QRUCIALDAO WHITEPAPER

The protocol for transparent on chain security audits

QRUCIAL OÜ
hello@qrucial.io

outline

01

Abstract

Abstract

This Whitepaper proposes a new blockchain based security system built on Substrate ready for polkadot.

QRUCIALDAO runs a web3 security toolbox in a verified container and stores their output in a dynamic soulbound NFT to create a Security audit Report.

The AuditreportNFT is non transferable and therefore only valid for the audited smart contract itself. The Auditreport NFT is dynamic so another auditor can apply updates to the report when necessary.These fixes are stored on chain as well, so an auditor cannot simply change his report or withhold vulnerabilities without leaving a trail. The Auditreport Data will have an optional encryption and can be decrypted by the Auditrequestor once the vulnerabilities are fixed or will autodecrypt it after 120 Days.

By storing the results of the on chain security toolboxs assesment into a soulbound NFT, a multitude of attack vectors are remediated.

Introduction

Cryptocurrencies and Web3 projects are claimed to be secure due to the utilization of decentralized infrastructure, shared security models, and security audits. However, security is often not the case.

The blockchain security industry is very opaque, this especially shows in security audits on which web3 falls short of its principles like trustlessness, decentralization, and venerability. Security audits are often times just PDFs, where no one verifies their content, the accuracy of the findings, or if the auditor is knowledgeable enough to do the audit.

QRUCIALDAO is a first-of-its-kind security toolbox, delivering a set of protocols e.g. on-chain security audit system to enhance polkadots security. For our consensus, we run polkadots Npos (Nominated proof of stake) consensus with the aura pallet used for block authoring instead of babe.

QRUCIALDAO will:
make Security Audits opens source by storing them and a state of the tools to generate them on chain, making its content public and verifiable
give auditors a containerized toolbox with well maintained and bleeding edge security tools that rock and deliver reproduceable results
remediate against bad actors: When an auditor acts careless or even malicious, his actions will be uncovered by other Auditors who benefit from challenging questionable security audits.

03

Undisclosed vulnerabilities would be discovered with a higher probability.
Remediate against bribery or blackmail by making the transaction trustless, this way the both parties can be assured the agreement made is kept. We want to make it hard for financially, more-powerful actors to leverage their market power against the market itself in order to manipulate audits or monopolize the market.

We rank auditors and tools based on their reputation, ensuring the market can stay decentralized but ineffective or malicious participants can be economically punished. This way, over time, the market will become unattractive for dishonest actors.

Reproduceable audits
Security audits are a vital part of today's WEB3 landscape which is why it is even more important to have an on chain record of how they were generated in the first place.

This Design benefits both Auditor and Auditee, since there is a clearly defined verifiable on chain record of the agreed upon scope and the delivery deadline of the security audit. This verifiable state can be valuable to find truth in legal disputes between auditor and auditee.
By executing this economic transaction on chain in a trustless process, we remediate against a different attack vectors such as intimidation tactics the withholding of payment or final report.
Chain agnostic through Polkadots architecure including XCM and Cross chain bridges like moonbeam.

Gamify community trough a variety of CTFs, Hackatons

- trustless payments
- verifiable

vision

Vision

We expect a multichain future in which multichain organisms interact with each other autonomously and interoperoperably, and where blockchain technology is the foundation for the next generation of our Internet.

Transparency and independence are to be the fundamental values here, which have to be reflected in all Web3 projects. For Web3 to have an actual future, daily hacker attacks and billions of stolen tokens must no longer be the rule.

Therefore, our core vision with QRUCIAL DAO is to provide a transparent on-chain security solution and let the community be certain about the correctness and validation of their favorite project's security audit. We want to build a future, where auditors and projects can interact seamlessly in an easy and secure environment.

How to ensure this security?
Through transparency and independent scoring procedures, QRUCIAL DAO can provide full access to the security audit and tooling. Moreover, through the scoring system, a high quality standard can be generated. As long as smart contract audits are created and submitted off-chain by Web2 companies, there is too much room for fraud or poor quality.

