



**SOLID**Proof  
*Bring trust into your projects*

**Blockchain Security | Smart Contract Audits | KYC**

MADE IN GERMANY

# Audit

**Security Assessment**  
**05. December, 2021**

**For**



**NAKAMOTO**  
**.GAMES**

Disclaimer	3
Description	5
Project Engagement	5
Logo	5
Contract Link	5
Methodology	7
Used Code from other Frameworks/Smart Contracts (direct imports)	8
Tested Contract Files	9
Source Lines	10
Risk Level	10
Capabilities	11
Inheritance Graph	12
Verify Claims	13
Modifiers	18
CallGraph	20
Source Units in Scope	21
Critical issues	22
High issues	22
Medium issues	22
Low issues	22
Informational issues	22
Audit Comments	23
SWC Attacks	24

# Disclaimer

SolidProof.io reports are not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. These reports are not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team. SolidProof.io do not cover testing or auditing the integration with external contract or services (such as Unicrypt, Uniswap, PancakeSwap etc’...)

**SolidProof.io Audits do not provide any warranty or guarantee regarding the absolute bug- free nature of the technology analyzed, nor do they provide any indication of the technology proprietors. SolidProof Audits should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.**

SolidProof.io Reports represent an extensive auditing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology. Blockchain technology and cryptographic assets present a high level of ongoing risk. SolidProof’s position is that each company and individual are responsible for their own due diligence and continuous security. SolidProof in no way claims any guarantee of security or functionality of the technology we agree to analyze.

Version	Date	Description
1.0	05. December 2021	<ul style="list-style-type: none"><li>• Layout project</li><li>• Automated- /Manual-Security Testing</li><li>• Summary</li></ul>

## **Network**

Polygon

## **Website**

<https://nakamoto.games/>

## **Telegram**

<https://t.me/NakamotoGames>

## **Twitter**

<https://twitter.com/NakamotoGames>

## **Medium**

<https://medium.com/@nakamotogames>



## Description

Over **65% of the world has an internet connection**. 43% of Americans can't meet monthly living expenses. Developing countries fare far worse with many relying on remittances from overseas family members.

Play-to-earn gives anyone with an internet connection the opportunity to earn cryptocurrency and generate a sustainable source of income.

**Nakamoto Games** is building the premier **play-to-earn ecosystem** where players can earn in endless blockchain-based games and **developers can deploy games** to a broad user base.

## Project Engagement

During the 03rd of November 2021, **NAKA Team** engaged Solidproof.io to audit smart contracts that they created. The engagement was technical in nature and focused on identifying security flaws in the design and implementation of the contracts. They provided Solidproof.io with access to their code repository and whitepaper.

## Logo



NAKAMOTO  
.GAMES

## Contract Link

v1.0

• TBA

# Vulnerability & Risk Level

Risk represents the probability that a certain source-threat will exploit vulnerability, and the impact of that event on the organization or system. Risk Level is computed based on CVSS version 3.0.

Level	Value	Vulnerability	Risk (Required Action)
<b>Critical</b>	9 - 10	A vulnerability that can disrupt the contract functioning in a number of scenarios, or creates a risk that the contract may be broken.	Immediate action to reduce risk level.
<b>High</b>	7 – 8.9	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.	Implementation of corrective actions as soon as possible.
<b>Medium</b>	4 – 6.9	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.	Implementation of corrective actions in a certain period.
<b>Low</b>	2 – 3.9	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.	Implementation of certain corrective actions or accepting the risk.
<b>Informational</b>	0 – 1.9	A vulnerability that have informational character but is not effecting any of the code.	An observation that does not determine a level of risk

# Auditing Strategy and Techniques Applied

Throughout the review process, care was taken to evaluate the repository for security-related issues, code quality, and adherence to specification and best practices. To do so, reviewed line-by-line by our team of expert pentesters and smart contract developers, documenting any issues as there were discovered.

