundant



Redundant Constructs

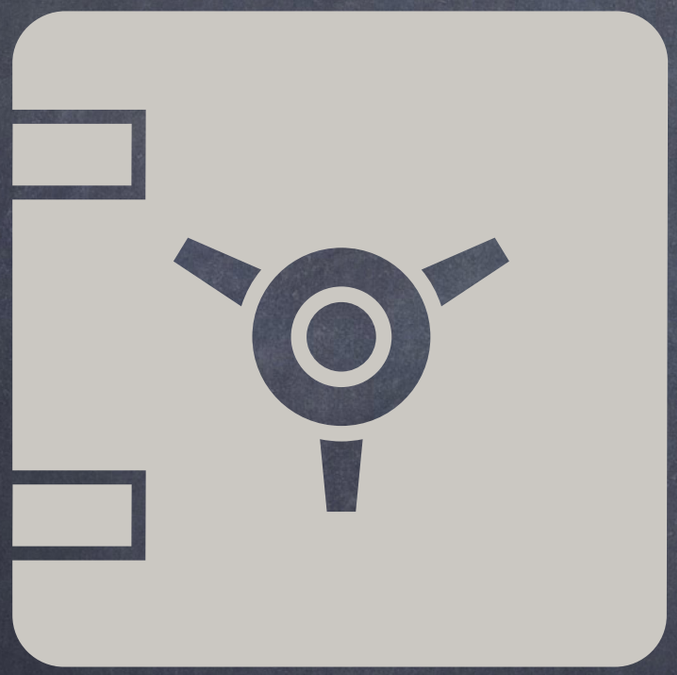
Code & Comments

Reduce Gas
Improve Auditability/
Maintainability

Missing Logic & Assumptions
Remove/Fix Redundant
Constructs

#158

ETH



ETH Handling
Deposit/Withdraw/Transfer

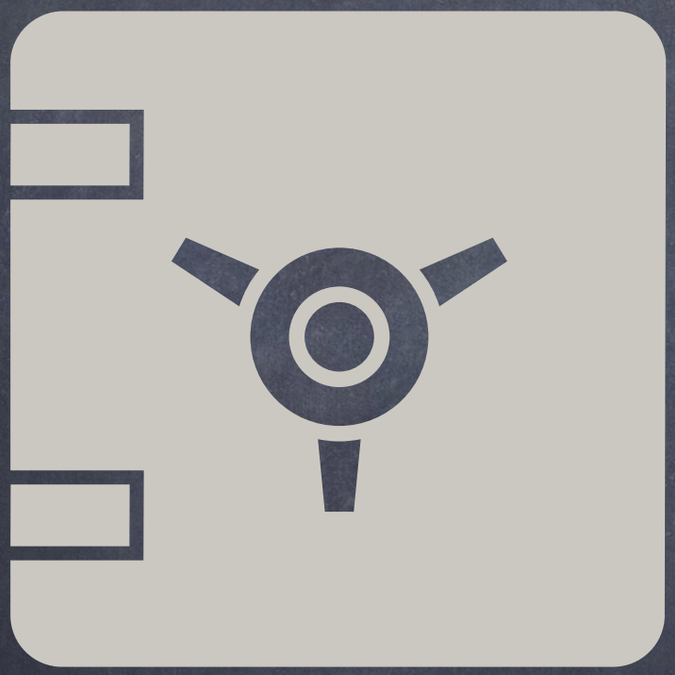
msg.value/payable/
withdraw/balance/transfer

Reentrancy/Locking/Access
Control/Input Validation/Error
Handling

Contracts/Functions
Ensure Correct ETH Handling

#159

Tokens



Token Handling
Deposit/Withdraw/Transfer

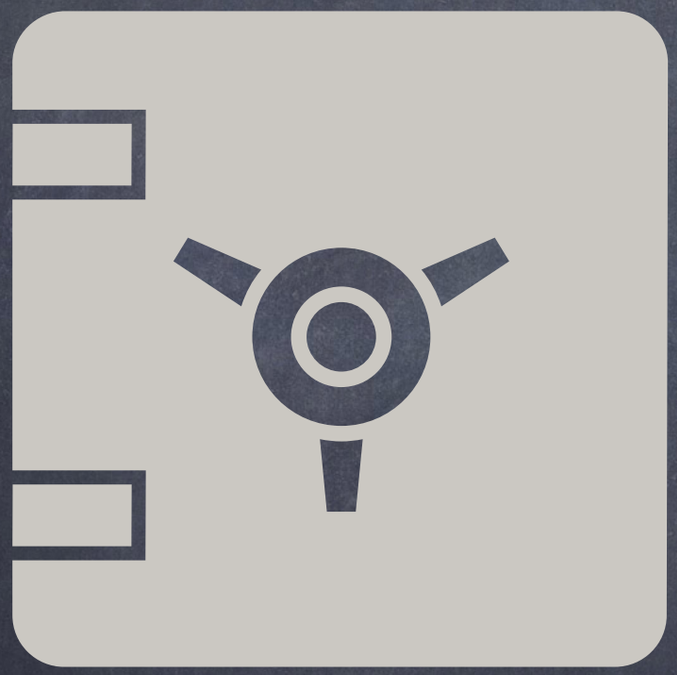
Types of Tokens
Token Functions

Reentrancy/Locking/Access Control/Input Validation/Error Handling

Contracts/Functions
Ensure Correct Token Handling

#160

Actors



System Actors
Users/Admins/Roles

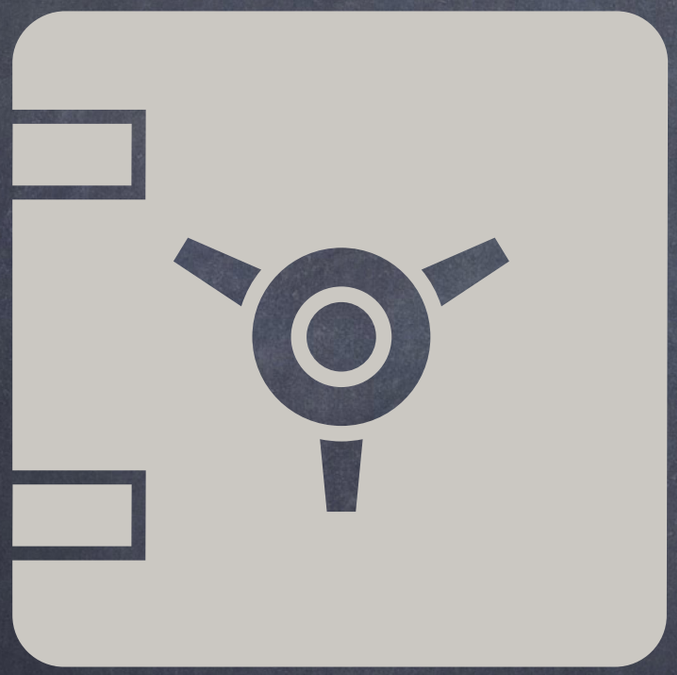
Trusted Vs Untrusted
Use <-> Abuse

Actors -> Assets -> Actions
Specify & Implement & Evaluate

Actors -> Trust Vs Threat
Byzantine Threat Model

#161

Privileged Roles



Privileged Roles/Actions

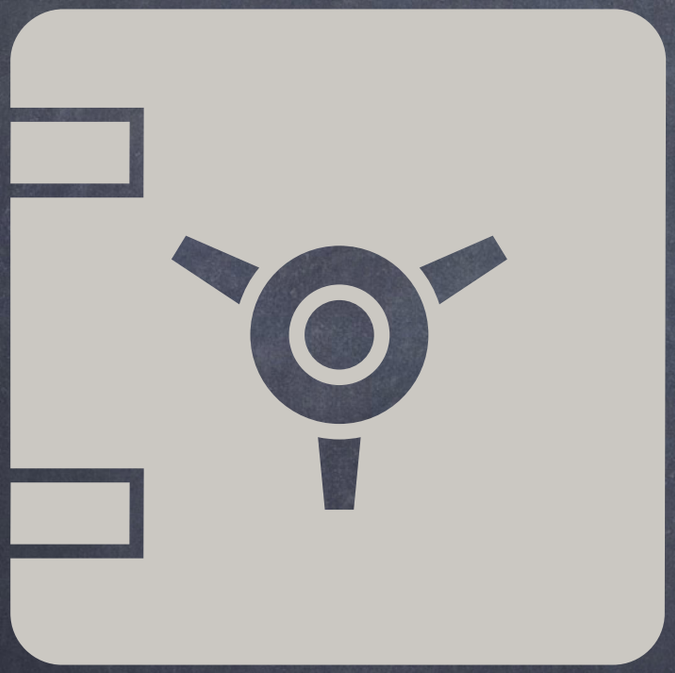
Deploy/Modify/Pause/
Shutdown/Withdraw/Whitelist

EOA Vs MultiSig

EOA -> Single Point of Failure
MultiSig -> Privilege Separation

#162

Privileged Roles



Two-step Change

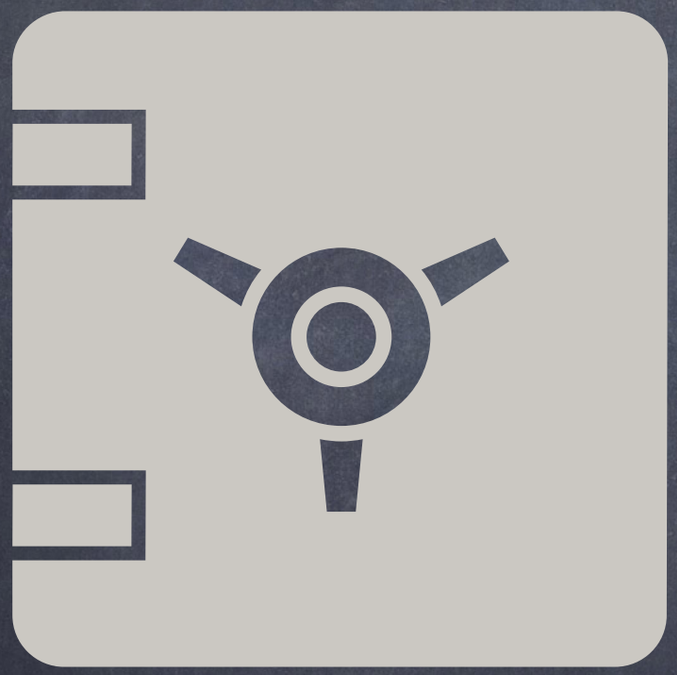
One-step -> Error-prone
Zero/Incorrect Address