Fundamentally, audits should be an open, auditable, continuous process, not a one-time event to secure long-term security of a project.
Below, we describe the network architecture of QRUCIAL DAO and show step by step how a transparent and self-sufficient on-chain security audit system will work.

05

Roadmap

Roadmap

Q3 2022
- Website development
- Development of Core logic
- Grant procedure
- Launch of Ambassador program

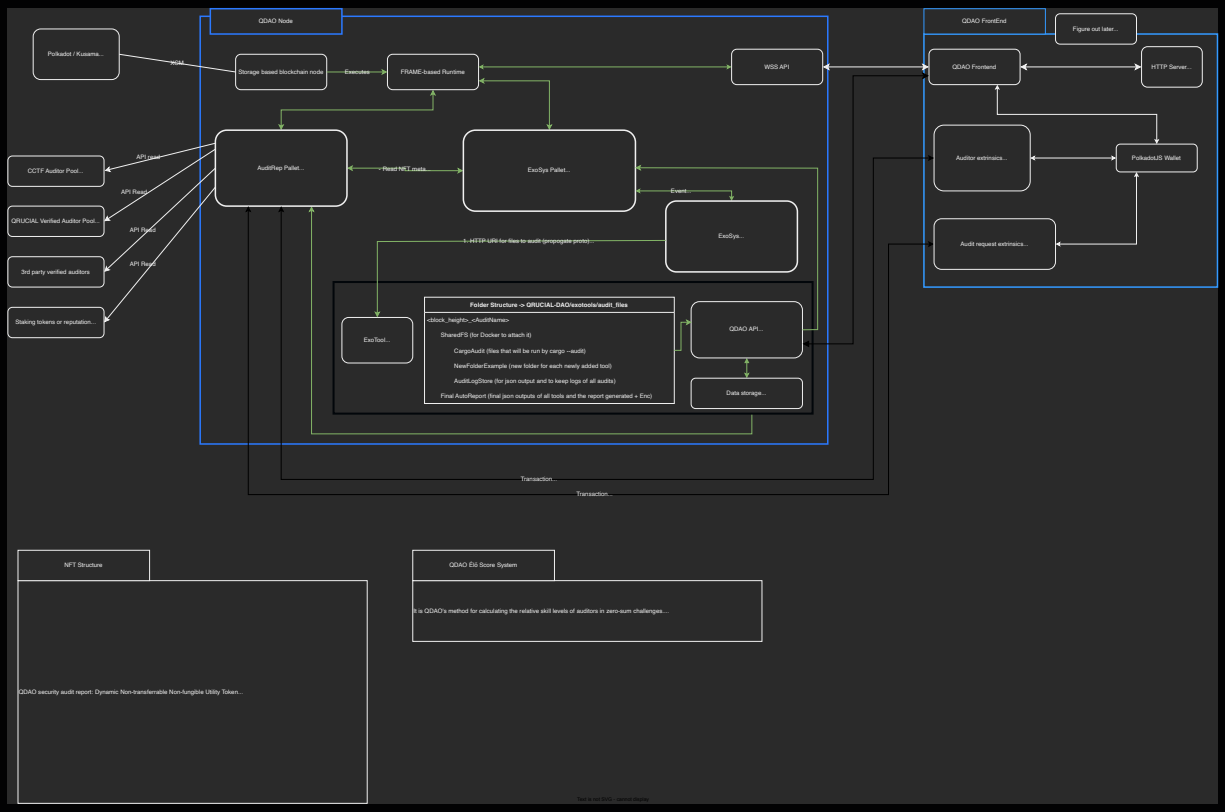
Q4 2022
- Grant procedure Milestone 2
- Substrate Builders Program application
- Seed Funding
- DAPP development
- Addition of fuzzers static analizers to QRUCIALs Web3 Security toolbox

Q1 2023
- Security audit of QRUCIALDAO
- Entering Testnet
- XCM oracle integration

Q2 2023
- EVM compatibility
- Onboading of Industry partners
- Organization of conferences ctfs hackatons and various communtiy events.

