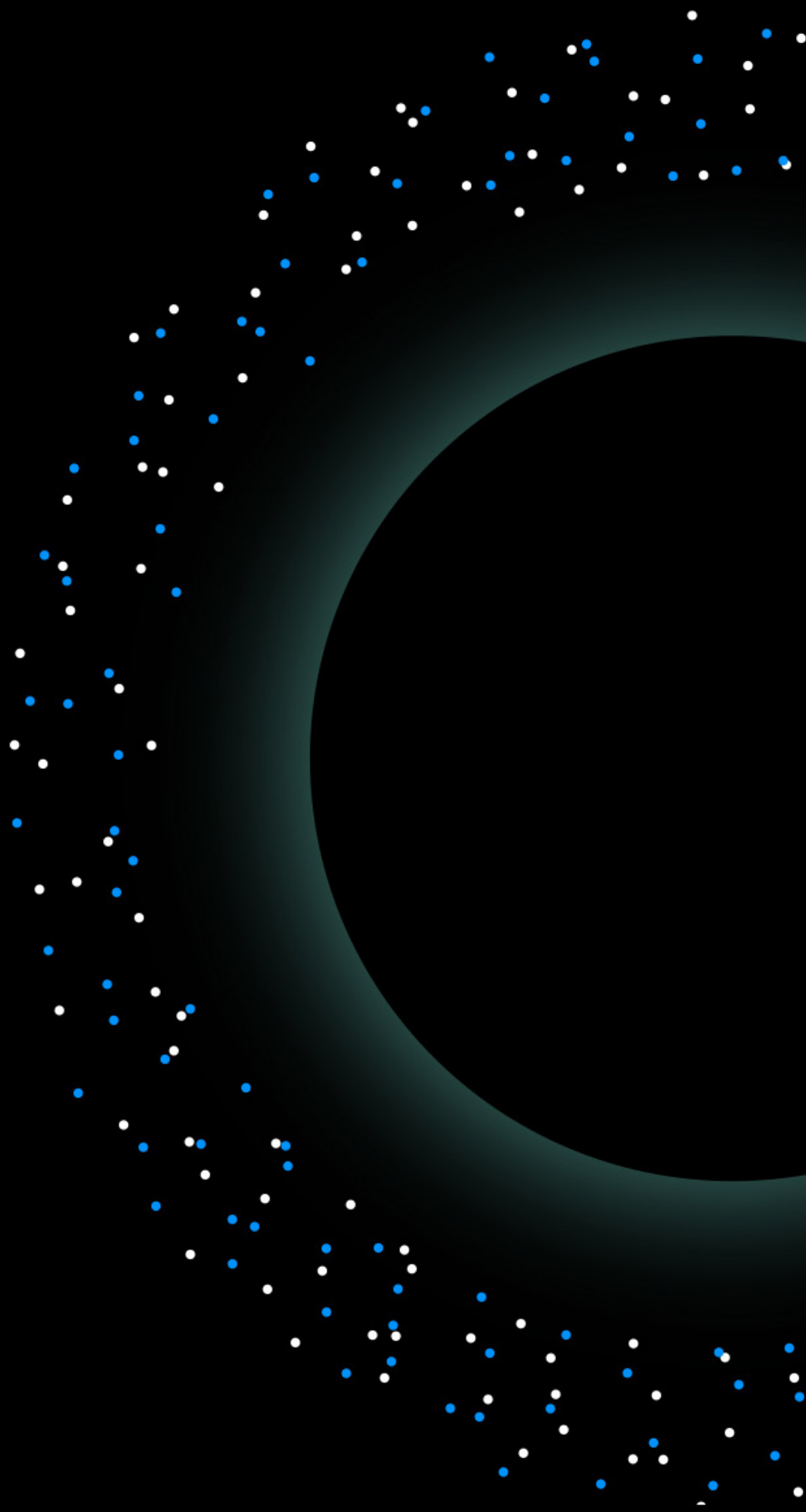
QRUCIAL DAO



QDAO Litepaper

Introduction

Qrucial DAO is a system for trustless audits, and certification using non-transferable NFTs, tooling and decentralized Consensus.

(We are working on creating a system and methodologies in web3 to make audits more transparent.)

