

SOLIDProof

Bring trust into your projects

Blockchain Security | Smart Contract Audits | KYC Development | Marketing

MADE IN GERMANY



Table of Contents

Security Audit Agreement....3
Whereas....3
1. Scope of Services....4
1.1 Audit target and commit freeze....4
1.2 Review depth....5
2. Audit Procedure and Deliverables....6
2.1 Activities....6
2.2 Deliverables....6
2.3 Remediation advisory....7
2.4 Re-audit after remediation....7
3. Timeline....9
4. Fees and Payment....10
4.1 Rate....10
4.2 Contracted scope and fee....10
4.3 Payment schedule and settlement....10
4.4 Change orders....11
5. Client Obligations....12
6. Coordinated Disclosure and Live-Chain Handling....12
7. Limitation of Liability....13
8. Intellectual Property....14
9. Confidentiality and Non-Disclosure....14
10. Dispute Resolution....15
11. Termination....15
12. Governing Law and Jurisdiction....16
13. Compliance with Data Protection Regulations....16
14. Contracting Entity and Acceptance....16
15. Entire Agreement and Amendments....17
Appendix A....18
Audit Scope and Methodology....18
1. Core Focus Areas....18
2. Audit Methodology....20
3. Vulnerability Classes Targeted....21
4. Tools and Resources....22
5. Explicit Exclusions....22
6. Audit Goals....22
Appendix B....23
Components in Scope....23
1. In scope, with review depth....23
2. Reviewed for adequacy rather than line by line....25
3. Out of scope....25
4. Audit target summary at the frozen commit....25
5. Framework versions at the frozen commit....25

28.10.2026

Security Audit Agreement

This Security Audit Agreement ("Agreement") is made and entered into by and between:

FutureVisions Deutschland UG (haftungsbeschränkt)
Europastraße 81, 24976 Handewitt, Germany
(Hereinafter referred to as "Auditor")

AND

Terra Classic, represented by Terra Classic Core, a coalition of Bumeo Capital and LunaClassicDAO,acting through the authorised representatives identified on acceptance in accordance with §14 (Hereinafter referred to as "Client")

Whereas

The Auditor provides IT security audits, including the review of Layer 1 protocol code and smart contracts related to blockchain technologies.

The Client desires to engage the Auditor to perform a security audit on its Cosmos-based Layer 1 blockchain ("Audit").

The Client completed the "SDK53" upgrade in April 2026, which moved the chain across three major framework boundaries: Cosmos SDK 0.47 to 0.53, ibc-go v7 to v10, and from the private `classic-terra/wasmd` fork to upstream wasmd 0.61. The resulting code is live on mainnet and has not been independently audited. The Client is additionally preparing the Market Module 2.0 re-implementation, a new USTC staking module and the `v15` network upgrade on the `ustc_staking` branch, which are to be reviewed before deployment as part of this engagement. This Agreement supersedes the draft agreement dated 07.06.2025, which was scoped and priced against the pre-upgrade codebase.

This Agreement contracts the full scope of the Auditor's offer dated 15.09.2026, together with the Market Module 2.0, USTC staking and `v15` additions frozen under §1.1. It comprises the core protocol audit, the framework migration and state integrity review, the adversarial simulation and economic review, the review of the Market Module 2.0, the new `x/ustcstaking` module and the `v15` upgrade, and a full re-audit after remediation, at a total contracted effort of 568 engineer-hours and a fixed fee of USD 85,200.

The parties acknowledge that the Client funds this engagement through on-chain governance under the Terra Classic Pay Per Job process. A single governance text proposal first approves this one job — the Audit — and the two-step payment structure; that text vote moves no funds. The fee is then paid in two parts, each through its own community-pool spend proposal as defined in Appendix E and §4.3: forty per cent (40%) upfront, paid before the Auditor starts work, and sixty per cent (60%) on delivery of the audit findings. The full re-audit under §2.4 is included within the sixty-per-cent part and is not separately charged. Remediation of the findings is performed by the Client's own developers at no cost to the community pool and is not part of the Auditor's fee or obligations. This payment structure does not reduce the contracted scope: the full 568 engineer-hours and the full USD 85,200 fee remain contracted.

Now, Therefore, the parties hereby agree as follows:

1. Scope of Services

The Auditor shall perform a security audit that includes the following:

- Examination of the source code for the Terra Classic protocol, with particular focus on the eight custom modules, the thirteen Cosmos SDK module overrides, the transaction processing and fee handling chain, the application and IBC wiring, and the CosmWasm integration.
- Examination of the framework migration surface introduced by the SDK53 upgrade, including all twenty upgrade handlers and the hand-written migration of the CosmWasm key-value store that executed on mainnet at block height 25,619,230.
- Security assessment of the economic mechanisms as implemented: oracle vote aggregation, tally and reward distribution; treasury seigniorage and policy; burn tax collection, splitting and exemption; and dynamic validator commission enforcement.
- Examination of the pre-deployment additions on the `ustc_staking` branch frozen under §1.1: the Market Module 2.0 re-implementation and its re-activated swap economics; the new `x/ustcstaking` module and its staking and reward logic; the tax-redirect mechanism and market accumulator account in the fee and burn-tax path; the oracle TWAP and freshness hooks; and the `v15` upgrade handler.
- Adversarial simulation of the protocol under fuzz, localnet and interchain conditions, including oracle manipulation, burn tax bypass, treasury drain and denial of service scenarios.
- Identification of security vulnerabilities across the components in scope, with severity classification per Appendix C and concrete remediation guidance.
- A full re-audit of the remediated code after the Client's remediation window, with verification of each reported finding and an updated, publishable Final Audit Report.
- Adherence to the scope and methodology set out in Appendix A and Appendix B.

All focus areas and methodology sections listed in Appendix A are within the contracted scope. The scope is contracted in full; the two-step payment structure under Appendix E and §4.3 governs only when the fee is paid, and does not carve any focus area or methodology section out of scope.