Q3 2023
- Kusama Parachain application process

Network design



All blockchains require some consensus mechanism to agree on the state of the blockchain.
QRUCIALDAO is built with substrate and uses Nominated Proof of Stake (NPoS) as its consensus.
The requirement to reach consensus is split into two phases.

Block authoring:
For the process of block production we use substrates aura pallet.

Block Finalization:
For the finality we are using Substrates Grandpa pallet.

Network design

07

DOJO Auditor reputation scoring

QRUCIALs Auditor-reputation pallet contains the logic necessary to calculate and display the skill level of auditors relative to their competitors.

This calculation of performance in non absolute terms is necessary to generate healthy market conditions. With a display of skill in a unified and public way, we can protect the community as well as the on chain economy against low quality auditors and fraudsters disguising themselves as proficient security experts. To measure and display the level of skill we implemented the logic of the Elo rating system.

A method for calculating the relative strength of competitors in games such as chess. An eloscore is represented by a number which changes depending on the outcome of competitions won or lost.

After each competition, points are transferred from the looser to the winner the delta in points between the winner and the looser determines the amount or points transferred. If the higher ranking auditor wins only a few points will be transferred to from the looser. In case a lower skilled auditor gets a upset win many points will be transferred from the looser.

DOJO Auditor reputation scoring

$$E_a = \frac{1}{1 + 10^{\frac{R_b - R_a}{400}}}$$

The Expected probability of a win for Player A given Eloscore of Player A and Player B

$$R_a' = R_a + K\left(S_a - E_a\right)$$

New Eloscore for Player A given current score of Player A, K-Factor, Score and Probability above

DOJO Auditor reputation scoring

09

DOJO Auditor reputation scoring

This way QRUCIALDAOs on chain auditeconomy can be self correcting since Auditors who's rating is too low or too high will loose or win points until their score is a more accurate assessment compared of their skill.

The ELO score also public and visible on each auditors profile.

Auditor A

Score: 800

Auditor B

Score: 500

VS

Auditor A won

3 points are transferred	
The total score	
Auditor A	Auditor B
803	497

Auditor B won

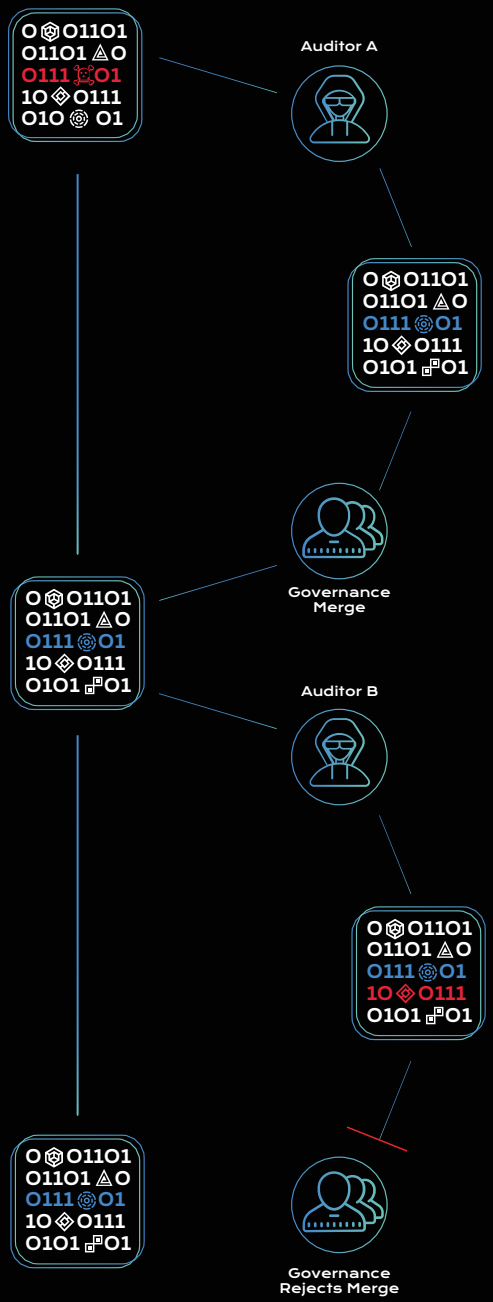
17 points are transferred	
The total score	
Auditor A	Auditor B
783	517