High level summary

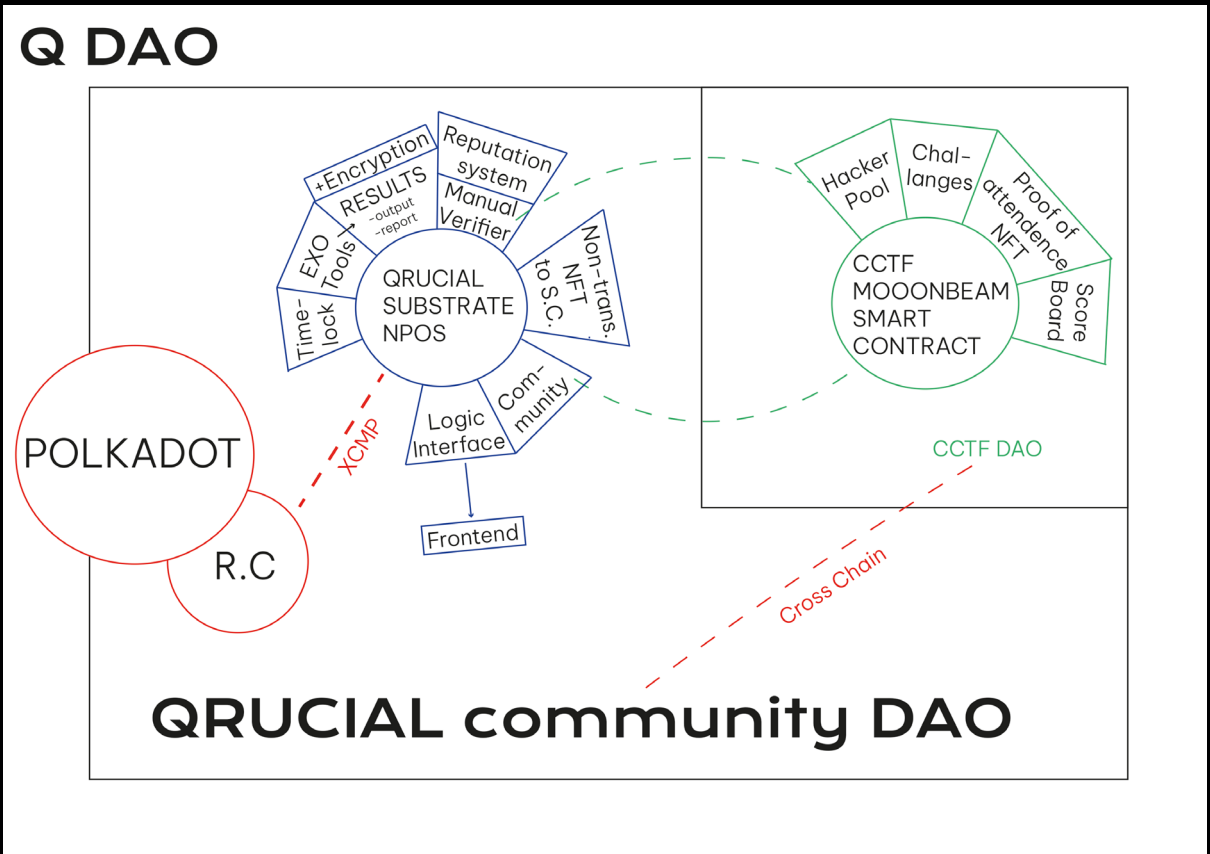
To us, it is ironic that web3 and trustless systems are trusting web2 auditors and legacy security companies to protect them from threat actors. This is the reason we want to build a system in which the community and the projects can trust that the work in fact has been done. Often, security audits of web3 projects are performed in a way that relies on in transparency and a blind trust in a company logo.

For example, no one verifies that the right tools have been used for the job or that the auditor performing the task is knowledgeable enough to perform the work professionally. Our project provides you a transparent on chain solution to this. We provide on chain tools which are developed by Qrucial as well as the community to test your project in a transparent and scalable way.

After this phase, you can choose from a pool of verified auditors who already proved their skills in on chain CTFs and through our on chain reputation system.

In the end you get the report as non-transferable NFT which is bound to the audited smart contract itself and therefore verifiable and transparent.

Topology


Q DAO
+Encryption
Reputation system
RESULTS
-output
-report
Manual Verifier
EXO Tools
Non-trans. NFT to S.C.
Time-lock
QRUCIAL SUBSTRATE NPOS
Logic Interface
Com-munity
Frontend
XCMP
POLKADOT
R.C
Hacker Pool
Chal-langes
Proof of attendence NFT
Score Board
CCTF MOOONBEAM SMART CONTRACT
CCTF DAO
Cross Chain
QRUCIAL community DAO