Step 1: Old Approves New
Step 2: New Claims Ownership

Error Recovery in Step 1
Risk Mitigation

#163

Critical Parameters



Delay Change -> Time Lock

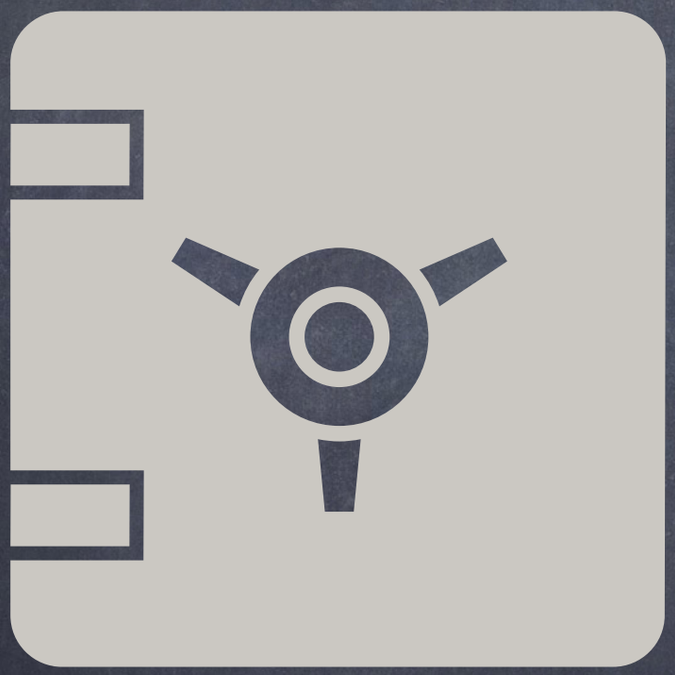
Immediate Change -> Unfair
E.g.: Lower Rewards, Increase Fees

Event + Time-delay
Users -> Exit/Engage

Time-delayed Change
Less Surprise, More Fair

#164

Explicit Vs Implicit



Favor Explicit Over Implicit

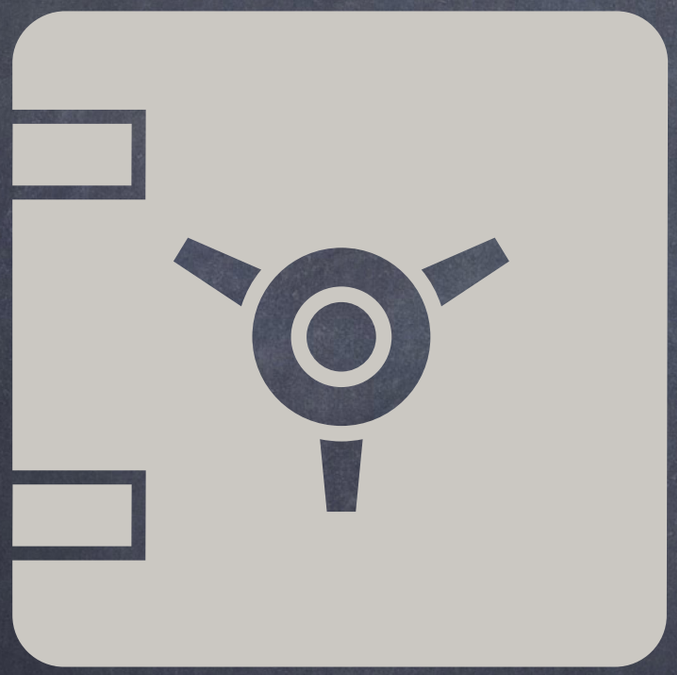
Solidity -> Explicit Visibility/Location

App -> Explicit Spec + Reqs + Validation + Docs

Implicit Reqs + Assumptions -> Dangerous

#165

Configuration



Misconfiguration -> Security Issues

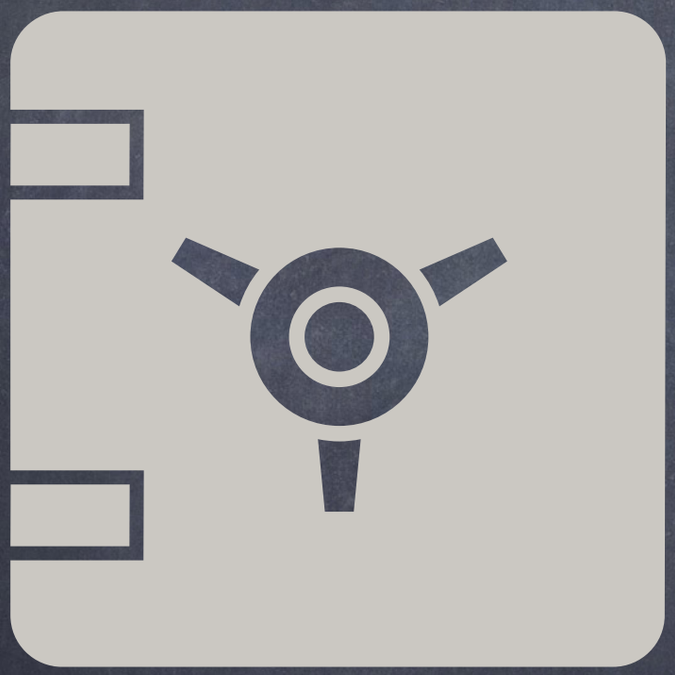
Contracts, Parameters, Addresses, Permissions

Production Vs Test

Check Configuration

#166

Initialization



Lack/Incorrect Initialization ->
Security Issues

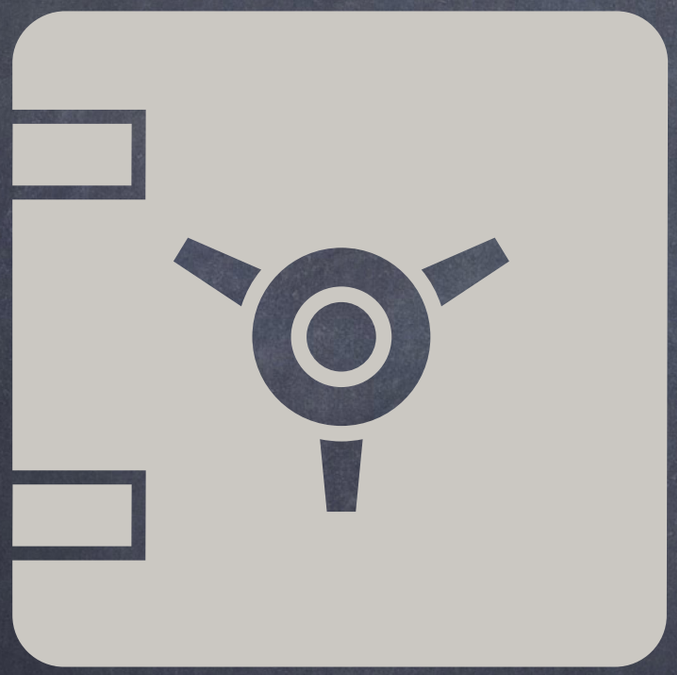
Parameters, Addresses,
Permissions, Roles