## **Methodology**

The auditing process follows a routine series of steps:

1. Code review that includes the following:
  - i) Review of the specifications, sources, and instructions provided to SolidProof to make sure we understand the size, scope, and functionality of the smart contract.
  - ii) Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
  - iii) Comparison to specification, which is the process of checking whether the code does what the specifications, sources, and instructions provided to SolidProof describe.
2. Testing and automated analysis that includes the following:
  - i) Test coverage analysis, which is the process of determining whether the test cases are actually covering the code and how much code is exercised when we run those test cases.
  - ii) Symbolic execution, which is analysing a program to determine what inputs causes each part of a program to execute.
3. Best practices review, which is a review of the smart contracts to improve efficiency, effectiveness, clarify, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.
4. Specific, itemized, actionable recommendations to help you take steps to secure your smart contracts.

## Used Code from other Frameworks/Smart Contracts (direct imports)

Imported packages:

### ItemVault

```
@openzeppelin/contracts/access/Ownable.sol
```

```
@openzeppelin/contracts/access/AccessControl.sol
```

### BalanceVault

```
@openzeppelin/contracts/token/ERC20/IERC20.sol
```

```
@openzeppelin/contracts/token/ERC20/utils/SafeERC20.sol
```

```
@openzeppelin/contracts/access/Ownable.sol
```

```
@openzeppelin/contracts/access/AccessControl.sol
```

```
@openzeppelin/contracts/security/ReentrancyGuard.sol
```



## Tested Contract Files

This audit covered the following files listed below with a SHA-1 Hash.

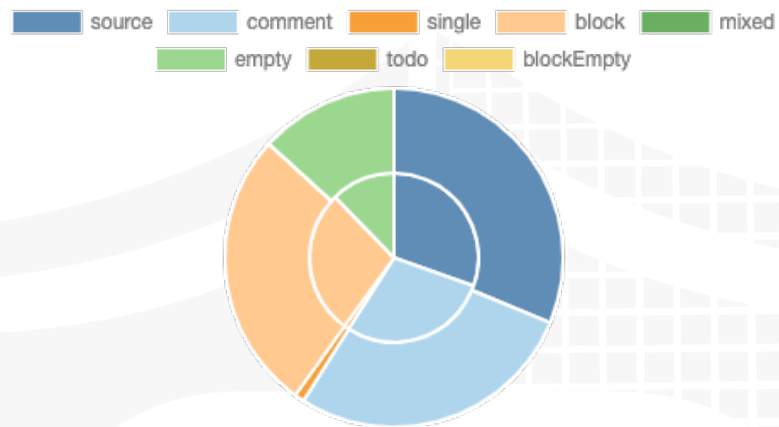
*A file with a different Hash has been modified, intentionally or otherwise, after the security review. A different Hash could be (but not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of this review.*

### v1.0

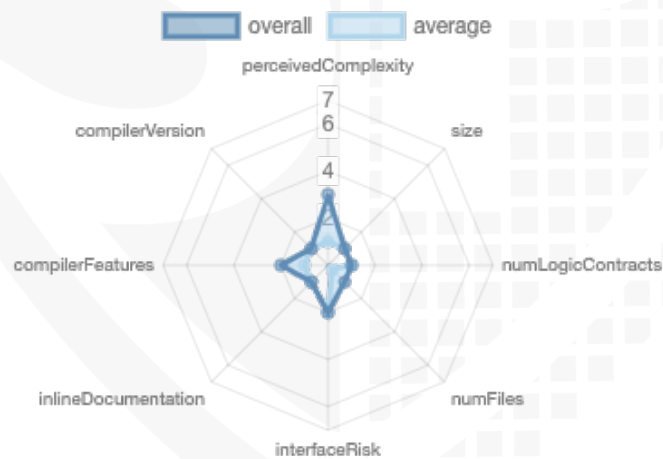
File Name	SHA-1 Hash
contracts/BalanceVault.sol	f7135449310f52ec29e3f994b1a1d0d79dcd9603
contracts/ItemVault.sol	a2dac908efb2aad6a1fb8c73a5c4c5947725a58e
contracts/utils/ItemVault.sol	f3ec8daacff53cfc430605f17d6540c73a55dec4
contracts/utils/IBalanceVault.sol	88a35ab692db14ff5bf4c28caac8f51d885f2368