1.1 Audit target and commit freeze

The Audit is performed against a single frozen commit of the repository at https://github.com/classic-terra/core:

```
Branch:      ustc_staking
Commit:      35d68fe1b3eb811c27e8bf3f398d5cc197897229
Date:        2026-10-15
Base:        f54cdec2ed8aa04a83d904fe21d5d2a63d35ff93 (v4.0.1-patch.3, live on
mainnet) plus 52 commits
```

The frozen commit is the tip of the `ustc_staking` branch, which extends the live mainnet code at `f54cdec` (tag `v4.0.1-patch.3`) with the Market Module 2.0 re-implementation (pull request #664), the new `x/ustcstaking` module, the `v15` upgrade handler and the tax-redirect mechanism in the fee and burn-tax path. The already-deployed core chain at `f54cdec` is live on mainnet; the additions on the `ustc_staking` branch are pre-deployment code that has not yet been merged to `main` or released. The audit target is the whole codebase at the frozen commit — the core chain

together with those additions. Development on the branch may continue during the engagement; changes landing after the freeze are not in scope, save for the remediation changes verified under §2.4, and re-basing onto a later commit constitutes a change order under §4.4.

At the frozen commit the audit target comprises 30,329 raw lines of non-test, non-generated Go source, equal to 23,203 nSLOC excluding blank and comment lines. Generated protobuf bindings (50,697 lines) are excluded; the 31 underlying `.proto` definitions are in scope.

1.2 Review depth

The Auditor allocates review depth by risk rather than uniformly across the codebase. Three levels apply, defined in Appendix A §2.B and mapped path by path in Appendix B §1:

- Level D1, deep review, covers approximately 68% of the audit target: all code that moves funds or can break consensus, including the new `x/ustcstaking` module and the Market Module 2.0 code.
- Level D2, targeted review, covers approximately 23%: entry points, state transitions and authorisation boundaries read in full, internal helpers read selectively.
- Level D3, tooling sweep with spot checks, covers approximately 6%: thin SDK module wrappers, CLI packages, shared utilities and configuration.

This allocation is a material term of the Agreement. The Client acknowledges that a defect confined to a D3 path may not be detected. The depth map is reproduced in the final Audit Report so that readers of the published report can assess coverage directly. The parties may reallocate depth by mutual written agreement during the engagement provided total effort remains within the 568 contracted hours under §4.2 and the two payment amounts in §4.3 are not changed.

2. Audit Procedure and Deliverables

The Auditor will conduct the Audit using industry-standard security testing methodologies and tools as detailed in Appendix A. The Audit is manual-review-led; automated analysis serves as a coverage net rather than as the primary method.

2.1 Activities

Architecture and Threat Model: Construction of the module dependency and keeper graph, store key inventory, privilege and authorisation map, and an explicit threat model recording assets, adversaries and attack surfaces. Issued to the Client early in the engagement so that the Auditor's assumptions can be challenged before the bulk of the review is performed.

Code Review: Review of the protocol code at the depth assigned under §1.2 to identify security vulnerabilities including custom module logic flaws, Cosmos SDK and ibc-go integration defects, non-determinism and state divergence hazards, incorrect fee and tax arithmetic, missing authorisation on message handlers, state migration defects, and unmetered execution paths.

Migration Verification: Differential replay of the CosmWasm store migration functions against mainnet-derived key material, determinism analysis of the legacy store compatibility shim, and review of all twenty upgrade handlers against the declared store upgrades.

Risk Assessment: Evaluation of the impact and exploitability of each identified issue on the security, liveness and economic integrity of the Terra Classic protocol, classified per Appendix C.

Testing and Adversarial Simulation: Dynamic testing techniques to assess protocol behaviour under adversarial conditions, including property-based and fuzz testing of oracle tally, tax computation, commission enforcement and migration key handling; localnet and interchain scenarios for IBC, mempool and governance behaviour; multi-validator misbehaviour scenarios; and the economic attack scenarios set out in Appendix A §1.H.

Reporting: Preparation of a detailed Audit Report including findings, threat analysis and remediation recommendations. The Auditor shall prepare a draft Audit Report for the Client's review, where the Client may provide comments and request factual amendments as necessary.

Remediation Verification: A full re-audit of the Client's remediation, per §2.4, feeding into the Final Audit Report.

2.2 Deliverables

Upon and during completion of the Audit, the Auditor will provide the Client with:

- Threat Model and Architecture Note: trust boundaries, privilege map, store inventory and prioritised attack surface, issued early for Client challenge.
- Interim Findings Report: all Critical and High severity findings identified to date, issued mid-engagement rather than withheld until completion.
- Audit Findings and Draft Audit Report: delivery of the Auditor's findings, being the deliverable on which the sixty-per-cent payment under §4.3 falls due. A comprehensive report detailing all findings, their severity per Appendix C, affected code paths with file and line references, preconditions, potential impact, proof-of-concept or reproduction steps where

feasible, and specific remediation recommendations including code examples where appropriate.

- Public Audit Status Note: a public note suitable for the Client's governance process, issued twice — once at engagement start to accompany the forty-per-cent upfront spend proposal, stating the agreed scope, frozen commit, timeline and deliverables; and once on delivery of findings to accompany the sixty-per-cent spend proposal, stating the paths covered and their review depth, the engineer-hours performed, and the count of findings by severity (Critical and High findings stated as counts only while under the embargo in §6.2). It does not disclose the content of unremediated Critical or High findings.
- Final Audit Report: the draft report updated after the re-audit under §2.4, stating the remediation status of every finding, and including the review depth map from Appendix B and a risk assessment matrix evaluating likelihood and impact for each finding. The Final Audit Report is suitable for publication.
- Recommendation Summary: a concise, prioritised summary of key recommendations, separating consensus-breaking fixes that require a governance upgrade from non-breaking fixes.
- Hardened Continuous Integration Configuration: a `.golangci.yml` and workflow addition with the security-relevant linters enabled and existing violations triaged, delivered as a pull request early in the engagement. The Client's current configuration disables `errcheck`, `staticcheck`, `revive` and `unparam`, with the result that unchecked error returns are not detected anywhere in the repository. Where a triaged violation is itself security-relevant, it is reported to the Client confidentially under §6 and is not disclosed in the public pull request until the embargo in §6.2 has run.
- Fix Verification Statement: a per-finding statement of whether the remediation is verified, partially verified or not effective, issued as part of the re-audit under §2.4.

2.3 Remediation advisory

The Auditor shall provide remediation advice on reported findings for four weeks from delivery of the draft Audit Report, included in the contracted fee. Following the Auditor's recommendations, the Client may implement such recommendations and take any other relevant actions in respect of its protocol.

2.4 Re-audit after remediation

A full re-audit is included in this Agreement and is budgeted at 32 engineer-hours within the total under §4.2. The re-audit comprises:

1. Verification of each reported finding against the Client's remediation, re-testing against the original reproduction or proof of concept where one exists.
2. Review of the remediation diff for regressions and for defects newly introduced by the fixes.
3. Confirmation, per fix, of whether it is consensus-breaking and therefore requires a governance upgrade.
4. Issue of the Fix Verification Statement and the updated Final Audit Report.