Default/Incorrect Values

Check Initialization

#167

Cleanup



Lack/Incorrect Cleanup ->
Security Issues

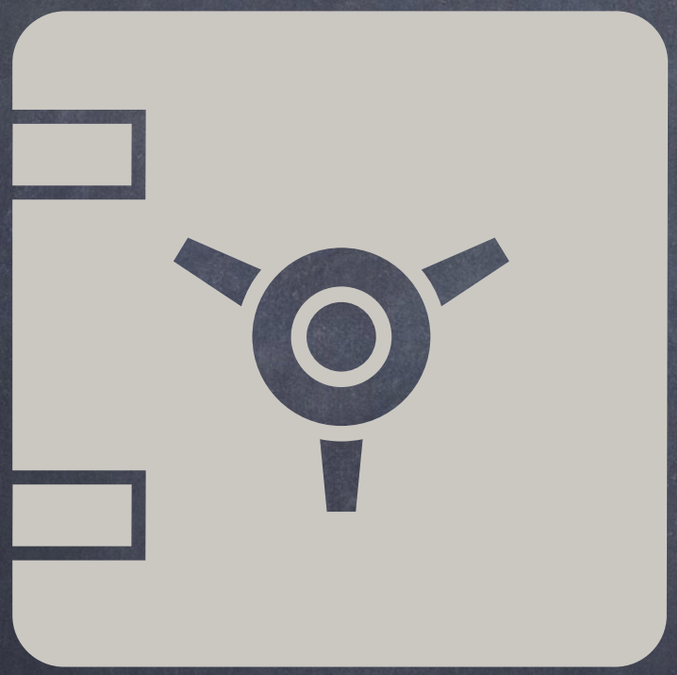
Contract State

Stale State -> Old Values
Incorrect Reads/Writes

Cleanup -> Gas Refunds +
Better Security

#168

Data Processing



Processing Issues ->
Security Issues

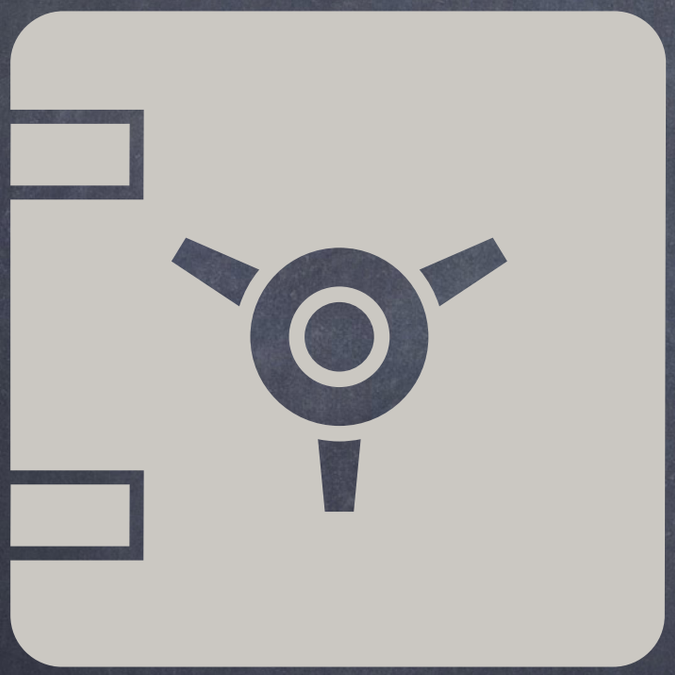
Application Logic
Critical/Tainted Data

Missed/Incorrect
Processing

Spec -> Implement
Check Data Processing

#169

Data Validation



Validation Issues -> Security Issues

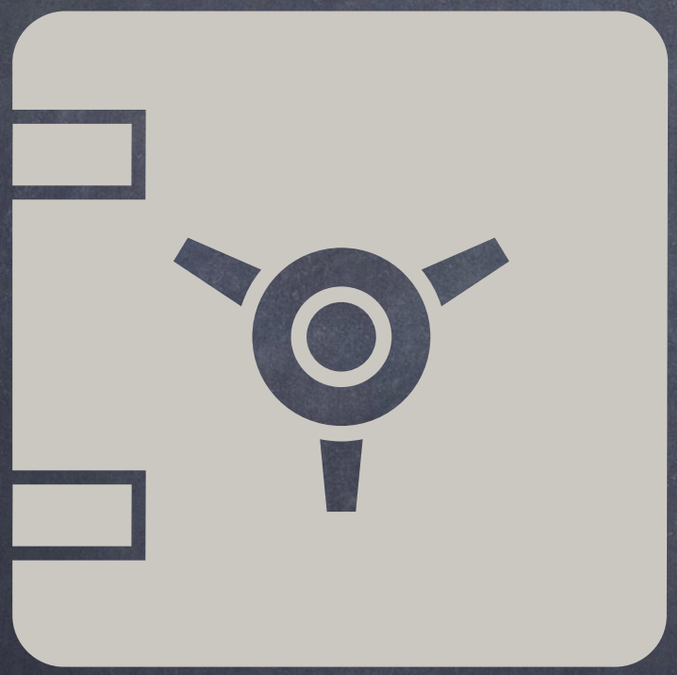
Untrusted Users & Tainted Data

Missed/Incorrect Validation

Sanity/Threshold Checks Check Data Validation

#170

Numerical Issues



Numerical Issues -> Security Issues

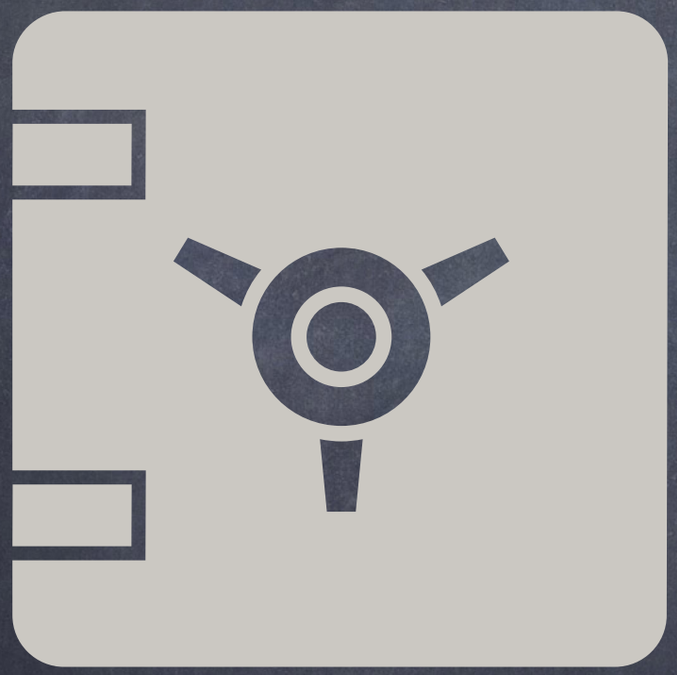
Overflow/Underflow, Precision, Casting, Parameters/ Returns, Decimals, Bounds/Gas

Widely-used Libraries, Best-practices

Testing/Fuzzing
Check Numerical Issues

#171

Accounting Issues



Accounting Issues -> Security Issues

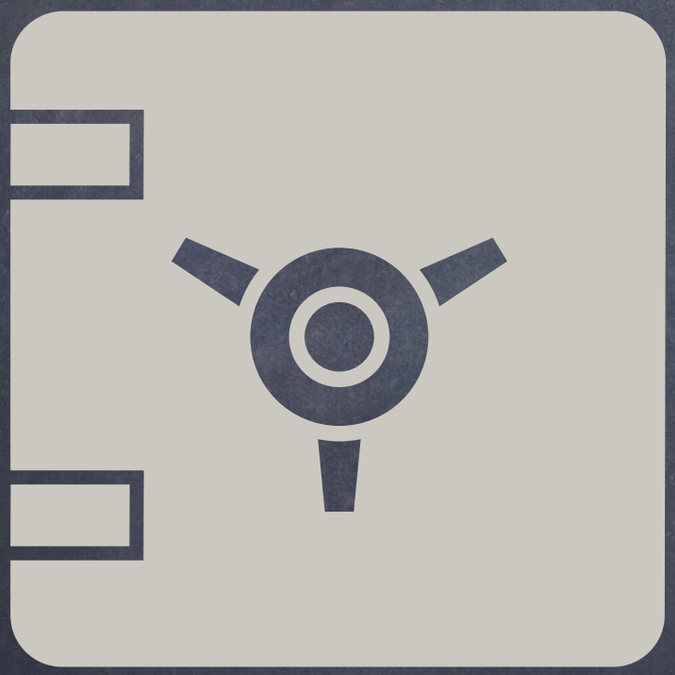
E.g.: Users, Balances, Rewards/Penalties, Fees

App Logic -> State Updates/Transitions

Spec -> Implement
Check Accounting Issues

#172

Access Control



Access Control -> Authorization

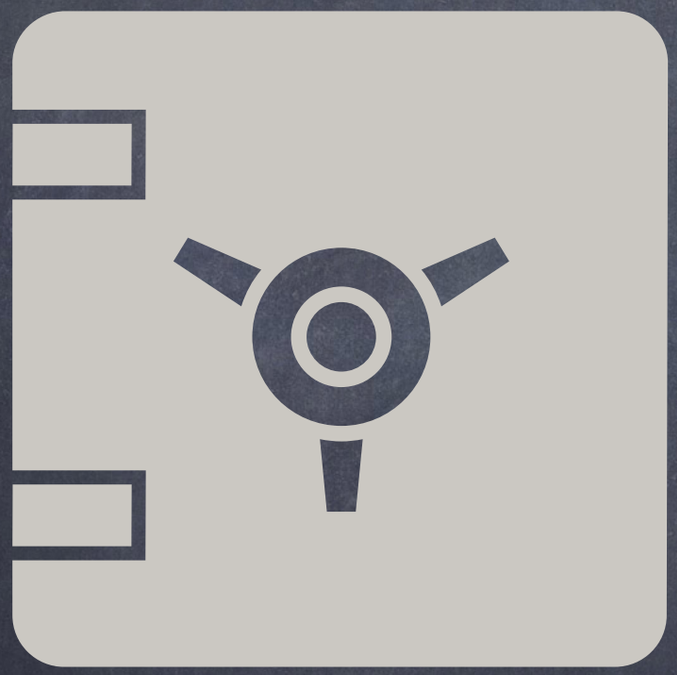
E.g.: Users, Roles, Permissions, Modifiers, Visibility, Address, Accounts, Keys

Assets/Actors/Actions
Trust/Threat Model

Spec -> Implement
Check Access Control

#173

Auditing & Logging



Auditing & Logging -> Monitoring Security

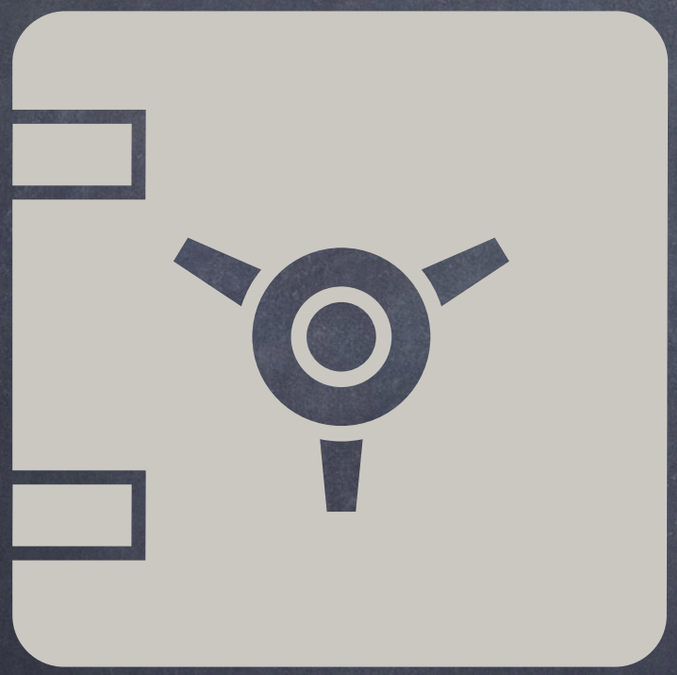
E.g.: Events/Emits, Public Variables, Public/External Getters, Error Strings