modules and extensibility

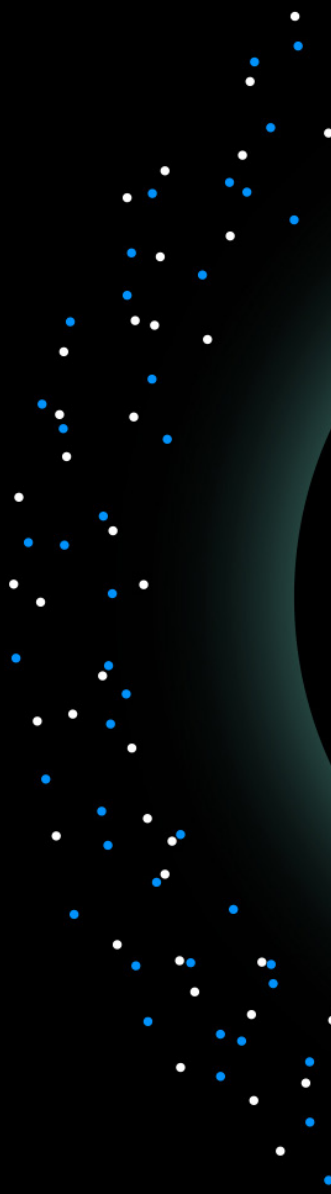
Exogenous security tooling

QDAO is a multichain solution which brings security services and tools to the blockchain. Such services include automated smart contract audits and tools like symbolic analyzers. We are the first connecting defensive as well as offensive security tool execution to the blockchain.

A Web3 Security Toolkit is to be built, and the tools inside will be executable on QDAO nodes. In the beginning, we will be focusing on auditing tools.

The tooling itself is bundled in a container and is being developed and maintained and voted on by qrucial and the DAO though the nominated proof of stake governance system. The distribution of the containers is done through decentralized means.

Runtime upgrades are used to update the toolbox on each node.



CCTF auditor pool

CTF players can solve challenges, so we have an on-chain record of individual players being able to solve rust reverse engineering or find and exploit vulnerabilities, for example.

Reputation system

The reputation system is there to reward good auditors and tool creators and weed out the bad ones.

Remediation strategies against malicious nodes

Qrucial Token is staked by the nodes. If they compute correctly, they get rewarded. If they misbehave, they get slashed. Randomized test are paid by the Network pool. In fact, it is not economically viable to target the nodes because the risk of being slashed outweighs the benefits by far.

Governance, staking, rewards

Core consensus will be using Nominated Proof of Stake. The beginning governance and the security toolkit will be controlled by QRUCIAL (e.g. we'll use sudo pallet). After the test period finishes, we remove the sudo pallet and let the system run on its own. Governance is to be pushed to the best/merit contributors and QRUCIAL control will be continuously taken away. Ultimately, the system should be working without QRUCIAL's interaction.

Why do we apply for the grant?

We apply for the grant to be able to build our project the right way from the start without compromising on our values by onboarding investors or build our idea to benefit centralized pump and dump ecosystems.

We want to build on substrate. Not only because it gives us new possibilities, but also because we see an overlap of values between Polkadot and Qrucial in building an unstoppable system. This will not be bound to the will of legislators and centralized single point of failure.

With QRUCIAL we aim to make the Polkadot ecosystem more secure.

Example Process:

Wallet x1 requests an audit of smart contract x2.

In the request wallet, x1, points to the deployed contract of x2 and pays a network fee.

When the execution is finished, the hash of the result gets written into a non-transferable NFT which is bound to the smart contract itself.

The data lies in an encrypted format and the assessment of the auditor.

The auditor pool will then verify the results, weeding out false positives.

Their assessment gets written into the same NFT and gets finalized.

The result can be encrypted and x1 will be able to access it.
The audit result is hashed, the hash will go on the non-transferable NFTs.

Report is still encrypted.
X1 can decrypt the report and make it public, we then verify our validator then verify that the hash is correct.

EXAMPLE

FOUNDING TEAM

FOUNDERS

Sebastian Kraus

Sebastian is the founder and strategic mind behind a multitude of companies. Ranging from the first sustainable real estate consulting company he founded at 22 while being bored in college to Elfzandtrollz a company which started as a joke and has since become a serious player in crypto marketing and QRUCIAL an information security company who stands for blockchain security without the bullshit and aims to bring more security to web3.

In 2016, he became interested in blockchain and hacking and has since refined his skills in the field.

David Pethes (six)

David is a web3 security expert and cofounded Qrucial which stands for Blockchain security without the Bullshit and founded CCTF the largest crypto hacking competition in the world. He has more than 10 years experience in IT penetration testing and got several global certifications. Since 2021 he is Regional Head Ambassador for Eastern Europe of Polkadot.

Since 2013 he is into blockchain and keeps improving his skills through related projects since then.