DOJO Auditor reputation scoring

DOJO Auditor reputation scoring

In order to sign up, an auditor has to stake a certain amount of QRD Coins. When QRUCIALDAOs governance decides in his favor, the auditor starts with a default score which meets the threshold, enabling him to accept audits. When he is rejected, the applicant gets back his stake.

To stay active in the market, the auditor needs a certain amount of QRD Coins as a stake, n case the auditor misbehaves a percentage of his stake is slashed as well.



DOJO Auditor reputation scoring

Audit process:
As soon as one of the following statements is true the auditreport is up for challenge by other auditors. The auditrequestor has the right to make the final report public. The timelock threshold of 90 days after submission of the report by the auditor is reached.

This design was chosen because it mitigates against certain attack vectors.
The auditor cant withhold vulnerabilities without running into the risk of being discovered by other auditors. Misbehavior is not only punished economically but also socially through a lowering of the reputation score, up to a point at which an auditor is not able to work on additional audits.

Vulnerability-research and bug bounty's are incentiviced, thus increasing the quality of security-audits. Auditors are held accountable for the quality of their work in a direct feedback loop with their peers.

Wiki:
DOJO-PALLET wiki can be found here

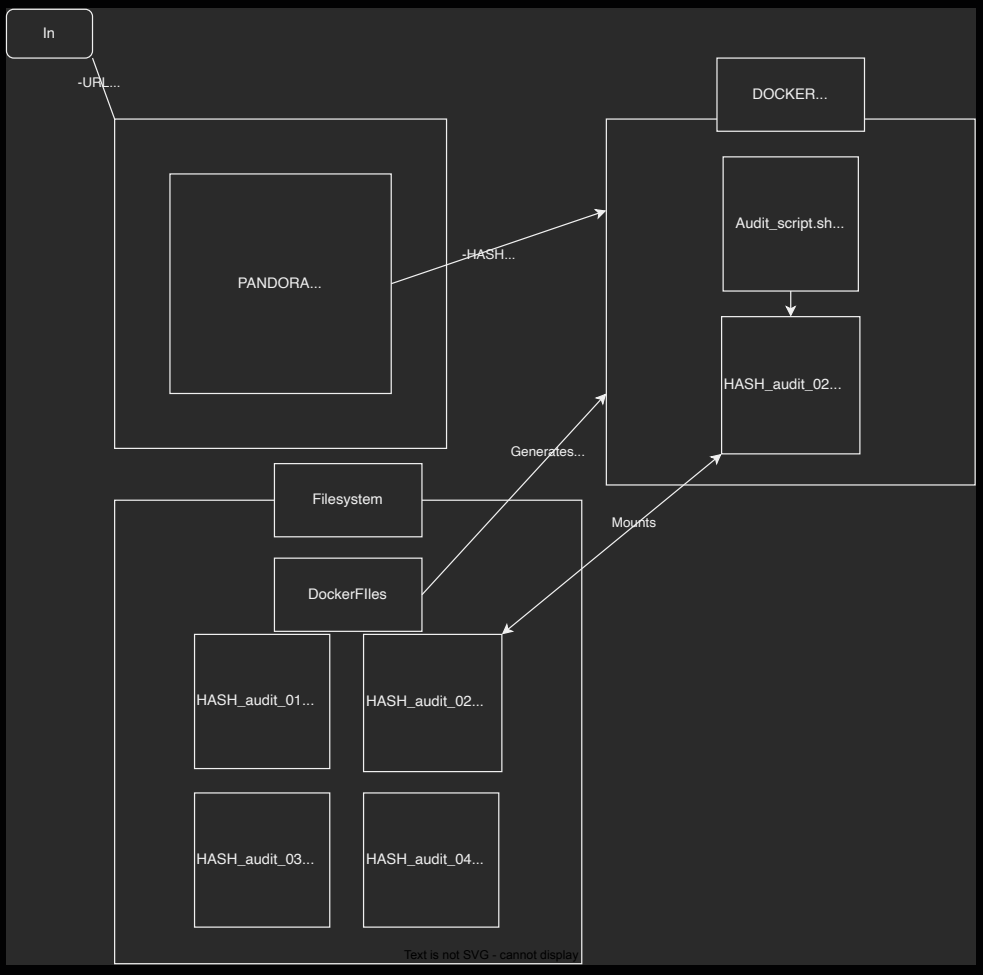
DOJO Auditor reputation scoring

Pandora

On chain security toolbox
QRUCIALs security toolbox contains of a set of tools, that run within a docker container and are used to give security professionals, auditors or curious minds a better insight into the security properties of smart contracts.

Such tools will include vanilla development tools like cargo audit and clippy as well as static analyzers and fuzzers, see roadmap.

This containerized approached makes it possible to bundle tools together in a familiar interface (Docker) and deliver security audit reports in a reproduceable way.



Pandora

Pandora runs in two parts, one side is managing the majority of the logic and decision making, whilst the other side (located within the docker image) is conducting the automated audits, and saving them.