Off-chain & On-chain Monitor/Detect/Recover

Correct & Sufficient Audit Logs -> Security

#174

Cryptography



Cryptographic Primitives
On-chain & Off-chain

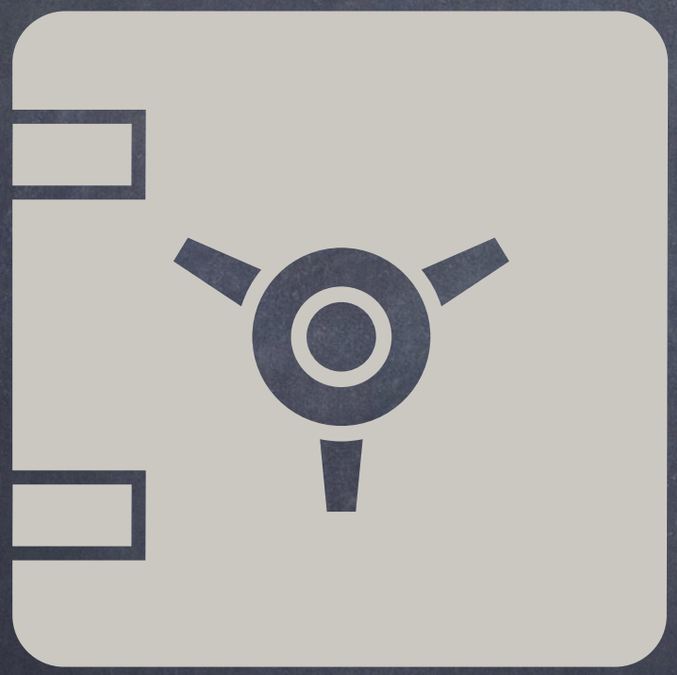
Keys, Accounts, Hashes,
Signatures, Randomness

ECDSA & Keccak-256
More: BLS, RANDAO, VDF, ZK

Fundamental -> Critical
to Security

#175

Error Reporting



Errors -> Exploit
Security Issues

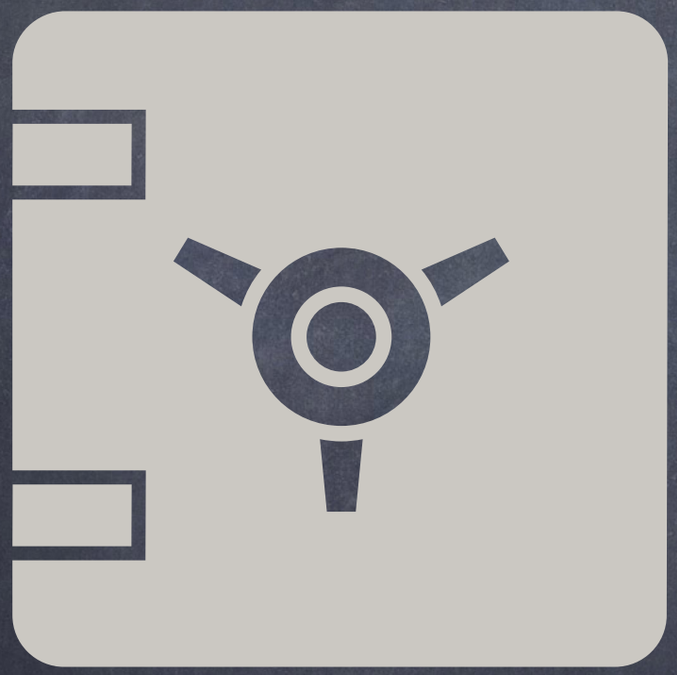
Error Conditions ->
Exceptional Behavior

Spec -> Normal
Deviation -> Error

Detect + Report + Handle

#176

DoS



Denial of Service
CIA -> Availability

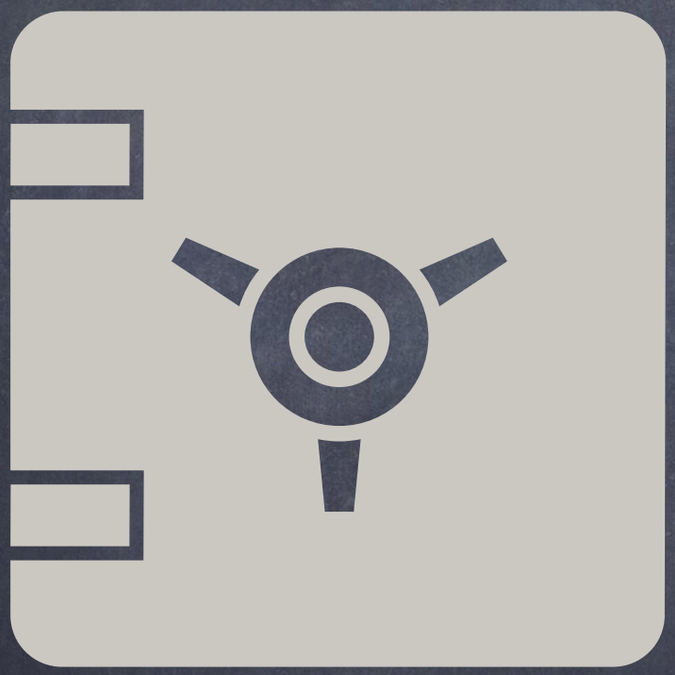
Users -> Access
Affect Shared State -> DoS

Effects: Lock Funds, Lose Profit, Tx Inclusion, Griefing

Recognize & Minimize DoS Attributes

#177

Timing



Timing Issues
Security Impact

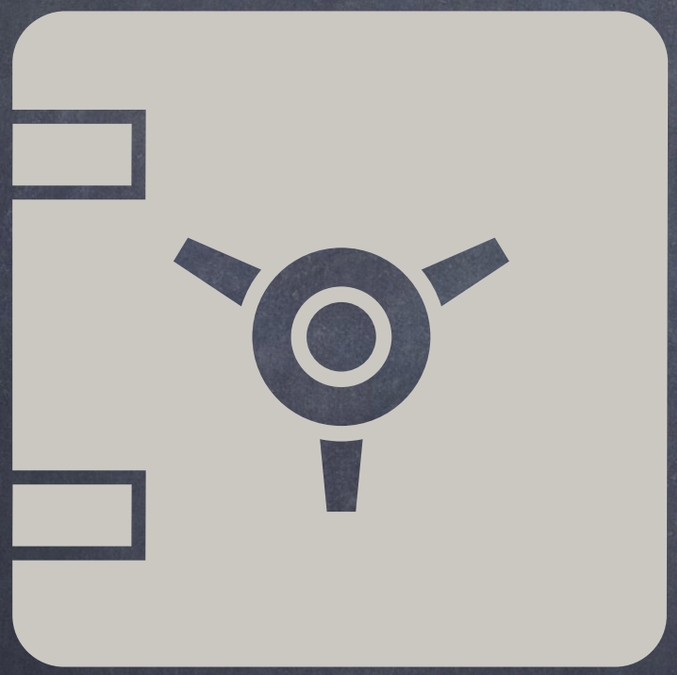
User/Contract/Blockchain
block.timestamp

Timing Assumptions
Functions -> Transitions

Actors -> Actions
Timing Attributes

#178

Ordering



Ordering Issues
Security Impact

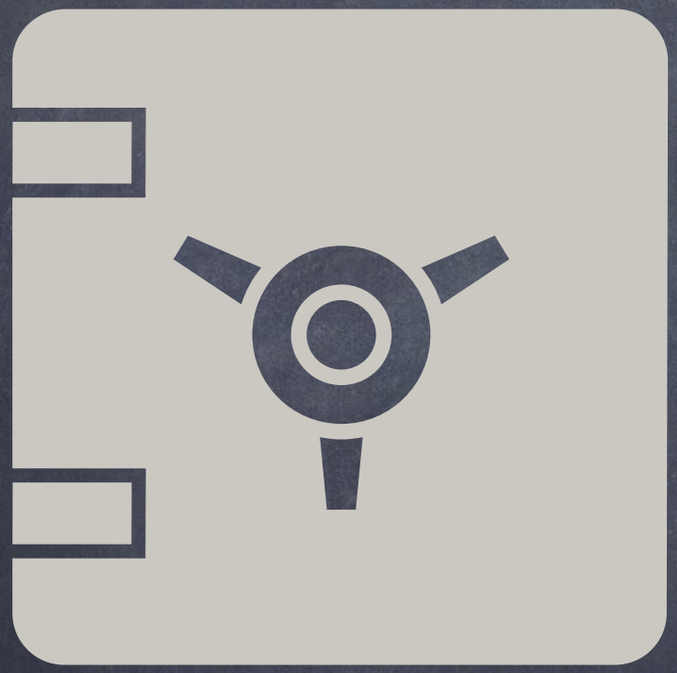
User Actions, State
Transitions, Transactions

