Built on the Cardano Blockchain

QuantumAI Whitepaper Cryptography and Security Protocol

QuantumAI is a tokenized computing security protocol with the ability to learn and create a Quantum resistant network through the Cardano Blockchain with its artificial intelligence computing system.

QuantumAI will use quantum computing for computation of machine learning algorithms. Thanks to computational advantages of quantum computing, QuantumAI can help achieve results that are not possible to achieve with classical computers. Quantum mechanics is a universal model based on different principles than those observed in daily life. A quantum model of data is needed to process data with quantum computing. Hybrid quantum-classical models are also necessary in quantum computing for error correction and correct functioning of the quantum computer.

Overview

Token Information

PolicyID:
354a6c0acd846b195768ead31c92693ad26d82ba013e7df5d9777081

Fingerprint: asset1nylmp38l5uq2szj6kguellahjvpsj6a7uhwxzs

Asset Name: QAI (514149)

Total Supply: 1,000,000,000
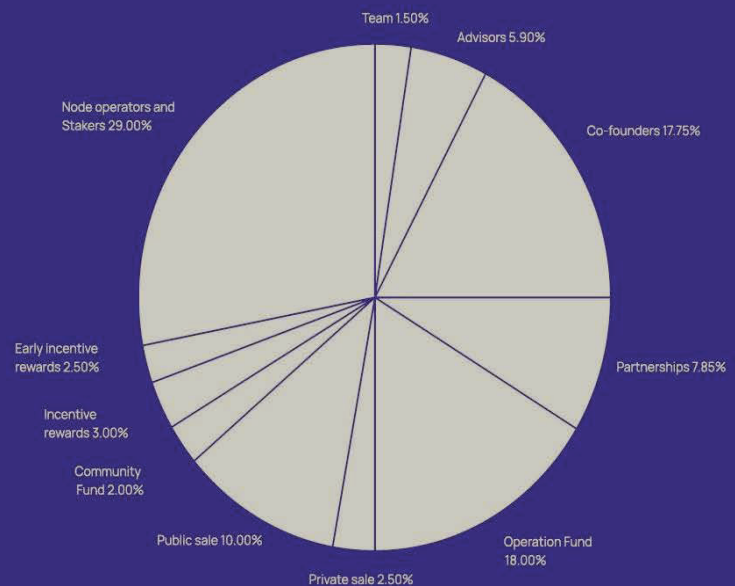**Max Supply: 1,000,000,000**
Website: QuantumAI.Computer

Token Economics Distribution

QuantumAI Token distribution.

Max Supply: 1 Billion Tokens

Lockup Terms (months)	Lock-up	Linear Unlock
Co-founders	18	24
Team	12	24
Advisors	12	24
Partnership	Allocated at the time of Partnership	
Operation Fund	6	72
Private sale	9	None
Public sale	None	None
Community Fund	24	48
Incentive rewards	None	None
Early staking rewards	None	None
Node operators and stakers	None	None

Pie chart labels:
- Team 1.50%
- Advisors 5.90%
- Co-founders 17.75%
- Node operators and Stakers 29.00%
- Partnerships 7.85%
- Early incentive rewards 2.50%
- Incentive rewards 3.00%
- Community Fund 2.00%
- Public sale 10.00%
- Private sale 2.50%
- Operation Fund 18.00%

What is cryptography and how is it used?

Cryptography is literally the art of "secret writing". It is used to secure communication by protecting the confidentiality and integrity of messages and sensitive data. Without it, anyone could read a message or forge a private conversation. Messages are made secret by transforming them from "plaintext" into "ciphertext" using a cipher and performing the process of encryption. Decryption turns scrambled and unreadable ciphertext back into plaintext.

When cryptographers talk about a "key", they are referring to a shared secret that controls the ability to hide and un-hide information. There are two types of cryptography that are often referred to as
"symmetric key" and "public key" cryptography:

1. In symmetric key cryptography, the same key is used for both encryption and decryption, and that key needs to be kept a secret by everyone who is sending and receiving private messages. The major difficulty of symmetric key cryptography is to provide the secret keys to legitimate parties without divulging the keys to eavesdroppers.

