QuantumCoin: The Vision

Authors: The QuantumCoin Community

Publication Date: September 2021

Revision 5: March 2026

Contents

Disclaimer

QuantumCoin is a community driven project. All visions and projects are aspirational. There is no value attributed to anything. All projects are community driven and there is no guarantee of delivery. QuantumCoin is not intended to be, or to be the subject of, an investment opportunity, investment contract, or security of any type.

Background

We are in an age of decentralization, wherein previously centralized approaches in areas like domain name systems, trading exchanges, finance, storage and computing are being slowly replaced and/or augmented by decentralized solutions. We are just at the tip of the iceberg in the era of decentralization. This paper attempts to explore the various possibilities that can be opened up by decentralization. Note that the goal is not to decentralize just for the sake of decentralization, but rather to solve real-world problems.

QuantumCoin

QuantumCoin is a combination of decentralized networks, smart contracts and decentralized apps (DAPPS), that form the backbone of this decentralization initiative. The primary component of QuantumCoin is a quantum-resistant blockchain that supports smart contracts, satellite chains and is scalable in the number of transactions. QuantumCoin aspires to be a combined multi-fork of Bitcoin, Ethereum, Dogecoin and DogeP tokens. The whitepapers go over the technical details of this blockchain but in this vision paper, we shall see a high-level overview.

Community Driven

The QuantumCoin project is entirely community driven. There is no centralized owner or entity that controls development of the project. The community itself is open and decentralized. Anyone can contribute to the project. The development community itself are from around the world with no single point of governance. The vision of this community is that even many decades or a century from now, the project development should continue without involvement of any centralized entity.

QuantumCoin Blockchain

A robust and scalable blockchain is required to serve as the backbone for executing the vision of QuantumCoin, upon which other building blocks can be developed.

Quantum Resistance

There is also a specific reason why blockchains must be quantum-resistant. Due to the advent of quantum computers, there is an imminent threat to existing asymmetric encryption systems like RSA, ECDSA that are used to secure almost all the current blockchains. Using algorithms like Shor's (rapid integer factorization) and Grover's (quadratic mining speedup on Proof of Work systems), Quantum Computers can break current blockchains in different ways.

Bitcoin, Ethereum and Dogecoin are three of the largest and popular blockchains. They are vulnerable to quantum computers because of the above reasons. One of the visions of the QuantumCoin is that it should secure these three blockchains from quantum computer threats. Security itself evolves over time, hence no algorithm should be deemed future proof, including current quantum-resistant algorithms. However, from the current landscape, quantum computers are a viable threat to blockchains.

Hence the vision is to multi-fork Bitcoin, Ethereum, Dogecoin and DogeP to form a combined blockchain that is resistant to currently known quantum computer threats. The goal is also to keep improving it based on the changing security landscape. The actual technical details of the quantum resistance are published in the Quantum Resistant Blockchain whitepaper.

Consensus System

The blockchain uses a 3 phase pBFT proof-of-stake consensus that provides immediate finality after the block is mined. The relevant trade-offs made to support immediate finality are increase in wait times such as for offline validators & block proposers, to mitigate liveness problems, within the limits of the FLP (Fischer, Lynch, and Paterson) Impossibility theorem.

Decentralization

To enable adoption and wider decentralization, the new blockchain may also fork off other blockchain, giving existing users of other blockchain a stake in the QuantumCoin system.

One of the important goals of the QuantumCoin blockchain ecosystem is that even if the current decentralized community stops contributing, the community should grow and contribute forever, to keep the ecosystem running. This can only be achieved with wide adoption of the blockchain ecosystem.

Token System

The blockchain also supports both fungible and -non-fungible tokens, similar to ERC20 and ERC721 on the Ethereum network. Token support is an important requirement of modern blockchains.

Doge Protocol Token

Doge Protocol Token (dogep) was released in September 2021, fairly on the Ethereum blockchain, with 100% of liquidity added to UniSwap and SushiSwap. A cap of 0.99% tokens per account was also enforced. The liquidity was also locked in UniCrypt till 2050.

Satellite Chains

Satellite Chains are other blockchains of the protocol that support other use cases like audio & video streaming, file storage, key-value systems etc. Not to be confused with "side chains", these satellite chains are meant to be loosely coupled with the main blockchain and expose a different set of capabilities. Satellite chains may also use a different coin but the goal is to integrate into the main chain. More on this in a follow-up whitepaper.

Key-Value Store

The key-value store is a decentralized store that makes it easy to build DAPPS, by allowing to store and retrieve arbitrary JSON using REST APIs. This key-value store needs to be enabled as a satellite chain in the QuantumCoin ecosystem. The APIs need to be published as an Open API swagger spec allowing a variety of clients to be created for various programming languages and platforms.

File Storage

This satellite chain provides a decentralized API to store and retrieve any binary data using REST APIs. This is different from other decentralized storage systems like FileCoin, in that the data interface is REST API and this store may use one or more of the other blockchains as a conduit.

Streaming

This satellite chain can enable audio and video streaming akin with an ecosystem consisting of content creators, distributors, and enablers, to keep the ecosystem running. By "enablers", we mean one or more of (but not limited to) node operators and validators or miners; in other words, the actors that provide the infrastructure to run the streaming satellite chain.

Other Satellite Chains

- Decentralized Domains
- Decentralized Chat / Instant Messaging
- Decentralized File Sharing
- Decentralized Search

Decentralized Applications

The following section lists various DAPPS that can be built using the QuantumCoin, as a community driven initiative.

Decentralized Classifieds

A simple use case for decentralization is classified ads, based on a bidding model.

Decentralized Book Database (ISBN)

Instead of ISBN, a decentralized approach to book identification can be created. Anyone would be able to register their book information, use in point of sales systems for billing and also view a list of such registered books transparently.

Decentralized NFT Marketplace

An NFT marketplace can be added as part of the QuantumCoin ecosystem. Anyone is able to list for sale eBooks, Articles, Paintings etc. and customers are able to buy

them. Various ways of selling like master resale rights, PLR (public label rights) etc. can be offered.

Decentralized Ads

The internet AD market is currently a duopoly with two major centralized vendors offering AD functionality. This dapp can provide a marketplace and ad distribution network that can connect publishers, advertisers and audiences.

Decentralized Finance (DEFI)

Decentralized Finance is one of the most important applications of blockchains. Instead of building DEFI apps from the ground up, the QuantumCoin vision is to work with existing DEFI systems and have them run on the QuantumCoin blockchain.

Decentralized Exchanges (DEX)

Decentralized Exchanges provide a way to swap tokens created on the blockchains, in a decentralized fashion.

About this paper

This paper details the vision of the QuantumCoin community. There is no guarantee of execution or time of execution of any of the items called out in this vision document. QuantumCoin is a community-driven initiative.

References

1. Decentralization: https://en.wikipedia.org/wiki/Decentralization

2. DEFI: https://ethereum.org/en/defi/

3. ISBN: https://en.wikipedia.org/wiki/International_Standard_Book_Number

4. Ethereum: https://ethereum.org/en

5. DEX: https://en.wikipedia.org/wiki/Decentralized_exchange

6. ISBN: https://en.wikipedia.org/wiki/International_Standard_Book_Number

7. QuantumCoin: https://QuantumCoin.org/