Front/Back Running,
Sandwiching

Ordering <-> Timing
Ordering Attributes

#179

Undefined Behavior



Undefined + Malicious -> Security

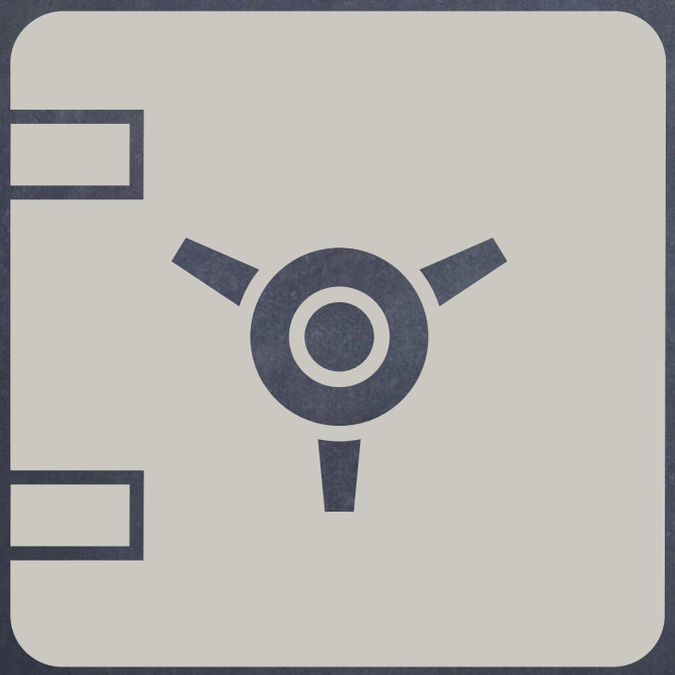
In Spec -> Defined
Not in Spec -> Undefined

Undefined Behavior
Revert/Exploit

Defined Behavior
Spec + Implement + Doc

#180

Interactions



External Interactions
Security Impact

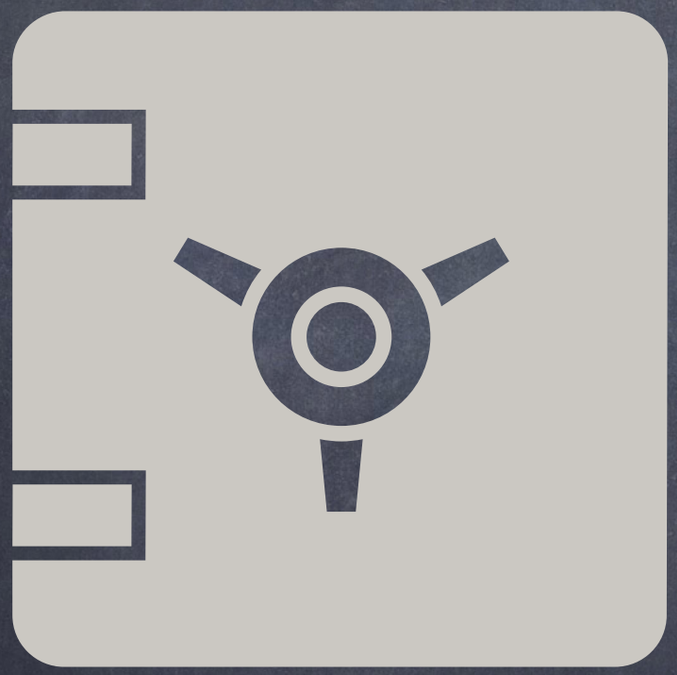
External Actors/Assets/Actions
Trust/Threat Model

Tokens/Contracts/Oracles
Correctness/Availability

External <-> Internal
Interactions -> Implications

#181

Trust



Trust Minimization

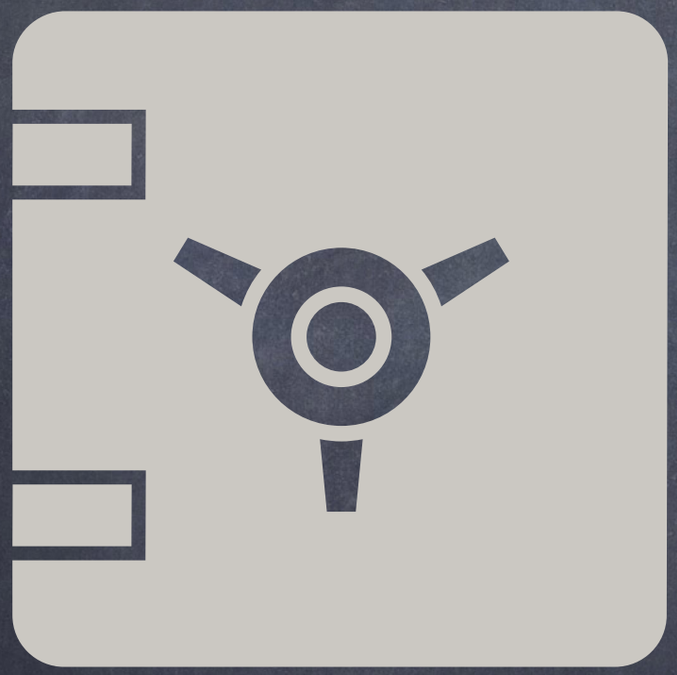
Foundational Value
Decentralization

Insider <-> Outsider
Use <-> Misuse

Never Trust, Always Verify

#182

Gas



Gas Issues
DoS -> Security

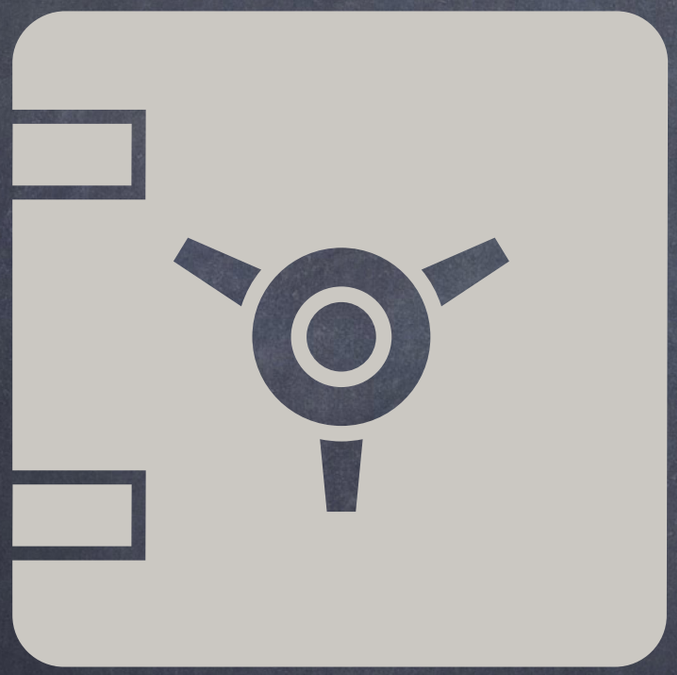
Turing Complete
Bound Computation

Loops, External Calls
OOG -> Lock/Fail

Gas Assumptions
Security Implications

#183

Dependency



Dependency Issues
External Factors

Imports, Contracts, Tokens,
Oracles, Relayers

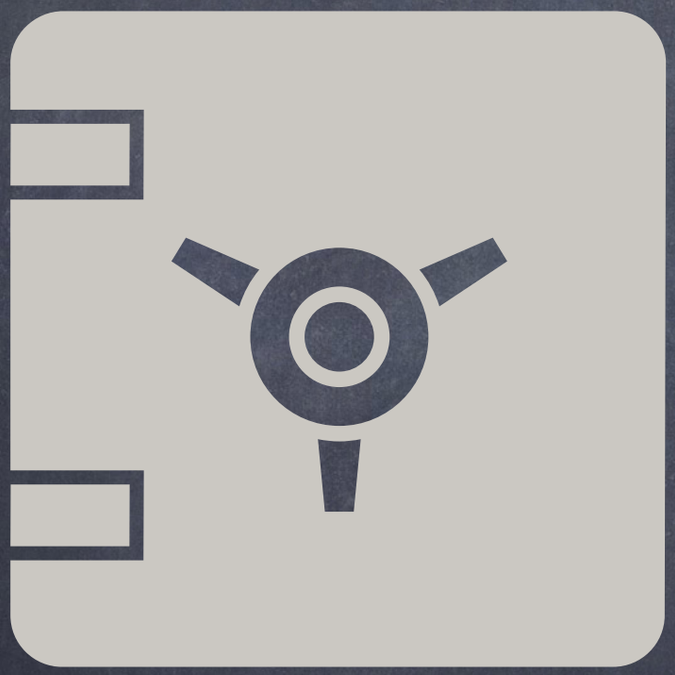
Trust, Correctness,
Availability

Dependencies
Security Implications

#184

Constant

Constancy Issues
Constant -> Wont Change



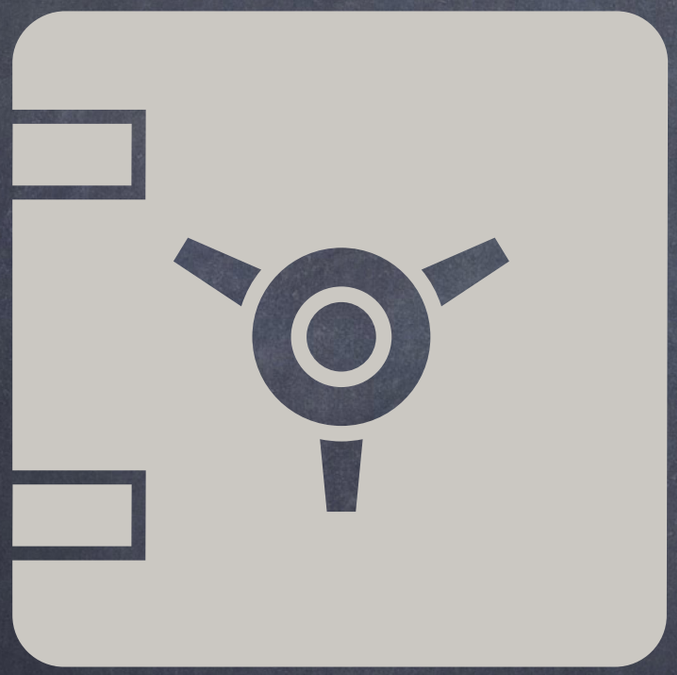
Hardcoded Parameters
Hardcoded Assumptions