2. Public key cryptography[1] is more involved and complex. There are two keys, one for encrypting and another key for decrypting. The two keys are mathematically related, and only one key is intended to be kept a secret. Public key cryptography allows anyone to send an encrypted message, but only one person, with the private key, can decrypt the message. Public key cryptography can also be used for digital signatures where someone with a private key can sign a message that anyone can verify with the public key.[ZZDS14] Jiang Zhang and Zhenfeng Zhang and Jintai Ding and Michael Snook, Article 56, Quantum Authenticated Key.

Figure 1 - Cryptography Basics - Encryption and Decryption
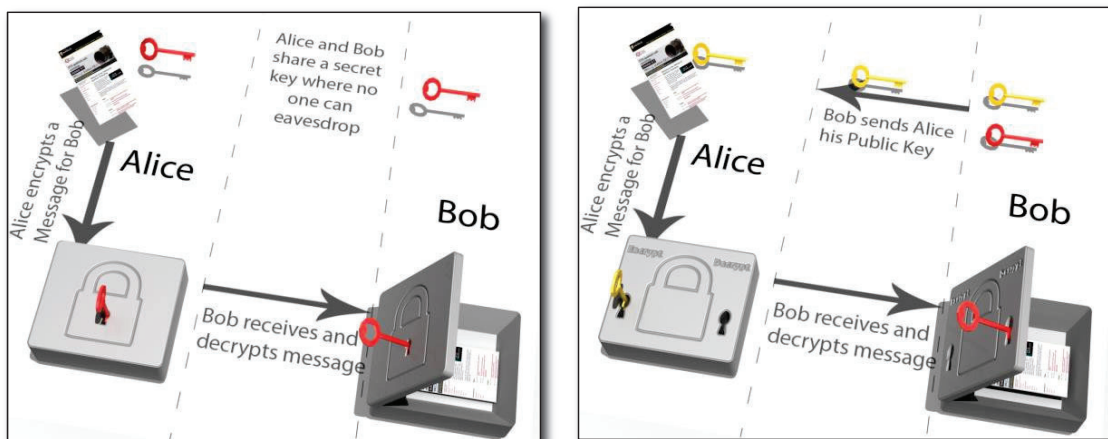
A - Symmetric Key Cryptography   **B - Public Key Cryptography**

---

[1] Also sometimes referred to as "asymmetric key cryptography"

[QPQ11] Markus Jakobi et al. Practical private database queries based on a quantum-key-distribution protocol. Phys. Rev. Article 83, 022301 (2011).

What is quantum computing?

Today's computers are governed by the laws of classical physics and Moore's law which states that, historically speaking, computers double their speed and capacity every 18 months because chip makers are able to squeeze twice as many transistors onto a computer chip. In order for these computing improvements to continue, placing more transistors on a computer chip means that transistors need to get smaller. But physics presents a natural barrier in that once technology has shrunk a transistor to the size of a single atom there are no more improvements to be made to transistor size. But what if the transistor could be replaced with a better technology, a technology that allows for a new paradigm of computing?

The laws of physics that can be seen, observed, and understood through experiences in everyday life are referred to as classical physics, and these laws govern the workings and computational capabilities of computers as they are known today. However, everything that is described by classical physics at a macroscopic level can be described by quantum physics at a nanoscopic level, and these different physical laws are known as quantum mechanics. In the past few decades, researchers have realized that the ways in which the laws of physics allow different things to happen to very small objects can be harnessed to make computers out of novel materials, with hardware that looks and behaves very differently from the typical classical computers that people use in their homes and offices today. [GIS02] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden. Quantum cryptography. Review of Modern Physics Pages - 74, 95-145 (2002).

Quantum computers, obeying the laws of quantum mechanics, can calculate things in ways that are unimaginable from the perspective of people's regular day-to-day experiences.