The re-audit covers the remediation diff measured against the commit frozen under §1.1. Unrelated development that landed on `main` during the remediation window is not in scope. The Client

shall declare remediation complete in writing within the four-week window under §2.3 and shall provide the material listed in §5 item 7. Where the remediation diff is materially larger than the reported findings require, for example because the Client has restructured code beyond the scope of the fixes, the Auditor shall notify the Client and propose a change order under §4.4 rather than reduce verification quality to remain within the budgeted hours. A further re-audit pass beyond the one included here is a change order under §4.4.

3. Timeline

The Audit will commence once the governance text proposal that approves this Agreement has passed and the forty-per-cent upfront payment under §4.3 has been received, subject to team availability and requiring three weeks' lead time from receipt of that payment. The timings below are measured from commencement.

Phase	Deliverable	Timing measured from commencement
1	Threat Model and Architecture Note, hardened CI pull request	end of week 1
2	Interim Findings Report	end of week 5
3	Delivery of Audit Findings and Draft Audit Report (triggers the 60% payment per §4.3)	end of week 8, report within three business days
4	Client remediation window per §2.3, remediation performed by the Client's own developers at no cost to the community pool	Client-controlled, up to four weeks
5	Re-audit and Fix Verification Statement per §2.4	within one week of the Client's written declaration that remediation is complete
6	Final Audit Report	within five business days of the re-audit

Active Auditor effort is approximately 8 weeks to delivery of findings plus the re-audit under §2.4, the latter included within the sixty-per-cent payment and performed after the Client's remediation window. Elapsed time to the Final Audit Report is approximately eleven to twelve weeks of active work, assuming a Client remediation window of two weeks, plus the time taken by the two spend-proposal votes. Each additional week the Client takes for remediation extends the calendar by the same amount without changing the contracted effort or fee.

Calendar durations assume two reviewers working in parallel and assume the Client meets its obligations under §5. Delay in Client response, and the duration of the two spend-proposal votes, extend the calendar but not the contracted effort.

4. Fees and Payment

4.1 Rate

All work is billed at a single rate of USD 150 per engineer-hour, equal to USD 1,200 per eight-hour engineer-day. There is no separate project fee, management surcharge or tooling licence charge. Every figure in §4.2 is hours multiplied by this rate.

4.2 Contracted scope and fee

Workstream	Reference	Hours	Fee (USD)
Core protocol audit	Appendix A §1.A, B, D, E, F, G	288	43,200
Framework migration and state integrity review	Appendix A §1.C and §2.E	88	13,200
Adversarial simulation and economic review	Appendix A §1.H and §2.F	64	9,600
Market Module 2.0, USTC staking module and v15 upgrade	Appendix A §1.I and Appendix B	96	14,400
Full re-audit after remediation	§2.4 and Appendix A §2.G	32	4,800
Total contracted effort and fee		**568**	**85,200**

The fee of USD 85,200 is fixed for the scope defined in this Agreement and its appendices. The hour figures per workstream are the Auditor's internal allocation and are shown for transparency; the Auditor may reallocate hours between workstreams provided all contracted scope is delivered, the total does not exceed 568 hours, and the two payment amounts in §4.3 are not changed.

Plus the statutory value-added tax if no VAT-ID is provided. This tax is not applicable if the customer is a registered business outside the European Union.

4.3 Payment schedule and settlement

The fee is paid in two parts under the Pay Per Job process, each through its own community-pool spend proposal after the governance text proposal approving this Agreement has passed:

Part	Trigger	Share	Fee (USD)
Upfront	Before the Auditor starts work, after the text proposal passes	40%	34,080
On delivery of findings	On delivery of the Audit Findings and Draft Audit Report under §2.2	60%	51,120
Total		**100%**	**85,200**

The forty-per-cent upfront payment is made before commencement; the Auditor begins the three-week lead time under §3 on receipt of it. The sixty-per-cent payment falls due on delivery of the Audit Findings and Draft Audit Report and covers the remainder of the engagement, including the full re-audit under §2.4, which the Auditor performs after the Client's remediation window without further charge.

Settlement currency and conversion. The fee is fixed in USD and is paid to the Auditor in USDC at the address in Appendix D; the Auditor bears no LUNC price, conversion or slippage risk. Each spend proposal requests the LUNC required for its share, sized at the LUNC/USD rate at the time that spend is submitted, with the rate source, date and resulting LUNC amount stated in the proposal. No buffer is added to either spend. The disbursed LUNC is received by the Client's receiving multisig (Appendix D), converted off-chain through SimpleSwap at a cost of approximately one per cent, and the USD fee is remitted to the Auditor in USDC. Any LUNC or converted funds left after the Auditor is paid are returned by the Client to Terra Classic Core, with the transaction published in the governance thread. The approximate one-per-cent conversion cost is borne by the community pool, not by the Auditor.

Each payment is conditional on its spend proposal passing. The Auditor does not commence work until the upfront spend proposal has passed and the upfront payment has been received, and is under no obligation to continue work if the second spend proposal does not pass, as set out in §11.

4.4 Change orders

Scope changes, commit re-basing, review depth upgrades and additional review rounds are quoted in hours at USD 150 per engineer-hour and require written agreement before work commences. Indicative add-ons:

Add-on	Hours	Fee (USD)
Upgrade the D3 paths to D2 review	24	3,600
Upgrade all D2 paths to D1 review	56	8,400
Double the depth on the existing D1 set	184	27,600
Exhaustive replay of the store migration over the full mainnet key space	40	6,000
A further re-audit pass beyond the one included under §2.4	32	4,800
Support for patch preparation and validator communication under §6.4	as incurred	at the §4.1 rate
Re-base onto a later commit	by quotation on the actual diff	by quotation

A change order agreed in writing is funded through its own community-pool spend proposal and settled on the same terms as §4.3: the fee is fixed in USD, paid to the Auditor in USDC, with the Client's multisig converting the disbursed LUNC off-chain and bearing the conversion cost, and no buffer added. The additional `x/market` and `x/vesting` code referred to in §1.1, once published by the Client, is quoted and funded as such a change order or as a separate job.