E.g.: Block Time, Addresses, Permissions, Roles

Constant -> Change
Security Implications

#185

Fresh



Freshness Issues
Fresh -> Not Stale

Tx Nonce -> Replay
Oracle -> Price

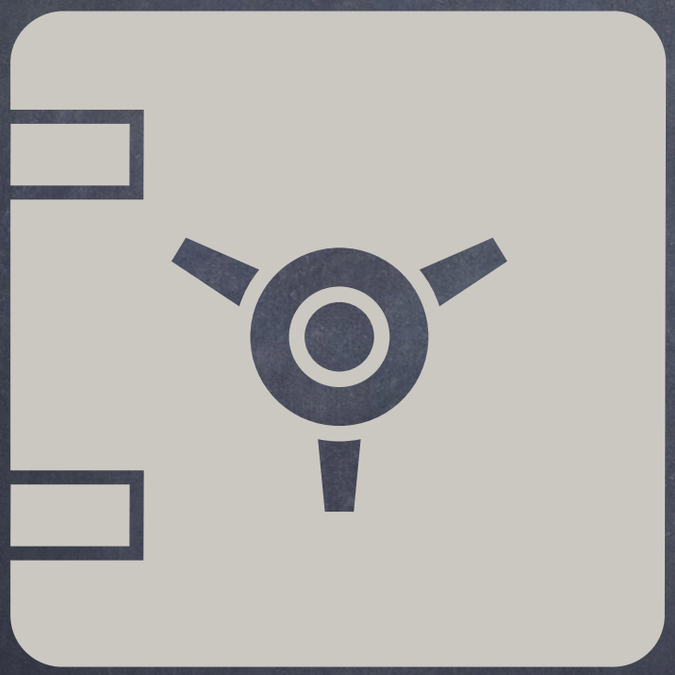
Lack of Timely Update
Lack of Availability

Fresh -> Stale
Security Implications

#186

Scarcity

Scarcity Issues
Less -> Secure?



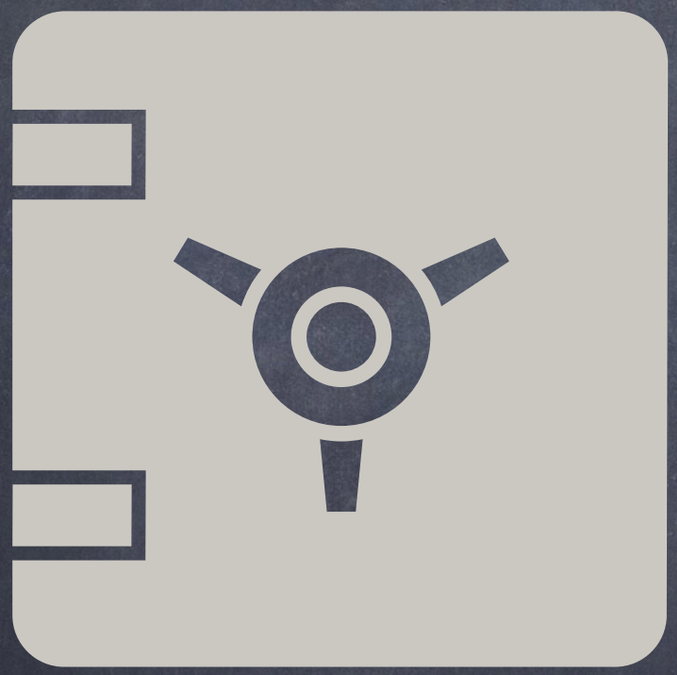
Assumptions
Funds/Tokens/Users

Flash Loans/Mints
Sybil Attacks

Scarcity -> Abundance
Security Implications

#187

Incentive



Incentive Issues
What? How Much?

Use <-> Abuse

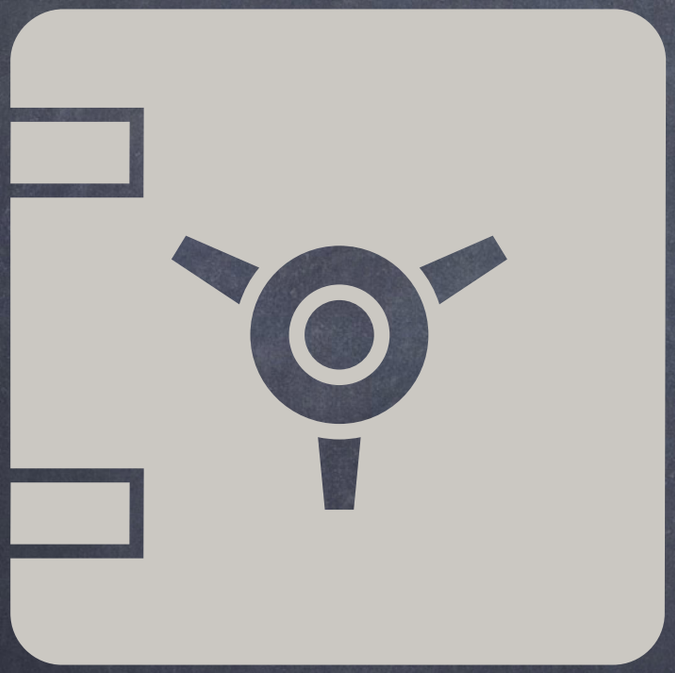
Liquidity/Liquidations
DoS, Griefing

Incentive -> Yes/No
Security Implications

#188

Clarity

Clarity Issues
Assets/Actors/Actions



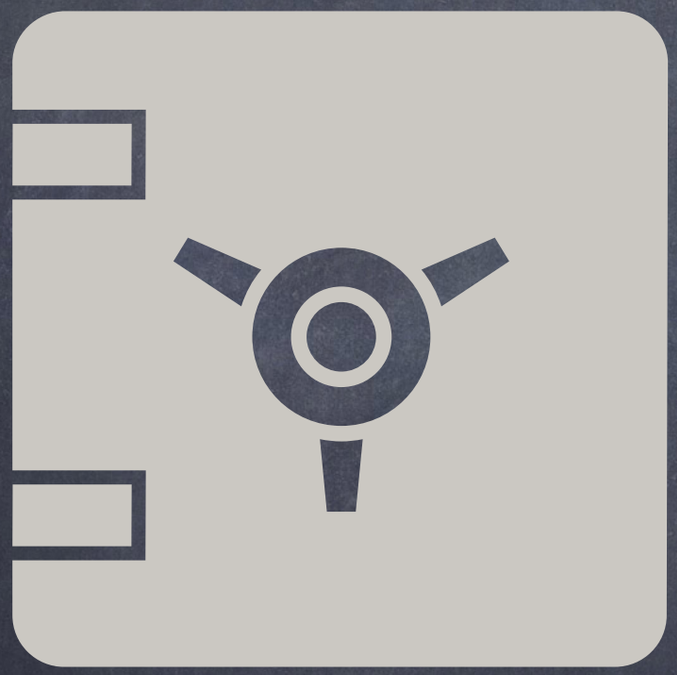
Spec, Implementation,
Documentation, UI/UX