In classical computing, information is stored in fundamental units called bits, where a bit can hold a binary digit with the value of 0 or 1. In quantum computing, the fundamental unit can hold both a 0 and a 1 value at the same time; this is known as a superposition of two states. These quantum bits are known as qubits and measuring the state of a qubit causes it to select or "collapse into", being a 0 or a 1. Interestingly, if you prepare a string of qubits of the same length in the same way, the resulting bit string will not always be the same. This gives quantum computers an advantage over classical computers in that they can perform very rapid parallel computations. [Gro96] Lou Grover. A fast quantum mechanical algorithm for database search. Proceedings, 28th Annual ACM Symposium on the Theory of Computing, page 212, 1996.

Quantum mechanics has some novel properties that researchers have realized can be harnessed to make quantum computers that behave very differently than the classical computers commonly used today. Using these novel quantum properties, a quantum computer is able to solve certain problems like searching and factoring much faster than the time it would take a classical computer, with the best known algorithms, to solve the same problem. [QPQ11] Markus Jakobi et al. Practical private database queries based on a quantum-key-distribution protocol. Phys. Rev. Article 83, 022301 (2011).
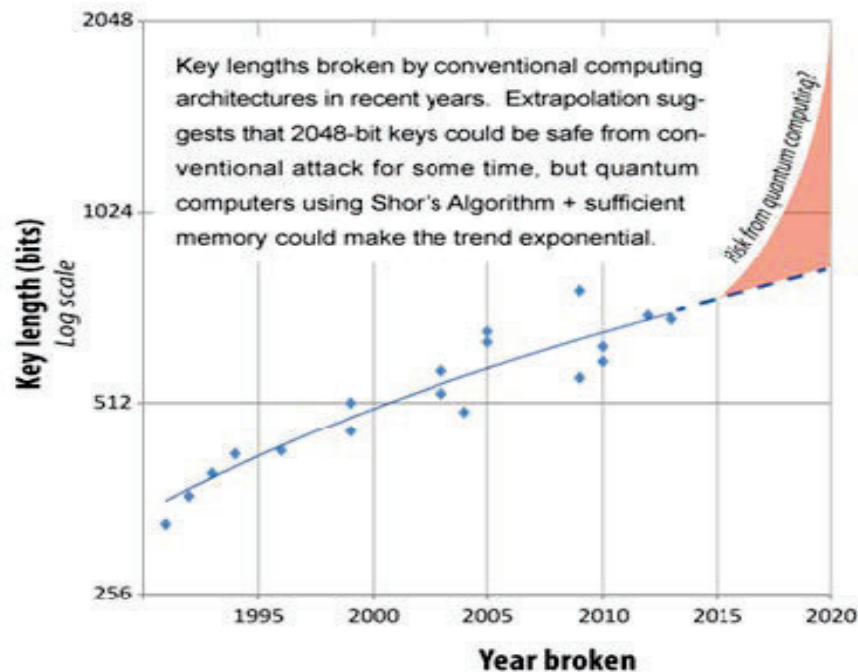

Figure 2 - Breaks of the RSA cryptosystem in recent years using conventional computation.

2 Moore's law is not an actual law of physics, but instead a general observation and prediction made by a co-founder of Intel that describes the speed in which computing has matured. [GIS02] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden. Quantum cryptography. Review of Modern Physics Pages - 74, 95-145 (2002).

Coding

What is Qis|krypt?

Qis|krypt is a software suite of protocols of quantum cryptography and quantum communications, as well, other protocols and algorithms, built using IBM's open-source Software Development Kit for quantum computing Qiskit. [IBM] Rúben Barreiro - open source coding - https://qiskrypt.github.io/

What is Plutus?

Plutus is the smart contract platform of the Cardano blockchain. It allows you to write applications that interact with the Cardano blockchain. [Cardano] source -https://developers.cardano.org/docs/smart-contracts/plutus/

How we will implement Qis|krypt with Plutus?