# Metrics

## Source Lines v1.0



## Risk Level v1.0



## Capabilities

### Components

Version	Contracts	Libraries	Interfaces	Abstract
1.0	2	0	2	0

### Exposed Functions

*This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.*

Version	Public	Payable
1.0	20	0

Version	External	Internal	Private	Pure	View
1.0	20	20	0	0	4

### State Variables

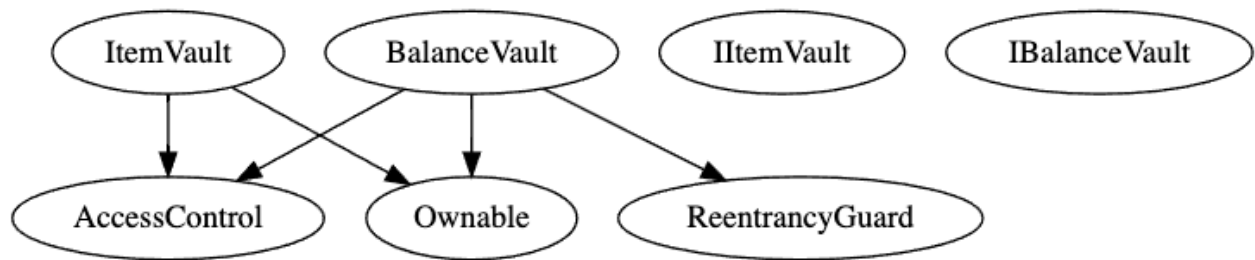
Version	Total	Public
1.0	7	4

### Capabilities

Version	Solidity Versions observed	Experimental Features	Can Receive Funds	Uses Assembly	Has Destroyable Contracts
1.0	^0.8.7			**** (0 asm blocks)	

Version	Transfers ETH	Low-Level Calls	Delegated Call	Uses Hash Functions	Ecrec over	New/ Create/ Create 2
1.0				yes		

## Inheritance Graph v1.0



## Verify Claims

### Write functions of contract

BalanceVault

decreaseBalance

depositNaka

grantRole

increaseBalance

pauseBalanceVault

renounceOwners...

renounceRole

revokeRole

transferOwnership

unpauseBalanceV...

withdrawNaka

ItemVault

decreaseItem

grantRole

increaseItem

pauseItemVault

renounceOwners...

renounceRole

revokeRole

transferOwnership

unpauseItemVault

## Deployer cannot mint any new tokens

Name	Exist	Tested	Verified
Deployer cannot mint	—	—	—



## Deployer cannot burn or lock user funds

Name	Exist	Tested	Verified
Deployer cannot lock	—	—	—
Deployer cannot burn	—	—	—



## Deployer cannot pause the contract

Name	Exist	Tested	Verified
Deployer cannot pause	✓	✓	✗

Comments:

**v1.0**

- Only Owner can pause ItemVault and BalanceVault





## Overall checkup (Smart Contract Security)

Tested	Verified
✓	✓

### Legend

Attribute	Symbol
Verified / Checked	✓
Partly Verified	⚠
Unverified / Not checked	✗
Not available	—

## Modifiers

### BalanceVault

```
depositNaka  
withdrawNaka  
increaseBalance  
decreaseBalance  
pauseBalanceVault  
unpauseBalanceVault
```