5. Client Obligations

The contracted effort assumes the Client provides:

1. A named technical counterpart reachable within one business day and authorised to answer design-intent questions, together with answers to the Auditor's scoping questions before commencement.
2. Architecture and design context, including the rationale for the Cosmos SDK module overrides, the intended behaviour of the burn tax and exemption mechanism, and the design intent behind the store migration. The Client acknowledges that `CHANGELOG.md` has not been maintained since 2023 and cannot serve this purpose.
3. A reproducible build and a working local network. The `make` targets and the end-to-end and interchain test suites must run from a clean checkout of the frozen commit.
4. Current mainnet parameter values for the market, oracle, treasury, tax and tax exemption modules, and the list of upgrade heights already executed.
5. A mainnet state snapshot spanning the store migration height at block 25,619,230, or a documented reason why none can be provided.
6. A designated security contact and disclosure channel per §6, established before commencement.
7. For the re-audit under §2.4: a remediation branch or set of pull requests against the frozen commit, a mapping from each finding identifier to the commits that address it, and a written declaration that remediation is complete.

Material failure to provide items 1 to 6 entitles the Auditor to extend the schedule without reduction in fee. Failure to provide item 7 within the window under §2.3 entitles the Auditor to issue the Final Audit Report without the re-audit and without the Fix Verification Statement. The re-audit under §2.4 is included within the sixty-per-cent payment already made on delivery of findings; accordingly no fee is refundable on this account, and the 32 unused re-audit hours are credited to the Client against any subsequent engagement.

6. Coordinated Disclosure and Live-Chain Handling

The parties acknowledge that the core chain at the base commit `f54cdec` is live on mainnet and that a Critical finding in that code is therefore an incident response and validator coordination matter rather than a pre-launch fix. The Market Module 2.0, the `x/ustcstaking` module and the `v15` upgrade frozen under §1.1 are pre-deployment code; for those components a Critical or High severity finding is a pre-deployment fix, and the Client should not deploy them until such findings are remediated. The provisions below apply to both, with the reporting timings in §6.1 applying to findings in the already-deployed code in all cases. Accordingly:

6.1 The Auditor shall report Critical severity findings to the Client's designated security contact within 24 hours of identification, out of band and ahead of any written report. High severity findings shall be reported within three business days.

6.2 Both parties shall observe an embargo on unfixed Critical and High severity findings until a patch has been released and validator adoption confirmed, or for 90 days from the report, whichever occurs earlier.

6.3 The Final Audit Report may be redacted for publication by mutual written agreement where a finding remains unremediated. The Auditor shall not publish or otherwise reference unremediated Critical findings.

6.4 The Auditor will, on request and at the rate in §4.1, support patch preparation and validator communication. The Auditor does not perform the upgrade and bears no responsibility for its execution or outcome.

6.5 Reporting of Critical and High severity findings under §6.1 does not depend on payment status. Because the audited code is live on mainnet, the Auditor shall report any Critical or High severity finding to the Client's designated security contact within the time stated in §6.1 even where the second spend proposal under §4.3 has not yet been submitted, is under vote, or has failed. This obligation is a live-chain safety requirement and overrides §8 to the extent of any conflict.

7. Limitation of Liability

7.1 General Limitation. The Auditor shall perform the Audit using the degree of skill and care required by current professional standards and practices. However, the Auditor does not guarantee that the Audit will identify all potential security vulnerabilities or that the recommendations will secure the blockchain protocol. The Client acknowledges that, in IT security, risk cannot be eliminated, and that the review depth allocation under §1.2 is a deliberate and disclosed limitation on coverage.

7.2 Undetected Errors. The Client acknowledges that even a diligent audit provides reasonable, not absolute, assurance and may not uncover all potential issues. Subject to §7.5, the Auditor is not liable for issues, errors or vulnerabilities that are not identified during the Audit, provided the Audit was performed with the skill and care required under §7.1 and at the depth contracted under §1.2.

7.3 Future Security Guarantees. The Auditor makes no warranties or representations that the Client's systems, including Terra Classic, will be secure from breaches or intrusions in the future. The Audit is a risk assessment at a point in time, against the code at the commit frozen under §1.1, the remediation diff verified under §2.4, and the threats known at the time of the Audit.

7.4 Indirect and Consequential Damages. To the extent permitted by law, the Auditor is not liable for indirect, incidental, special, consequential or exemplary damages arising out of or in connection with the services provided under this Agreement, including damages for loss of profits, goodwill, use, data, tokens or other intangible losses, even if the Auditor has been advised of the possibility of such damages.

7.5 Mandatory Liability. Nothing in this Agreement excludes or limits the Auditor's liability for intent (Vorsatz), for gross negligence (grobe Fahrlässigkeit), for injury to life, body or health, for the culpable breach of an essential contractual obligation (Kardinalpflicht), or in any other case where liability may not be excluded or limited under mandatory German law. In the case of simple negligence in respect of an essential contractual obligation, liability is limited to the foreseeable damage typical for this type of contract.

7.6 Cap on Liability. Save where §7.5 applies, the total aggregate liability of the Auditor under this Agreement shall not exceed the total fees paid by the Client for the services rendered. This cap is an agreed allocation of risk between the parties, reflecting the fee level and the disclosed depth limitation under §1.2.

8. Intellectual Property

The findings, reports and documentation generated during the Audit remain the Auditor's property until the sixty-per-cent payment on delivery of findings under §4.3 has been received. From the moment any deliverable is delivered to the Client, and irrespective of payment status, the Client is granted a non-exclusive, non-transferable licence to use that deliverable for its internal purposes, including implementing the remediation through its own developers; this licence survives any later failure of the second spend proposal and any termination.

Upon receipt of the sixty-per-cent payment under §4.3, all intellectual property rights in the findings, reports and documentation relating to the Audit, including the Audit Report, belong to the Client, and the Auditor shall take all necessary steps to give effect to that transfer. The Client may thereafter use and publish the Audit Report without restriction, subject only to the embargo in §6.2.

Where the second spend proposal finally fails under §11 and the sixty-per-cent payment is therefore not received, the Auditor retains all intellectual property rights in the findings, reports and documentation, subject always to the internal-use licence above and to the live-chain reporting obligation in §6.5.

The Auditor may reference the engagement and the published Audit Report in its own marketing materials.

All property rights in any and all source code subject to the Audit remain exclusively with the Client at all times.