Pandora execution flow:
When executed you supply it with a URL and a hash, the URL is used to download the file to be audited.
The file is then compared against the supplied hash, if the hash is correct and the URL is valid, then a docker image is built and deployed.
On execution of the docker image, it is supplied the correct, hash and date, this is to ensure compatibility so no de-sync happens.
The docker also mounts the local folder a folder in the docker, this is so we can share data between them while still ensuring containerization.

Docker Audit script:
Within the docker the audit script is executed, this script is what executes the automated audit.
First it searches for a cargo.lock file, which is required for an automated audit. If it does not find a cargo.lock, it will generate one based on the Cargo.toml.Once it has a cargo.lock the audit report generation happens, where it searches all dependencies for security vulnerabilities. These vulnerabilities are stored in a .json file, within a date specific folder so it never overwrites old reports. this will be useful once reports can very depending on the users inputs.

Pandora

The output of the web3securitytoolbox is filled into the soulbound NFT by Gemini at mint time.

The metadata filled by Gemini at minttime

Hash of the audited package
Date of request
Deadline for audit
List of files
Report encrypt it or not? Hash of it if requested
Finalization of audit: request + 2 months (idea is to increase this based on contract size)
Deployed address and network (optional)

Audit data stored in

Assignee (first manual auditor, need to stake coins)
Vulnerabilities found (list)
CVE ID, CWE ID <<< was changed from vuln id double check
Found automated or manually?
Risk level (crit, high, mid, low, misc)
Title
Description
ExploitÊ**PoC**
Exploitable: Unchecked / False Positive / Positive --> to be decided by Greybeards(council)
Fixed?
First audit done? Yes/No
Audit finish/quality verified by "Ambassador" -> Accepted/PleaseFix
Challenges (list + what they found)

Sandworm

Sandworm

Security audit request handling and event based tool activation.