Since Plutus allows you to write applications that interact with the Cardano blockchain, we will use this feature to create the QuantumAI Protocol and bring together the world of QuantumAI and Blockchain technology. Plutus allows our team to create customized smart contracts and through the Plutus Playground and together with EVM and KEVM virtual machine environments, the Marlowe and Marlowe Playground. These will all be necessary to implement the Qis|krypt coding into our smart contract. We will also take a look at future plans for greater programming language support on Cardano, and what efforts can be made in scope of this area.

A Plutus contract is a Haskell program that will be partly compiled to on-chain Plutus Core code and partly to off-chain code. Plutus contracts contain pieces of code that run on the blockchain, as well as off-chain code that runs on the user's machine. While the on-chain component of Plutus smart contracts compiles in the Plutus compiler, the off-chain elements are compiled by the Glasgow Haskell Compiler (GHC).[Cardano] source -https://developers.cardano.org/docs/smart-contracts/plutus/

Our team will be using Plutus to write a smart contract for your DApp or DeFi solution, Cardano engineers at IOHK have built the Plutus Playground for us to work with. This is a lightweight browser-based development environment that allows engineers to write and simulate their smart contracts before they are compiled to a mainnet environment.

Our Goal

Our goal is to protect and secure the worlds data at the tip of its fingers. We hope the QuantumAI Security Protocol will change the way you use the Internet & IoT.

QuantumAI is a Community based Token project and is open any and all ideas to make the future of cryptocurrency easier to understand and more secure. QuantumAI is developing a secure and decentralized governance model. A model to give everybody a voice, and control over the future development of the platform and the applications and services that emerge from it in the most secure way possible.

The Mission

The mission is to revolutionize the world of finance as we know it. Bringing together Human and QuantumAI capabilities to help protect assets, predict market trends, secure data and finances from Quantum hacks with our QuantumAI Secuirty Protocol.

The Vision

Our vision of QuantumAI Token is to play a big role in the future of our financial society. We will work to collaborate Humans and AI technologies to make our human lives easier in all aspects of life. This will include Agriculture, Business & Finance, AI Ads and much more.

We hope this will be one of the most comprehensive overviews of Cardano's smart contract environment by a non-Cardano entity and we hope it brings deep value to our community. It will all start with Plutus then IBM's open source coding will be added to the smart contract as we develop further.

This whitepaper is an updated one to our previous whitepaper and briefly explains how we will use our token and build on top of the previous whitepaper using the Cardano Blockchain and its Native Token QuantumAI to implement the QuantumAI protocol. - QuantumAI Team.

We are in no way or form affiliated, associated or in partnership with any other Quantum AI projects or company. All references, sources and citations are listed below.

References & Citations

(Source of previous whitepaper is on our GitHub, references & citations: https://github.com/C-QuantumAi/QuantumAI/blob/main/QuantumAI-Whitepaper.pdf)

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies.
NOTE: While any hyperlinks included in this clause were valid at the time of publication, QuantumAI cannot guarantee their long term validity.
[ZZDS14] Jiang Zhang and Zhenfeng Zhang and Jintai Ding and Michael Snook, Article 56, Quantum Authenticated Key.
[QPQ11] Markus Jakobi et al. Practical private database queries based on a quantum-key-distribution protocol. Phys. Rev. Article 83, 022301 (2011).
[GIS02] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden. Quantum cryptography. Review of Modern Physics Pages - 74, 95-145 (2002).
[Gro96] Lou Grover. A fast quantum mechanical algorithm for database search. Proceedings, 28th Annual ACM Symposium on the Theory of Computing, page 212, 1996.
[QPQ11] Markus Jakobi et al. Practical private database queries based on a quantum-key-distribution protocol. Phys. Rev. Article 83, 022301 (2011).
[GIS02] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden. Quantum cryptography. Review of Modern Cryptography Pages - 74, 95-145 (2002).
[IBM] Rúben Barreiro - open source coding - https://qiskrypt.github.io/
[Cardano] source - https://developers.cardano.org/docs/smart-contracts/plutus/