9. Confidentiality and Non-Disclosure

9.1 Confidentiality Obligation. Both parties agree to treat all information exchanged during the Audit, including audit findings, reports, client data, technical and financial information and any other proprietary information disclosed during the performance of the Audit, as confidential ("Confidential Information"). Both parties shall refrain from disclosing Confidential Information to any third party except as required by law, as permitted under §9.8, or as agreed in writing by both parties.

9.2 Use of Confidential Information. The Confidential Information shall be used solely to execute the obligations and rights under this Agreement. Both parties shall ensure that their employees, agents and subcontractors with access to the Confidential Information are bound by equivalent confidentiality and non-disclosure obligations.

9.3 Security Measures. Both parties shall take all reasonable precautions to protect the confidentiality of the Confidential Information, at a level of protection no lower than that which the receiving party applies to its own most confidential information.

9.4 Exclusions. The obligations of confidentiality shall not apply to information that is or becomes publicly known through no breach of this Agreement by the receiving party; is received from a third party without breach of any obligation of confidentiality; or is independently developed by the receiving party without use of or reference to the disclosing party's Confidential Information.

9.5 Duration. The confidentiality obligations shall remain in effect for three years after the termination or expiration of this Agreement, unless a longer period is required by law or agreed in writing.

9.6 Breach. In the event of a breach or threatened breach of this Section, the other party shall be entitled to seek injunctive relief, which remedy is cumulative and not exclusive and is in addition to any other rights and remedies available at law.

9.7 Termination or Expiry. Upon any termination or expiry of this Agreement, the recipient party shall promptly return to the disclosing party or, at the disclosing party's option, destroy all of the disclosing party's Confidential Information received during the term.

9.8 Publication. The parties acknowledge that the Client intends to publish the Final Audit Report as part of its governance process. Publication of the Final Audit Report by the Client, subject to §6.2 and §6.3, does not constitute a breach of this Section. The parties further acknowledge that the Pay Per Job process requires certain governance-facing material to be public: the Public Audit Status Note issued with each spend proposal under §2.2, the governance text proposal that approves this Agreement, and the two spend proposals. Publication of those items does not constitute a breach of this Section, provided that the content of unremediated Critical and High severity findings remains subject to the embargo in §6.2 and is not disclosed in any publicly posted material.

10. Dispute Resolution

Any disputes arising from this Agreement shall be resolved through binding arbitration following the laws of Germany.

11. Termination

30-Day Termination Right. Either party may terminate this Agreement with thirty days' written notice. Upon termination, the parties settle the engineer-hours actually performed to the effective date at the rate in §4.1 against the forty-per-cent upfront payment: the Auditor retains that payment to the extent of hours performed, and any portion of the upfront payment not so earned is returned by the Auditor to Terra Classic Core. The Auditor shall deliver all work product completed to the effective date.

Failed Spend Proposal. A spend proposal under §4.3 is treated as failed if it is rejected, is defeated by NoWithVeto, or fails to reach the quorum required under the Client's governance rules. On a first failure the Auditor, or the Client's representatives, may submit one resubmission of that spend proposal within fourteen days.

- If the forty-per-cent upfront proposal fails and is not carried on resubmission, the Auditor has no obligation to commence work and either party may terminate on written notice, with no fee due on either side.
- If the sixty-per-cent proposal fails and is not carried on resubmission, the Auditor may terminate immediately on written notice. In that event the Auditor has delivered the Audit Findings but is not paid the sixty-per-cent part; it retains the intellectual property in the findings and reports under §8, is not obliged to perform the re-audit under §2.4, and retains the forty-per-cent upfront payment. The internal-use licence in §8 and the live-chain reporting obligation in §6.5 survive.

Immediate Termination. Notwithstanding the above, either party shall have the right to terminate this Agreement immediately if:

1. The other party has materially breached any of its obligations under this Agreement, including failing to make required payments, failing to adequately perform the audit services, or failing to deliver the Audit Report;
2. There has been fraud, misrepresentation, willful misconduct or a violation of law by the other party or its representatives;

3. The other party becomes the subject of a voluntary or involuntary petition in bankruptcy, or any voluntary or involuntary proceeding relating to insolvency, receivership or liquidation for the benefit of creditors, or ceases doing business; or
4. Performance of this Agreement becomes impossible for that party as a result of significant changes in applicable laws.

Upon any such termination, the Auditor shall deliver all work product completed to the effective date, and the parties shall settle the engineer-hours actually performed to that date at the rate in §4.1 against the forty-per-cent upfront payment, with any unearned portion of that payment returned by the Auditor to Terra Classic Core.

12. Governing Law and Jurisdiction

12.1 Governing Law. This Agreement shall be governed by and construed following the laws of Germany, without regard to its conflict of law principles.

12.2 Jurisdiction. The parties agree that any legal action or proceedings arising out of or in connection with this Agreement shall be exclusively brought in the courts of Flensburg, Germany, and each party hereby consents to the jurisdiction of such courts.

13. Compliance with Data Protection Regulations

13.1 Data Protection Compliance. Both parties will comply with all applicable data protection laws concerning the processing of personal data under this Agreement, including the General Data Protection Regulation (GDPR) as implemented by the European Union.

13.2 Data Processing and Security. Where the processing of personal data is required, both parties agree to process the data only to fulfil their obligations under this Agreement; to ensure that all personnel involved in handling personal data are informed of the data's confidential nature and are bound by confidentiality obligations and use restrictions; and to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, considering the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

13.3 Data Subject Rights. Both parties shall assist each other in facilitating the exercise of data subject rights under the GDPR, including the right to access, rectify, erase, restrict processing, and data portability concerning the data subject's personal data.

13.4 Data Breach Notification. In the event of a personal data breach, both parties shall cooperate to inform the competent data protection authority and the affected data subjects in compliance with the obligations under the GDPR.

14. Contracting Entity and Acceptance

The parties acknowledge that a blockchain network is not a legal person and that a community governance proposal is not, by itself, a contracting party. The Client is Terra Classic Core, the coalition of Bumeo Capital and LunaClassicDAO, acting through the authorised representatives named below. Both payments under §4.3 are made through, and are conditional on the passing of, their respective community-pool spend proposals.

14.1 Authorised representatives. Terra Classic Core designates the following as its authorised representatives, who countersign this Agreement in that capacity and act as the Auditor's counterpart for the purposes of §5, §6 and the acceptance of deliverables: Puya (Bumeo Capital) and Classic DAO (LunaClassicDAO), with Renzo (LunaClassicDAO) and Till, also known as Frag (Bumeo Capital), as the developers responsible for remediating the findings at no cost to the community pool. Acceptance of this Agreement through the governance text proposal does not create personal liability for any representative beyond the role so described.