### ItemVault

```
increaseItem  
decreaseItem  
pauseItemVault  
unpauseItemVault
```

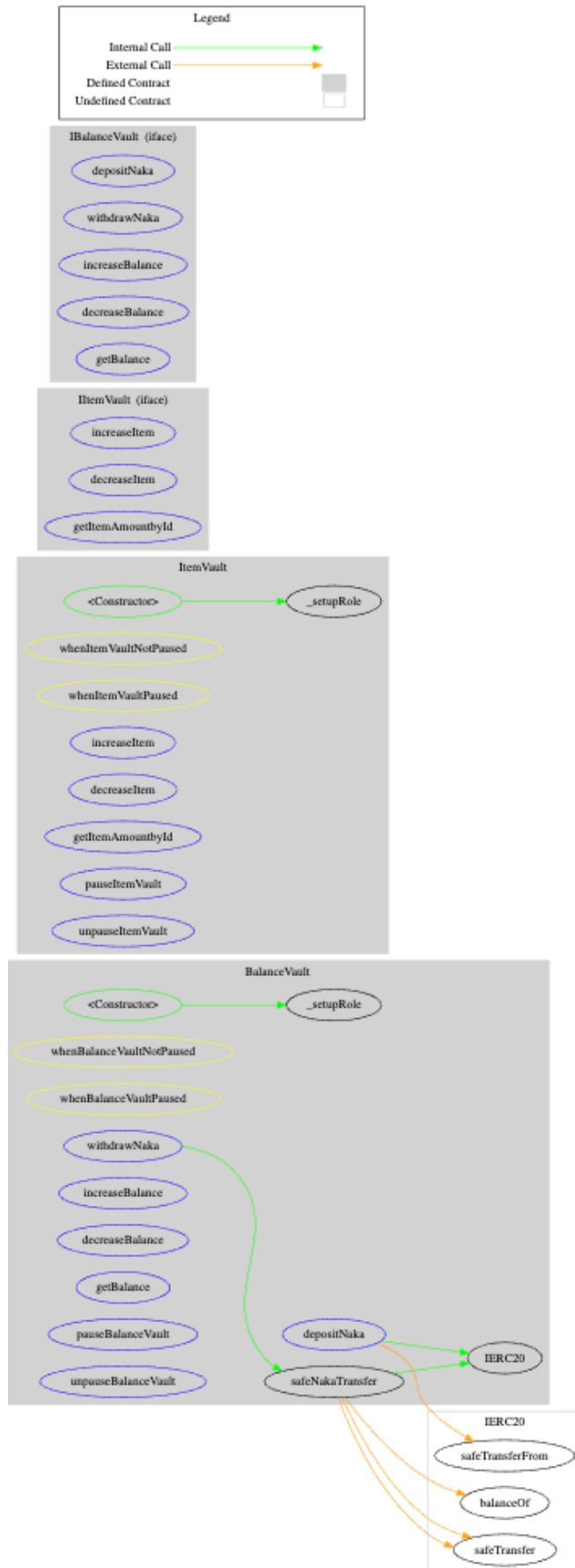
## Comments

- BalanceVault
  - depositNaka
    - whenBalanceVaultNotPaused
  - withdrawNaka
    - whenBalanceVaultNotPaused
    - nonReentrant
  - increaseBalance
    - whenBalanceVaultNotPaused
    - onlyRole
      - VAULT\_ADMIN
  - decreaseBalance
    - whenBalanceVaultNotPaused
    - onlyRole
      - VAULT\_ADMIN
  - pauseBalanceVault
    - onlyOwner
    - whenBalanceVaultNotPaused
  - unpauseBalanceVault
    - onlyOwner
    - whenBalanceVaultPaused
- ItemVault
  - increaseItem

- whenItemVaultNotPaused
  - onlyRole
    - VAULT\_ADMIN
- decreaseItem
  - whenItemVaultNotPaused
  - onlyRole
    - VAULT\_ADMIN
- pauseItemVault
  - whenItemVaultNotPaused
  - onlyOwner
- unpausesItemVault
  - onlyOwner
  - whenItemVaultPaused












# CallGraph



# Source Units in Scope

## v1.0

Type	File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score	Capabilities
	contracts/BalanceVault.sol	1	————	168	168	74	69	59	
	contracts/ItemVault.sol	1	————	111	111	44	46	36	
	contracts/utis/ItemVault.sol	————	1	11	6	3	1	7	————
	contracts/utis/IBalanceVault.sol	————	1	15	6	3	1	11	————
 	<b>Totals</b>	<b>2</b>	<b>2</b>	<b>305</b>	<b>291</b>	<b>124</b>	<b>117</b>	<b>113</b>	

## Legend

Attribute	Description
Lines	total lines of the source unit
nLines	normalized lines of the source unit (e.g. normalizes functions spanning multiple lines)
nSLOC	normalized source lines of code (only source-code lines; no comments, no blank lines)
Comment Lines	lines containing single or block comments
Complexity Score	a custom complexity score derived from code statements that are known to introduce code complexity (branches, loops, calls, external interfaces, ...)