Sandworm is implemented as a glue between the the execution of the web3securitytoolbox and the creation of its NFT certificate it is connected through the gemini pallet api sandworm (gemini daemon) is subscribed to Gemini events looking for auditreqests.
If given call is recieved it fill react based on given events of the Audit reqestor during the audit request process

Gemini

Gemini

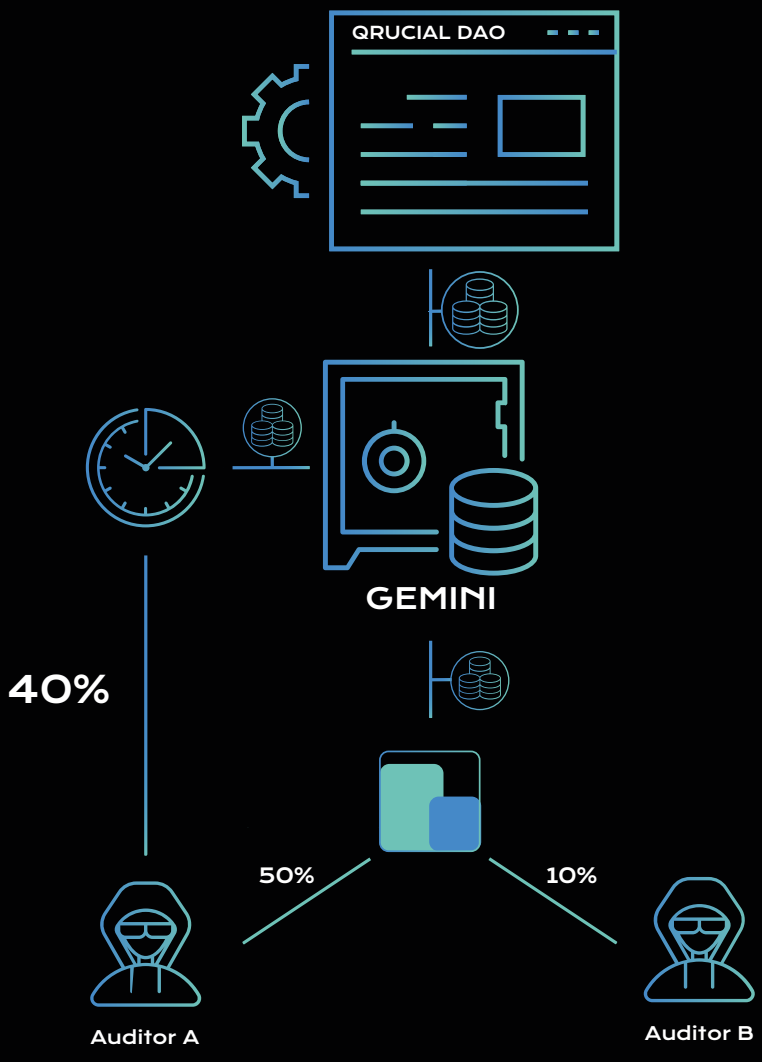
GeminiPallet handles the on chain economy.

It handles the balances of all market participants. It handles the monetary flow through a trustless transaction.
If an audit is requested a certain amount of QRD must be transfered to a smartcontract in a trustless transaction by the requestor.
When the transfer is recieved Gemini will be executed and calls PANDORAs execution. When the Security audits lifecycle enters the Manual audit phase Gemini will send a portion of the recived funds to the first of the autorized auditor. Auditors are chosen randomly. Auditors can become autorized by marking themselfes as open for work.

When the security audit report was publicated by the requestor or timelock the Auditreport is up for challenge. If AuditorB now finds aditional vulnerabilitys which are at least Medium he is rewarded proportionally to his findings by Gemini by transfering a portion of Requestors locked funds to AuditorB. In case no additional vulnerabilitys are found Gringots will release the full amount to AuditorA

Gemini logic is also responsible for the Security audit lifecylce:

- for minting the soulbound NFT
- updating its metadata when another auditor found an addidional CVE or CWE.
- finalizing the NFT marking a Report as final.



Perspective

Perspective

For Q3 2022 we plan to finalize our first milestone continuing with a proposal for a Milestone 02 within the Grants program.
Additionaly we will work on the integration of static analizers and fuzzers to QRUCIALDAOs Pandora.
Our aim is to bring provide web 3 builders with the nececary tools pice in mind.