Cyberscope

Audit Report

AME Chain

December 2022

Github https://github.com/AME-AMEChain/amechain_quantum

Commit 7be7537d0ac00ea980075f27463b7b22c22fcd54

Audited by © cyberscope

Table of Contents

Contract Review

Github	https://github.com/AME-AMEChain/amechain_quantum
Commit	7be7537d0ac00ea980075f27463b7b22c22fcd54

Audit Updates

Initial Audit	17 December 2022

Files

Domain	File
	main.py
	qrn_api.py
	sqs_functions.py
	run-1.sh
	run-2.sh
	run-3.sh
amechain	amechain_node.service
	run_amechain_node.sh
	start_amechain_node_service.sh
	config/config.toml
	config/genesis.json
	config/permissions_config.toml
quantum	Pipfile
	Pipfile.lock
	quantum.service
	run_qrn_code.sh
	start_quantum_service.sh

Architecture

The repository contains two main sections. The quantum section that initiates and communicates with a Quantum service and the Amechain section that initiates an Amechain node.

The codebase does not contain the Amechain implementation but provides the scripts in order to launch it.

The Quantum main purpose is to provide real entropy to the Amechain blockchain. It opens a communication channel with the a SQS queue. Once it receives a message that forms the next entropy value, it injected it to the operating system via the file system.

Amachain utilizes the Amazon Simple Queue Service in order to proceed with the messaging architecture.

AME Chain Quantum Technology

AME chain uses quantum security technologies like quantum random number generators (QRNG) to secure its digital assets.

Quantum Random Numbers (QRN)

- AME chain uses QRNs in its cryptographic protocols to generate seeds, initial random values, nonces (salts), blinding values and padding bytes and perform hashing and encryption.
- The QRNs are created by single photon splitting. A laser produces a stream of the elementary particle, photon. The photons generated from the laser are used to generate the random numbers.

AME chain quantum certification

AME chain's QRNG technology has undergone various standardized tests conducted by TÜV Rheinland and has passed all of them. The test suite included:

- Entropy test
- Diehard tests
- NIST tests

Quantum Blockchain

Quantum blockchain is a term used to describe a potential future development in the field of blockchain technology that combines principles from both quantum computing and blockchain technology.

Quantum computers are a type of computer that use principles of quantum mechanics, such as superposition and entanglement, to perform certain types of computation more efficiently than classical computers. These computers have the potential to solve certain problems much faster than classical computers, but they also have some limitations and are still in the early stages of development.

Blockchain technology is a decentralized, distributed database that is used to record transactions and other information in a way that is secure, transparent, and resistant to tampering. It is the underlying technology behind cryptocurrencies like Bitcoin and has many potential applications beyond just finance.

A quantum blockchain would potentially combine the benefits of both quantum computing and blockchain technology, potentially allowing for more efficient and secure transactions and computations. However, the development of a functional quantum blockchain is still in the early stages and there are many technical and practical challenges that need to be addressed before it can become a reality.

The functionalities that the quantum provides are:

- Quantum Random Number Generator
- Quantum key distribution
- Quantum signatures
- Post-quantum cryptography
- Certifiable randomness
- Fast Byzantine Agreement
- Built-in zero-knowledge proof
- The No-cloning theorem
- The No-measurement rule

Layer 1 EVM Blockchain

A quantum blockchain is a type of blockchain technology that makes use of quantum computing principles and techniques to secure and validate transactions on the blockchain. AME Chain is a Quantum Secured Layer-1 EVM compatible Blockchain.

Quantum computers are highly powerful computing devices that are based on the principles of quantum mechanics. They are able to perform certain types of calculations much faster than traditional computers, and they have the potential to revolutionize many fields, including cryptography and blockchain technology.

In a quantum blockchain, the security of the network is enhanced by using quantum techniques to verify transactions and protect against tampering or fraud. This can be achieved through the use of quantum-resistant cryptographic algorithms, which are designed to be resistant to attacks by quantum computers.

It is important to note that quantum blockchains are still in the early stages of development and are not yet widely deployed. However, they hold promise as a potential future evolution of blockchain technology that could provide improved security and scalability for decentralized networks.

Proof Of Authority

AMA chains utilizes a group of nodes that are connected to each other using a peer-to-peer schema. Each node holds the entire blockchain state and executes the transactions. The nodes are validating the transactions.

Proof of Authority (PoA) is a type of consensus algorithm that is used to validate transactions and secure the AMA network. In a PoA network, a set of "validators" or "authorities" are responsible for validating transactions and adding them to the blockchain. These validators are chosen based on their reputation or trustworthiness, and they are typically identified by a unique digital signature or identity.

The PoA consensus algorithm is often used in the AMA blockchain network, where the validators are known and trusted parties. These validators are responsible for verifying transactions and adding them to the blockchain, and they are typically required to follow specific rules and guidelines to ensure the integrity of the network.

One advantage of the PoA consensus algorithm is that it can be faster and more efficient than other algorithms, such as Proof of Work (PoW) or Proof of Stake (PoS), because it does not require a large number of nodes to reach consensus on each block. This can make it well-suited for use in high-throughput applications or environments where low latency is important.