# Audit Results

# AUDIT PASSED

## Critical issues

- no critical issues found -

## High issues

- no high issues found -

## Medium issues

Issue	File	Type	Line	Description
#1	Balance Vault	Reentrancy vulnerabilities	77	Apply the [ `check-effects-interactions pattern` ]( <a href="http://solidity.readthedocs.io/en/v0.4.21/security-considerations.html#re-entrancy">http://solidity.readthedocs.io/en/v0.4.21/security-considerations.html#re-entrancy</a> ).or nonReentrant modifier from OpenZeppelin

## Low issues

Issue	File	Type	Line	Description
#1	Balance Vault	A floating pragma is set	3	The current pragma Solidity directive is „^0.8.7“.
#2	ItemVault	A floating pragma is set	3	The current pragma Solidity directive is „^0.8.7“.
#3	Balance Vault	Missing Zero Address Validation (missing-zero-check)	49	Check that the address is not zero
#4	Balance Vault	State variable visibility is not set	23	It is best practice to set the visibility of state variables explicitly

## Informational issues

Issue	File	Type	Line	Description
-------	------	------	------	-------------

#1	Balance Vault	Missing inheritance	-	Inherit from the missing interface or contract
#2	ItemVault	Missing inheritance	-	Inherit from the missing interface or contract
#3	Balance Vault	Wrong comment	85-90	Modify comment for withdrawNaka function

## Audit Comments

**05. December 2021:**

[Read report for more information](#)



## SWC Attacks

ID	Title	Relationships	Status
<a href="#">SW C-13 6</a>	Unencrypted Private Data On-Chain	<a href="#">CWE-767: Access to Critical Private Variable via Public Method</a>	PASSED
<a href="#">SW C-13 5</a>	Code With No Effects	<a href="#">CWE-1164: Irrelevant Code</a>	PASSED
<a href="#">SW C-13 4</a>	Message call with hardcoded gas amount	<a href="#">CWE-655: Improper Initialization</a>	PASSED
<a href="#">SW C-13 3</a>	Hash Collisions With Multiple Variable Length Arguments	<a href="#">CWE-294: Authentication Bypass by Capture-replay</a>	PASSED
<a href="#">SW C-13 2</a>	Unexpected Ether balance	<a href="#">CWE-667: Improper Locking</a>	PASSED
<a href="#">SW C-13 1</a>	Presence of unused variables	<a href="#">CWE-1164: Irrelevant Code</a>	PASSED
<a href="#">SW C-13 0</a>	Right-To-Left-Override control character (U+202E)	<a href="#">CWE-451: User Interface (UI) Misrepresentation of Critical Information</a>	PASSED
<a href="#">SW C-12 9</a>	Typographical Error	<a href="#">CWE-480: Use of Incorrect Operator</a>	PASSED
<a href="#">SW C-12 8</a>	DoS With Block Gas Limit	<a href="#">CWE-400: Uncontrolled Resource Consumption</a>	PASSED