14.2 Governance acceptance and funds flow. The governance text proposal that approves this Agreement shall identify it by the SHA-256 hash of this document, so that the terms accepted are fixed and verifiable. Both payments are disbursed from the community pool to the receiving multisig identified in Appendix D, whose signers are Renzo (LunaClassicDAO), Frag (Bumeo Capital), Puya (Bumeo Capital) and Classic DAO (LunaClassicDAO); the multisig converts the LUNC off-chain and remits the USD fee to the Auditor in USDC under §4.3. Where a legal entity is later substituted as Client, it may pay the Auditor directly in USDC to the address in Appendix D only by prior written agreement with the Auditor.

15. Entire Agreement and Amendments

This Agreement, together with Appendices A, B, C, D and E, constitutes the entire agreement between the parties in respect of the Audit and supersedes all prior proposals, offers and drafts, including the earlier versions of this Agreement dated 16.09.2026, 01.10.2026 and 27.10.2026, the offer dated 15.09.2026 and the draft agreement dated 07.06.2025. Amendments require written form. Should any provision be or become invalid, the validity of the remaining provisions is unaffected, and the parties shall replace the invalid provision with a valid one that most closely reflects its commercial purpose.

IN WITNESS WHEREOF, the parties hereto have executed this Security Audit Agreement as of the date first above written.

Handewitt, dated

_____

Mails Nielsen CEO and Co-Founder of SolidProof.io
Operated by FutureVisions Deutschland UG (hbs.)

_____

For the Client: Terra Classic Core — authorised representatives Puya (Bumeo Capital) and Classic DAO (LunaClassicDAO) per §14, date

Appendix A

Audit Scope and Methodology

1. Core Focus Areas

All areas A to H are within the contracted scope of this Agreement.

A. Custom Module Implementation

- Oracle module: vote and prevote handling, ballot construction, weighted median tally, reward distribution, miss counting and slashing, and the module's ABCI hooks.
- Treasury module: seigniorage computation and distribution, tax and reward policy updates, economic indicators, burn account operations, and governance proposal handling.
- Market module: swap mechanism, constant-product pool behaviour, pool recovery, stability spread application, and oracle price integration.
- Tax and tax exemption modules: burn tax computation, splitting to the distribution module, exemption zones and address lists, governance proposal handling, and the interaction between the two modules.
- Dyncomm module: dynamic validator commission calculation and enforcement through its ante and post decorators.
- Vesting module: custom vesting account types and their interaction with staking and bank.

B. Transaction Processing and Fee Handling

- Composition and ordering of the custom ante handler chain, and the consequences of that ordering for authentication, gas metering and fee deduction.
- Correctness of fee and burn tax computation, including rounding and truncation direction, precision loss, and interaction with fee grants.
- The custom post handler chain and its state effects.
- Oracle vote spam prevention, IBC transfer spam prevention and minimum initial deposit enforcement, including correct separation of CheckTx-only from consensus-relevant behaviour.
- The custom transaction service and its compatibility layer.

C. Framework Migration and State Integrity

- The hand-written migration of the CosmWasm key-value store from the forked key layout to the upstream layout, including contract keys, code keys, contract storage keys, contract history, secondary indexes, sequence keys and params. Particular attention to the length-prefix and composite-key heuristics applied to attacker-influenced contract storage keys.
- The legacy store compatibility shim serving historical queries across the migration height, including its determinism on the contract execution path and its implications for archive node replay.

- All twenty upgrade handlers, the declared store upgrades against the actual store keys, handler idempotency, and the effect of handlers that reset module parameters.
- Height-conditional and chain-ID-conditional branches on the consensus path.
- Retained fork logic and the conditions under which it could be re-registered.

D. Cosmos SDK Override Layer

- All thirteen module overrides, with emphasis on the wasm, staking, bank and governance overrides, and on the legacy query servers and message services retained for backward compatibility.
- Correctness of the module manager ordering for PreBlock, BeginBlock, EndBlock and InitGenesis.
- Module account permissions and the blocked address set.
- The authority address on every parameter update message.

E. CosmWasm Integration

- The custom query and message plugins, including the Stargate query allow-list and its deterministic-response requirement.
- Reentrancy and state consistency across the virtual machine boundary, and gas accounting across that boundary.
- The custom wasm message service retained from the legacy chain.
- The migration surface introduced by wasmd 0.46 to 0.61 and wasmvm 1.5 to 3.0.

F. IBC Integration

- Composition and ordering of the ICS4 wrapper and the IBC hooks middleware relative to the transfer, interchain accounts and wasm stacks.
- Packet, acknowledgement and timeout handling, and the effect of the ibc-go v7 to v10 migration including the removal of the capability module.
- Whether the version 2 packet path is reachable in the absence of a registered version 2 application router.

G. Node-Level Availability and API Surface

- The custom FIFO mempool, its eviction and ordering behaviour, and the ABCI++ proposal preparation and processing handlers built on it.
- The custom HTTP middleware, including the transaction log reconstruction layer, assessed for unbounded allocation and parsing robustness.
- Default node configuration and its hardening.

H. Economic Mechanism Implementation and Adversarial Simulation

- Oracle price feed manipulation resistance, vote buying, and Sybil resistance of the voting mechanism as implemented.
- Burn tax bypass paths and exemption abuse.

- Treasury drain scenarios and seigniorage manipulation.
- Denial of service scenarios targeting the custom modules and the custom mempool.
- Where the market swap mechanism is enabled by on-chain parameters, market manipulation and arbitrage scenarios. The Auditor notes that the chain's historical fork logic set the minimum stability spread to 100%, which disables swaps; the Market Module 2.0 and `v15` upgrade under §1.I change this, so the market-manipulation and arbitrage scenarios are in scope as implemented on the frozen branch.

I. Market Module 2.0, USTC Staking and the v15 Upgrade (ustc_staking branch)

This focus area covers the pre-deployment additions frozen under §1.1.