Less Clarity
Assumptions -> Errors

Lack of Clarity
Security Implications

#189

Privacy



Privacy Issues
Assets/Actors/Actions

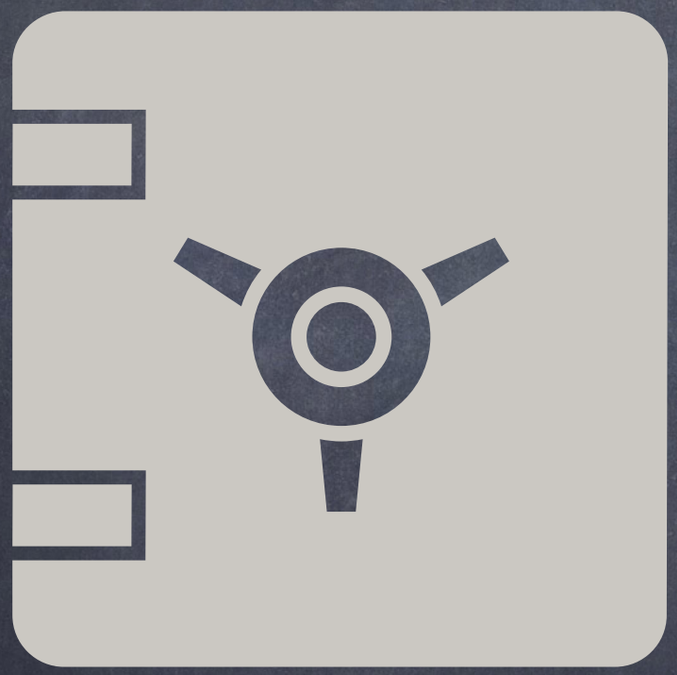
Transactions & Data
Blockchain

Mempool
On-chain Vs Off-chain

Privacy Assumptions
Security Implications

#190

Cloning



Cloning Issues
Copy Code

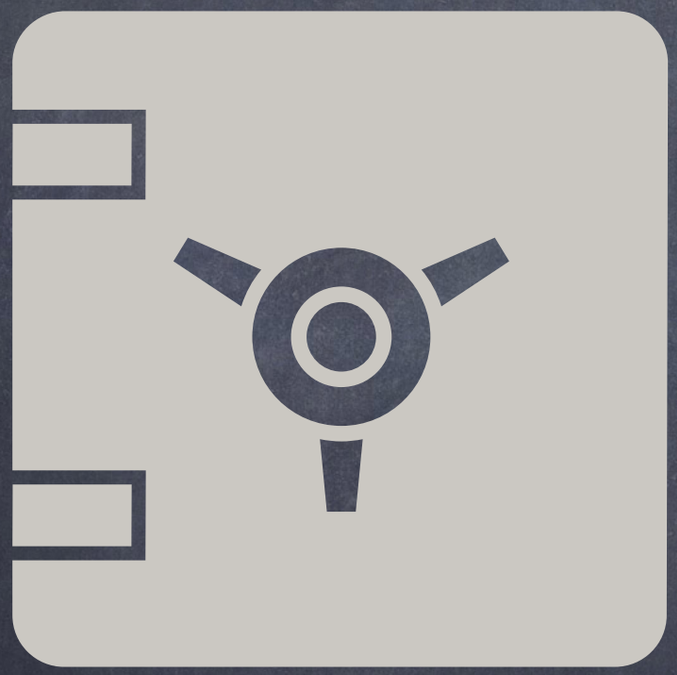
Libraries, Contracts,
Protocols

Context, Assumptions
Bugs, Fixes

Cloning Risks
Security Implications

#191

Logic



Business Logic
Application-specific

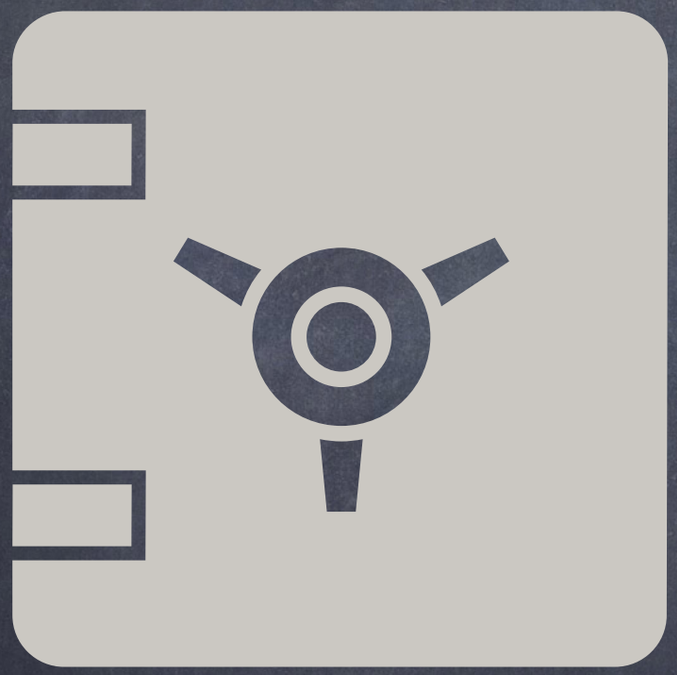
Reqs -> Spec
Assumptions -> Errors

Lack of Rules/Tools
Infer Constraints

High-Severity
Security Implications

#192

Principle #1



Least Privilege
Saltzer & Schroeder 1975

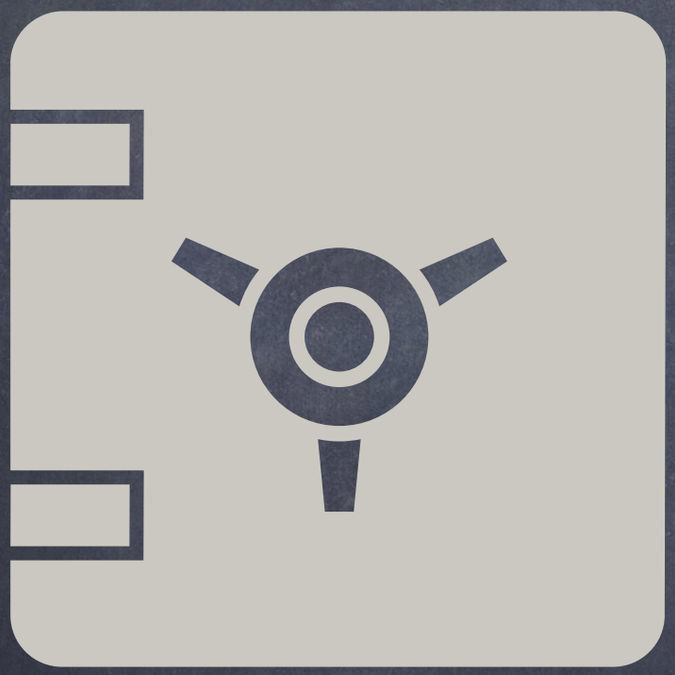
Privilege -> Job
Least Required

More Privilege
Abuse/Exploit

Privilege -> Need Based

#193

Principle #2



Separation of Privilege
Saltzer & Schroeder 1975

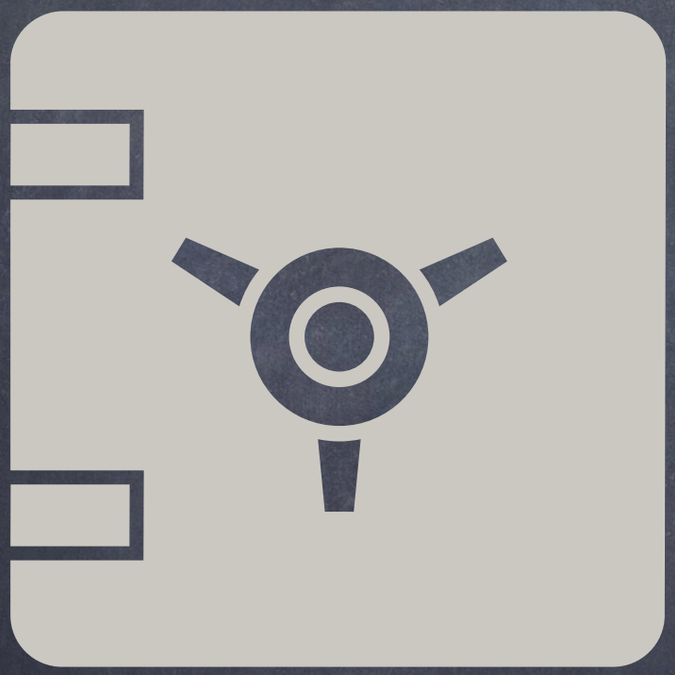
Privileges -> Separated
Multiple Actors

E.g.: Multi-Sigs vs EOA

Separation
No Single Point of Failure

#194

Principle #3



Least Common Mechanism
Saltzer & Schroeder 1975

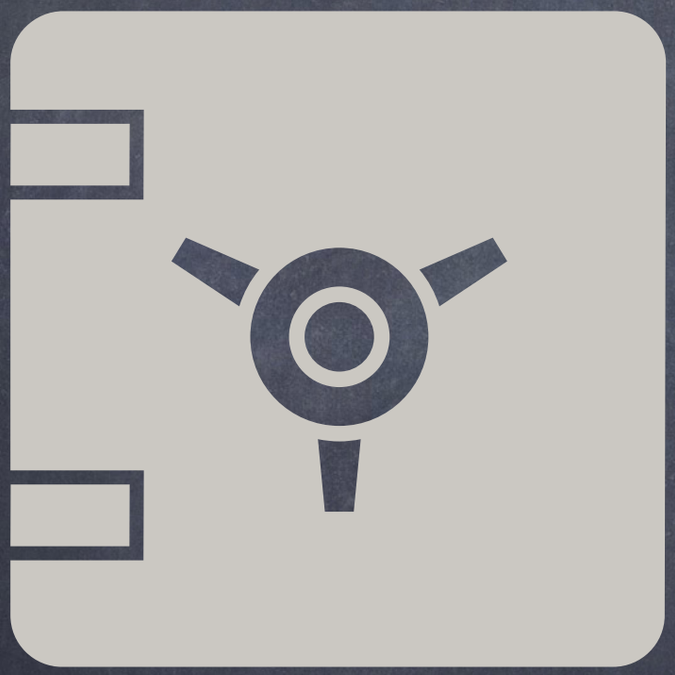
Minimize Sharing
Code, Roles

Common Points of Failure

Common -> Separate
Weigh Pros & Cons

#195

Principle #4



Fail-safe Defaults
Saltzer & Schroeder 1975

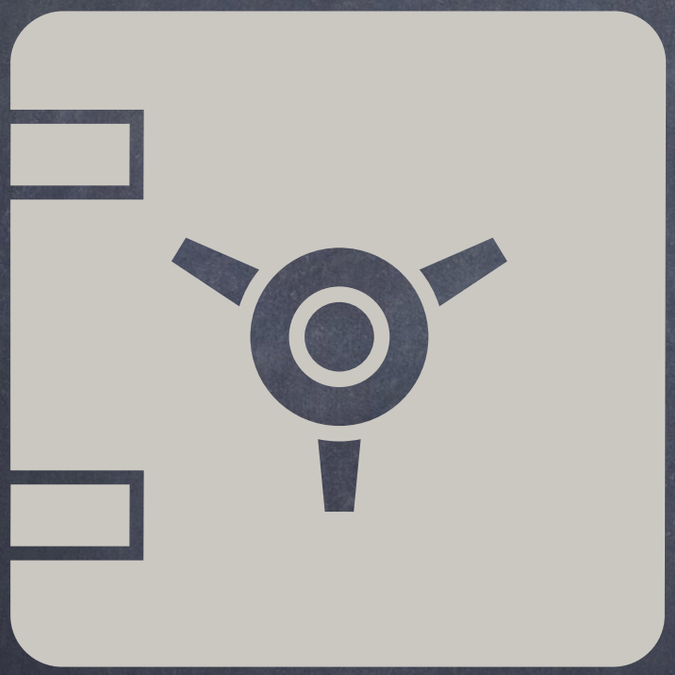
Permission Vs Exclusion
Guarded Launch

Defaults: Visibility,