However, the PoA consensus algorithm is also less decentralized than other algorithms, as it relies on a small group of trusted validators to maintain the network. This can make it less resistant to censorship or tampering, and it may be less secure if a validator is compromised or becomes untrustworthy. As a result, PoA is often used in combination with other algorithms or security measures to ensure the integrity of the network.

Quantum random number generators consern

There are several potential issues or challenges associated with using Quantum random number generators (QRNGs).

Limited availability

QRNGs can be difficult and expensive to build, and they may not be widely available. This can limit their use in some applications.

Calibration and maintenance

QRNGs may require frequent calibration and maintenance to ensure that they are generating truly random numbers. This can be a time-consuming and resource-intensive process.

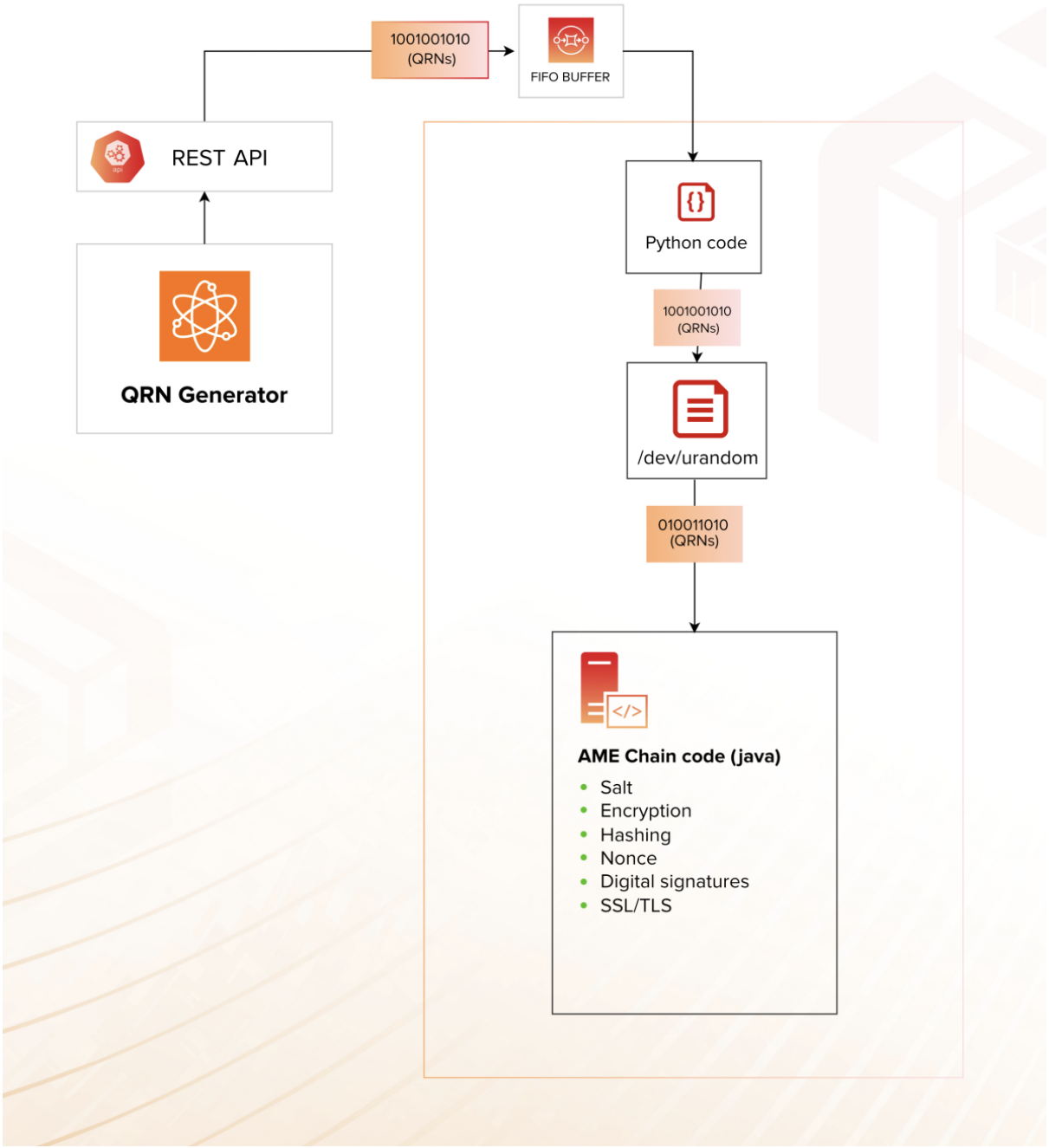
Security vulnerabilities

Like any computer system, QRNGs may be vulnerable to hacking or other security threats. This can be a concern in applications where the security of the generated numbers is critical.

Overall, while QRNGs have the potential to provide truly random numbers that are difficult or impossible to predict, they also come with a number of challenges and potential vulnerabilities that must be carefully considered when using them in various applications.

Quantom and Blockchain Integration

Random Numbers



Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope’s prior written consent. This report is not nor should be considered an “endorsement” or “disapproval” of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any “product” or “asset” created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment 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 Cyberscope’s position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope’s goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

The Cyberscope team

https://www.cyberscope.io