- Market Module 2.0: the re-implemented swap mechanism and its re-activated economics, the restriction of allowed swap denoms to `uusd`, the market accumulator module account, the oracle TWAP and freshness hooks feeding the market, and the integration of the distribution keeper into the market keeper. Reviewed for swap and pool arithmetic, manipulation and arbitrage resistance, and correctness of the accumulator accounting.
- Tax redirect: the refactored burn and tax split in the fee and burn-tax path that redirects a portion of taxes to the market accumulator, reviewed for rounding and truncation direction, conservation of value across fee collector, oracle, market accumulator and community pool, and interaction with the exemption mechanism.
- New `x/ustcstaking` module: message handlers, keeper state transitions, staking and reward arithmetic, authorisation on every message, module account permissions, genesis and invariants, and its ABCI hooks, reviewed at D1 as fund-moving code.
- The `v15` upgrade handler: the parameter changes it applies (allowed swap denoms, oracle meta denom in vote targets), its idempotency, and the absence or presence of store migrations, assessed against the declared store upgrades.

2. Audit Methodology

A. Architecture and Threat Model

Performed by the lead auditor at the start of the engagement. Produces the module dependency and keeper graph, store key inventory, privilege and authorisation map, trust boundaries, and a threat model recording assets, adversaries and attack surfaces. Issued to the Client for challenge before the bulk of the review is performed. Where this phase establishes that an area is denser or more irregular than assumed, the Auditor shall notify the Client and propose either a depth reallocation under §1.2 or a change order under §4.4, rather than silently reducing review quality to remain within the contracted hours.

B. Manual Code Review

Performed by the lead auditor and the senior auditor, organised by focus area and executed at one of three depths:

- D1, deep review: every state transition, arithmetic operation, authorisation check and error path read and reasoned about adversarially against the threat model. Findings pursued to a reproduction or a reasoned impossibility argument. Routine boilerplate within a D1 path,

such as codec registration, CLI wiring, accessors and genesis marshalling, is triaged quickly so that time is spent on the dense logic.

- D2, targeted review: entry points, message handlers, state transitions and authorisation boundaries read in full; internal helpers read selectively. Findings reported but not always driven to a proof of concept.
- D3, tooling sweep and spot check: hardened static analysis, dependency and advisory checks, and manual spot checks of anything the tooling flags or that appears anomalous. No systematic manual read.

C. Static Analysis and Supply Chain

Go static analysers run with a hardened configuration: gosec, staticcheck, errcheck, govulncheck, nilaway and golangci-lint. Review of module dependencies including the retained replace directives and known advisories affecting the pinned wasmvm, ibc-go, CometBFT and Cosmos SDK versions. Custom checks for Cosmos SDK patterns, including map iteration on the consensus path and unchecked error returns in keeper code.

D. Dynamic Analysis and Fuzzing

Property-based and fuzz testing of the paths where incorrect arithmetic or key handling has consequences: oracle ballot tally and reward distribution, burn tax and exemption computation, dynamic commission enforcement, and the migration key handling functions. Restoration and execution of the currently disabled application simulation with invariant checks.

E. Migration Verification

Differential replay of the migration functions against a representative sample of mainnet-derived key material, comparing pre- and post-migration key spaces for completeness, prefix collision and orphaned entries, and probing the length-prefix and composite-key heuristics with adversarially constructed keys. Determinism analysis of the legacy store read path and of archive replay across the migration height. At the contracted effort this verification is sampled and targeted; it is not an exhaustive replay of the full mainnet key space, which is available as a change order under §4.4 and requires the Client to supply a full archive snapshot.

F. Adversarial Simulation

Localnet and interchain test scenarios for adversarial IBC, mempool and governance behaviour; multi-validator misbehaviour scenarios; and the economic scenarios listed in §1.H.

G. Remediation Verification and Re-audit

Performed by the lead auditor after the Client declares remediation complete. Each finding is re-tested against its original reproduction or, where no reproduction exists, against the reasoning that established it. The remediation diff is read at D1 depth irrespective of the depth originally assigned to the path, on the basis that freshly written fix code carries higher defect density than reviewed code. The static analysis and fuzz harnesses from §2.C and §2.D are re-run against the remediated tree. Results are recorded per finding in the Fix Verification Statement and folded into the Final Audit Report.

3. Vulnerability Classes Targeted

The review is organised around failure modes specific to Cosmos SDK Layer 1 chains: non-determinism and state divergence; state migration defects; transaction lifecycle and fee handling errors; authorisation and privilege defects; economic mechanism implementation errors including precision

loss and manipulation resistance; CosmWasm integration defects including reentrancy and gas accounting; IBC integration defects; and node-level availability defects.

4. Tools and Resources

Security tools: Go native fuzzing and custom module fuzzers; the interchain test framework for cross-chain scenarios; localnet for multi-validator adversarial behaviour; the application simulation framework with invariant checks; custom scripts for oracle, tax and migration key testing.

Team: a lead auditor with Cosmos SDK and Go expertise responsible for the threat model, application wiring, migration review, report ownership, re-audit, Client interface and coordinated disclosure; a senior auditor responsible for custom modules, transaction lifecycle, SDK overrides and CosmWasm integration; and a part-time specialist for dynamic verification, state replay and economic modelling.

Client-side resources required: access to a working local network and the test suites, current mainnet parameter values, a mainnet state snapshot, and the remediation material for the re-audit, all per §5.

5. Explicit Exclusions

The following are outside the scope of this Audit:

- Upstream Cosmos SDK, CometBFT, ibc-go, wasmd and wasmvm source code, except where Terra Classic modifies, overrides, wraps or configures it. Consensus-layer properties of CometBFT, including long-range attack resistance, peer-to-peer eclipse resistance and the correctness of the consensus algorithm itself, are properties of the upstream implementation and are not re-derived here. The chain's use and configuration of those primitives is in scope.
- CosmWasm contracts deployed on the chain. Only the chain-side integration is reviewed.
- Generated protobuf bindings. The underlying `.proto` definitions are in scope.
- Off-chain infrastructure: validator operations, sentry topology, relayers, RPC providers, block explorers, wallets and price feeder deployments.
- Formal verification and machine-checked proofs. Where formal methods are referenced in this Agreement, this means property-based testing and model-based test generation.
- Economic and governance policy questions, such as the appropriate level of a tax rate or distribution split. Mechanism implementation is in scope; whether a parameter value is economically advisable is not.
- Development landing on `main` after the commit freeze under §1.1, other than the remediation diff verified under §2.4.

6. Audit Goals

The Audit verifies the security soundness of the Terra Classic custom module implementations and the economic properties of the oracle, treasury, tax and market modules as implemented. It establishes whether the Cosmos SDK, ibc-go and CosmWasm integrations maintain their security properties under adversarial conditions following the SDK53 migration. It assesses the integrity of the state produced by the CosmWasm store migration and the determinism of the compatibility layer serving historical state. It identifies security risks introduced through Terra Classic's customisations, delivers prioritised, implementable remediation guidance distinguishing consensus-breaking from non-breaking fixes, and

confirms through the re-audit that the remediation actually closes the reported findings without introducing new ones.