Initializations, Permissions,
Assets/Actors/Actions

Open Vs Closed
Weigh Pros & Cons

#196

Principle #5



Complete Mediation
Saltzer & Schroeder 1975

Access Control
All Assets/Actors/Actions

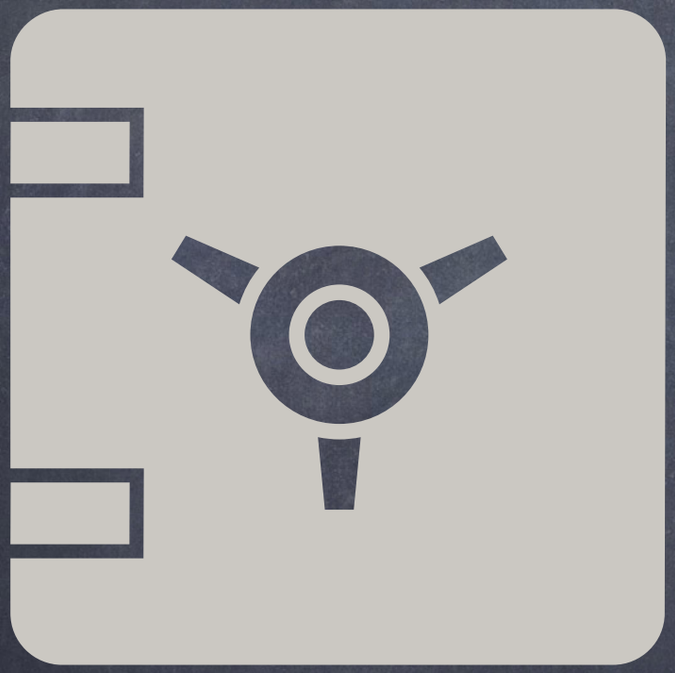
Missing Modifiers, Permissive Visibility, Missing Auth Flows

Mediation -> Every Thing/ One/Call

#197

Principle #6

Economy of Mechanism
Saltzer & Schroeder 1975



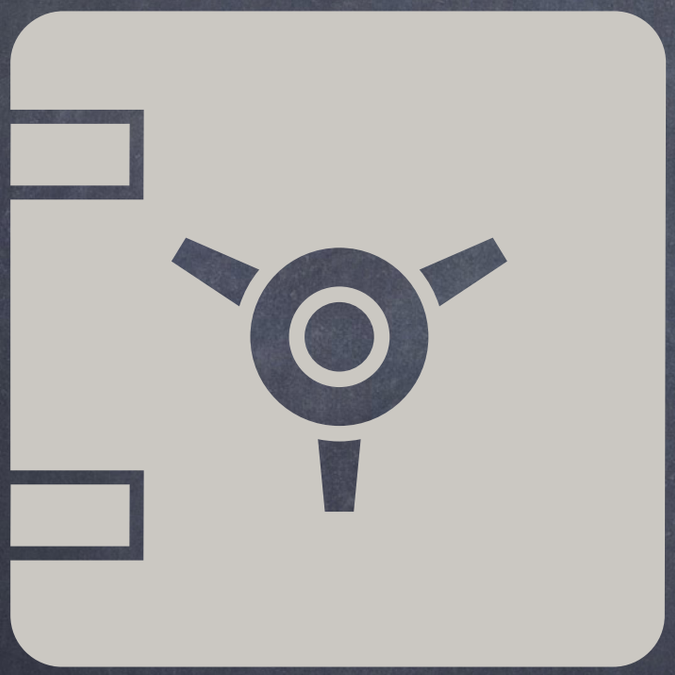
Design/Code: Simple/Small
Readability/Security

KISS Principle

More Complex -> Less Secure

#198

Principle #7



Open Design
Saltzer & Schroeder 1975

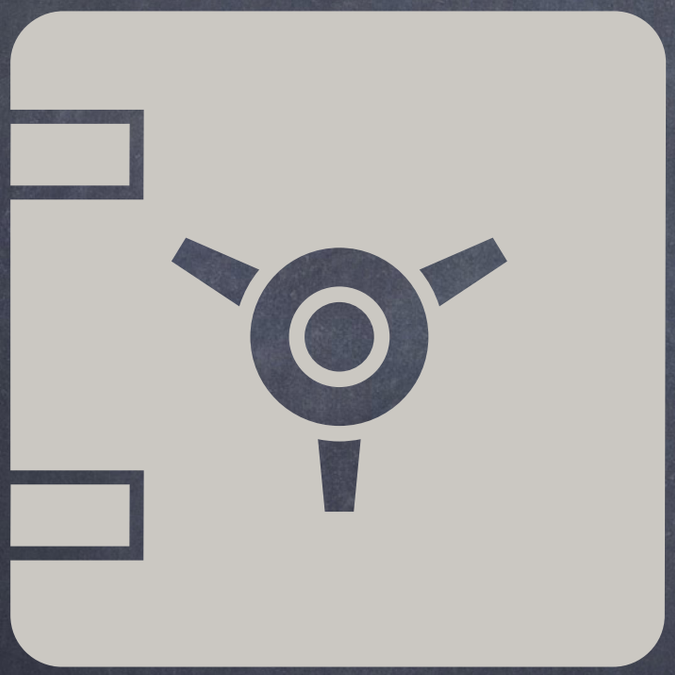
Open Design/Source
Permissionless Participation

Contract -> Open/Verified
Security -> Design/Code

No Security by Obscurity
Byzantine Threat Model

#199

Principle #8



Psychological Acceptability
Saltzer & Schroeder 1975

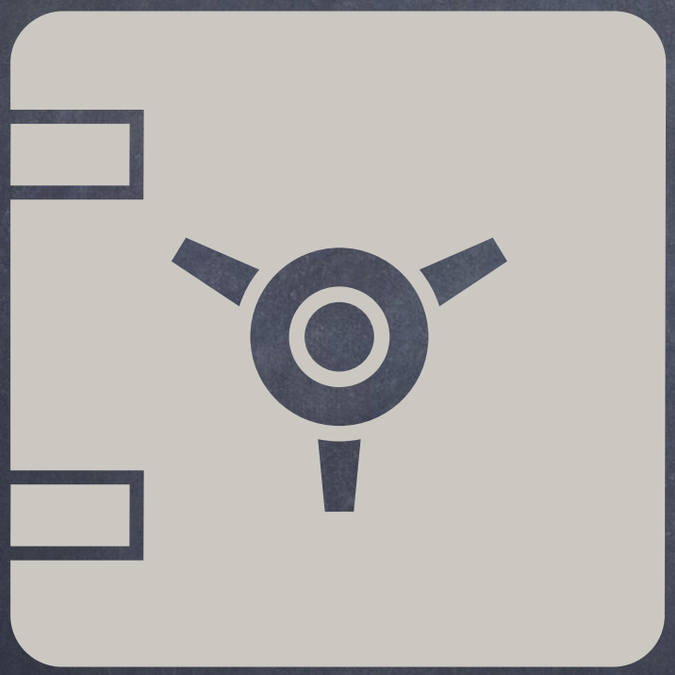
Human Interface
Ease of Use UI/UX

Humans -> Code/Use
Ease -> Apply Security

Design/Flow
More Intuitive & Less Risk

#200

Principle #9



Work Factor
Saltzer & Schroeder 1975

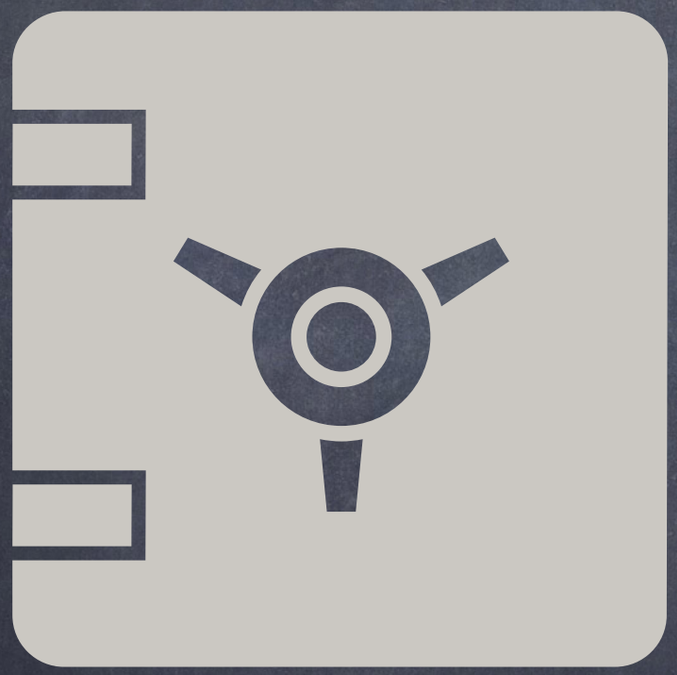
Cost of Circumventing
Benefit of Exploiting

Contracts -> M/Billions
Low Risk, High Reward

Maximum Incentives
Maximum Risks/Mitigations

#201

Principle #10



Compromise Recording
Saltzer & Schroeder 1975

Bug-Free Code?
Reduce Attack Surface

Residual Risk
Monitor & Detect & Fix

On-chain: Add Checks
Off-chain: Add Events