<a href="#">SW C-12 7</a>	Arbitrary Jump with Function Type Variable	<a href="#">CWE-695: Use of Low-Level Functionality</a>	<b>PASSED</b>
<a href="#">SW C-12 5</a>	Incorrect Inheritance Order	<a href="#">CWE-696: Incorrect Behavior Order</a>	<b>PASSED</b>
<a href="#">SW C-12 4</a>	Write to Arbitrary Storage Location	<a href="#">CWE-123: Write-what-where Condition</a>	<b>PASSED</b>
<a href="#">SW C-12 3</a>	Requirement Violation	<a href="#">CWE-573: Improper Following of Specification by Caller</a>	<b>PASSED</b>
<a href="#">SW C-12 2</a>	Lack of Proper Signature Verification	<a href="#">CWE-345: Insufficient Verification of Data Authenticity</a>	<b>PASSED</b>
<a href="#">SW C-12 1</a>	Missing Protection against Signature Replay Attacks	<a href="#">CWE-347: Improper Verification of Cryptographic Signature</a>	<b>PASSED</b>
<a href="#">SW C-12 0</a>	Weak Sources of Randomness from Chain Attributes	<a href="#">CWE-330: Use of Insufficiently Random Values</a>	<b>PASSED</b>
<a href="#">SW C-11 9</a>	Shadowing State Variables	<a href="#">CWE-710: Improper Adherence to Coding Standards</a>	<b>PASSED</b>
<a href="#">SW C-11 8</a>	Incorrect Constructor Name	<a href="#">CWE-665: Improper Initialization</a>	<b>PASSED</b>
<a href="#">SW C-11 7</a>	Signature Malleability	<a href="#">CWE-347: Improper Verification of Cryptographic Signature</a>	<b>PASSED</b>

<a href="#">SW C-11 6</a>	Timestamp Dependence	<a href="#">CWE-829: Inclusion of Functionality from Untrusted Control Sphere</a>	PASSED
<a href="#">SW C-11 5</a>	Authorization through tx.origin	<a href="#">CWE-477: Use of Obsolete Function</a>	PASSED
<a href="#">SW C-11 4</a>	Transaction Order Dependence	<a href="#">CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')</a>	PASSED
<a href="#">SW C-11 3</a>	DoS with Failed Call	<a href="#">CWE-703: Improper Check or Handling of Exceptional Conditions</a>	PASSED
<a href="#">SW C-11 2</a>	Delegatecall to Untrusted Callee	<a href="#">CWE-829: Inclusion of Functionality from Untrusted Control Sphere</a>	PASSED
<a href="#">SW C-111</a>	Use of Deprecated Solidity Functions	<a href="#">CWE-477: Use of Obsolete Function</a>	PASSED
<a href="#">SW C-11 0</a>	Assert Violation	<a href="#">CWE-670: Always-Incorrect Control Flow Implementation</a>	PASSED
<a href="#">SW C-10 9</a>	Uninitialized Storage Pointer	<a href="#">CWE-824: Access of Uninitialized Pointer</a>	PASSED
<a href="#">SW C-10 8</a>	State Variable Default Visibility	<a href="#">CWE-710: Improper Adherence to Coding Standards</a>	NOT PASSED
<a href="#">SW C-10 7</a>	Reentrancy	<a href="#">CWE-841: Improper Enforcement of Behavioral Workflow</a>	NOT PASSED
<a href="#">SW C-10 6</a>	Unprotected SELFDESTRUCT Instruction	<a href="#">CWE-284: Improper Access Control</a>	PASSED

<a href="#">SW C-10 5</a>	Unprotected Ether Withdrawal	<a href="#">CWE-284: Improper Access Control</a>	PASSED
<a href="#">SW C-10 4</a>	Unchecked Call Return Value	<a href="#">CWE-252: Unchecked Return Value</a>	PASSED
<a href="#">SW C-10 3</a>	Floating Pragma	<a href="#">CWE-664: Improper Control of a Resource Through its Lifetime</a>	NOT PASSED
<a href="#">SW C-10 2</a>	Outdated Compiler Version	<a href="#">CWE-937: Using Components with Known Vulnerabilities</a>	PASSED
<a href="#">SW C-10 1</a>	Integer Overflow and Underflow	<a href="#">CWE-682: Incorrect Calculation</a>	PASSED
<a href="#">SW C-10 0</a>	Function Default Visibility	<a href="#">CWE-710: Improper Adherence to Coding Standards</a>	PASSED

The logo features the word "SolidProof" in a white, elegant script font. The "P" is particularly large and stylized, with a long horizontal stroke that extends to the left. The background is a solid blue color with a faint, large shield emblem. The shield has a grid-like pattern on its right side and a solid blue area on its left side.

SolidProof

**Blockchain Security | Smart Contract Audits | KYC**

A small horizontal bar representing the German flag, with black, red, and gold stripes.

MADE IN GERMANY