Appendix B

Components in Scope

1. In scope, with review depth

Scope is defined by path. Depth levels are defined in Appendix A §2.B. This table is the reference against which coverage is judged.

Path	Contents	Raw LOC	nSLOC	Depth
`custom/auth/**`	Ante and post handler chain, fee and burn tax deduction, tax redirect, spam prevention, minimum deposit	1,485	1,112	D1
`x/tax/**`, `x/taxexemption/**`	Burn tax computation, tax redirect, exemption zones and lists, governance proposals	3,141	2,260	D1
`x/oracle/**`	Vote, ballot, tally, ABCI, slashing, reward distribution, market TWAP and freshness hooks	4,579	3,376	D1
`x/treasury/**`	Seigniorage, policy, indicators, governance proposals	3,315	2,482	D1
`app/app.go`, `app/keepers/**`	Wiring, keeper graph, IBC stack, ICS4 and hooks composition, module ordering, market/distribution and ustcstaking wiring	1,365	985	D1
`wasmbinding/**`, `custom/wasm/**`	Custom querier and messenger, Stargate allow-list, legacy query handler and server, legacy store shim	2,193	1,596	D1
`x/dyncomm/**`	Dynamic commission keeper, ante and post decorators	1,350	1,016	D1/D2
`app/upgrades/v13/**`	CosmWasm store key migration	460	330	D1
`x/market/**`	Market Module 2.0: swap and pool recovery, market accumulator, oracle TWAP integration	2,153	1,563	D1
`x/ustcstaking/**`	New USTC staking module: message handlers, keeper state, staking and reward logic, ABCI, genesis	2,890	2,652	D1
`app/upgrades/v15/**`	v15 upgrade: allowed swap denoms restricted to `uusd`, oracle meta denom in vote targets	63	45	D1
`x/vesting/**`	Custom vesting accounts and their interaction with staking and bank	443	300	D2

Path	Contents	Raw LOC	nSLOC	Depth
`custom/staking/**`, `custom/bank/**`, `custom/gov/**`	Staking hooks and legacy query server, bank overrides, governance customisation	1,400	1,000	D2
`app/mempool/**`, `server/**`	FIFO mempool, ABCI++ proposal handlers, HTTP middleware	506	370	D2
`app/upgrades/**` excl. v13 and v15, `app/{genesis,forks,modules,export,testnet}.go`, `app/{legacy,params,testing,helper}/**`	Remaining nineteen upgrade handlers, store upgrades, genesis, fork and testnet logic, legacy migration helpers	2,751	2,175	D2
`custom/{authz,distribution,evidence,feegrant,mint,params,slashing,upgrade}/**`	Thin SDK module wrappers, codecs, simulation, CLI	523	380	D3
`cmd/**`, `types/**`, `client/**`	Daemon root and configuration defaults, shared types and utilities	1,581	1,210	D3
Total core		30,329	23,203	
`proto/**`	31 protobuf definitions, message and query surface	n/a	n/a	D3
Configuration	`go.mod`, `.golangci.yml`, `.codecov.yml`, CI workflows, `Dockerfile`, `Makefile`, `5sims.mk`	n/a	n/a	D3

Resulting distribution of the 23,203 nSLOC audit target: approximately 68% at D1, 23% at D2 and 6% at D3, with the balance accounted for by rounding. Per-path nSLOC figures are derived from measured raw-to-nSLOC ratios and are indicative to within a few percent; per-directory raw line counts and the core total are measured exactly at the frozen commit.

The remediation diff verified under §2.4 is reviewed at D1 depth regardless of the depth assigned to the underlying path in this table.

2. Reviewed for adequacy rather than line by line

Path	Raw LOC	nSLOC
`**/*_test.go`	23,571	17,700
`tests/**`, end-to-end and interchain harness	4,386	3,456

Test code is assessed for coverage adequacy against the threat model, meaning which security-relevant paths lack tests and whether the existing tests would detect the failure modes in Appendix A §3. It is not reviewed line by line, as test code is not attack surface. The Auditor notes that the Client's coverage configuration excludes the entire `custom/` directory, comprising 3,774 nSLOC of consensus-critical overrides including the full ante and post handler chain, from coverage measurement.

3. Out of scope

Generated protobuf bindings (`**/*.pb.go`, `**/*.pb.gw.go`, 50,697 lines); vendored and upstream dependencies except as stated in Appendix A §5; deployed CosmWasm contracts; `docs/`, `contrib/`, `scripts/` and `assets/`.

4. Audit target summary at the frozen commit

```
Go files                                530
Raw LOC, non-test, non-generated     34,730
nSLOC, non-test, non-generated       23,203    audit target
Raw LOC, test files                  23,571
Generated protobuf                   50,697    excluded
Custom modules                            8
SDK module overrides                     13
Upgrade handlers                         21
Protobuf definitions                     31
```

5. Framework versions at the frozen commit

Component	Version at the 07.06.2025 draft	Version at the frozen commit
cosmos-sdk	0.47.17	0.53.6
cometbft	0.37.15	0.38.21
ibc-go	7.10.0	10.5.0
ibc-hooks	v7	v10
wasmd	classic-terra fork 0.46.0-classic.3	upstream 0.61.15
wasmvm	1.5.9	3.0.8
Go toolchain	1.22.12	1.24



Solidproof.io - Trust Made in Germany

Blockchain Security | Smart Contract Audits | KYC | Marketing

FutureVisions Deutschland UG (haftungsbeschränkt)

Heideland-Ost 34
24976 Handewitt
Germany, Deutschland

Sitz der Gesellschaft / Amtsgericht: Flensburg
HRB 16612 FL
USt-IdNr. DE364783510
Geschäftsführer: Mails Nielsen, Kevin Arens

Solidproof.io is a product of
FutureVisions Deutschland

Please note: You automatically accept our Terms and Conditions and Privacy Policy when using our services.

You can find the current version on our website: https://solidproof.io.

© 2026 SolidProof.io. All rights reserved. This document may not be reproduced or distributed without written consent.


Solid Proofed
Blockchain Security | Smart Contract Audits | KYC
Development | Marketing
MADE IN GERMANY