Quantum Coin: The Vision

Authors: The Quantum Coin Community

Publication Date: September 2021

Revision 3: October 2024

Contents

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.

Quantum Coin

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

Community Driven

The Quantum Coin project will entirely be community driven. There will be no centralized owner or entity that will control development of the project. The community itself will be open and decentralized. Anyone can contribute to the project. The development community itself will be 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.

Quantum Coin Blockchain

A robust and scalable blockchain will be required to serve as the backbone for executing the vision of Quantum Coin, 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 above reasons. One of the visions of the Quantum Coin is that it should secure these three blockchains from quantum computer threats. Security itself will evolve over time, hence no algorithm should be deemed future proof, including current quantum-resistant algorithms. However, but 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 will be published in the Quantum Resistant Blockchain whitepaper, but at a high level, one or more of the known post-quantum digital signature algorithms like Dilithium, Falcon or Rainbow will be used to secure this blockchain.

Consensus System

The blockchain will also need a consensus system that supports sharding (for scalability in terms of the number of transactions per second) and satellite chains (see the section below). At this point, various consensus systems including Proof-of-Stake (PoS), Delegated Proof-Of-Stake (DPoS), Hybrid model (PoS + PoW) are being evaluated. A follow-up whitepaper will detail the consensus model that will be used for the blockchain.

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 Quantum Coin system.

One of the important goals of the Quantum Coin 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. More details on this will be provided in a follow-up whitepaper.

Token System

The blockchain will also support 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.

This token will be used for various DAPPS and also give the holders a stake in the upcoming Quantum Coin Blockchain and also potentially stake into upcoming satellite chains (see the section on satellite chains below).

A snapshot of a given block will be taken on the target blockchain mainnet and holders of dogep as of that block will be given a stake in the Quantum Coin blockchain. Stakes in the satellite chain may be based on a different block in the future. Prior announcements and details will be given well in advance on the block number and also ways to get the coins in the Quantum Coin blockchain.

Since the other blockchain mostly is not quantum resistant as of the time of writing this vision paper, there will be a cutoff date for token holders to claim their stake in the blockchain. Now having this cutoff date can make the Quantum Coin blockchain and satellite chains vulnerable to quantum computers. The cutoff dates will be given well in advance.

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 will be loosely coupled with the main blockchain and expose a different set of capabilities. Satellite chains may

also use a different coin but will integrate into the main chain. More on this in a follow-up whitepaper.

Key-Value Store

The key-value store will be a decentralized store that makes it easy to builds DAAPS, by allowing to store and retrieve arbitrary JSON using REST APIs. This key-value store will be enabled as a satellite chain in the Quantum Coin ecosystem. The APIs will 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 will provide 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 will 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

As part of the ecosystem, the Quantum Coin community will also consider adding satellite chains like:

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

Decentralized Applications

The following section lists various dapps that will be built using the Quantum Coin. They will be community driven.

Decentralized Classifieds

A simple use case for decentralization is classified ads, based on a bidding model. This will be one of the first dapp that will be built using the Quantum Coin.

Decentralized Book Database (ISBN)

Instead of ISBN, a decentralized approach to book identification will 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 Quantum Coin ecosystem. Anyone will be able to list for sale eBooks, Articles, Paintings etc. and customers will be able to buy them. Various ways of selling like master resale rights, PLR (public label rights) etc. will be offered.

Decentralized Ads

The internet AD market is currently a duopoly with two major centralized vendors offering AD functionality. This dapp will provide a marketplace and ad distribution network that will 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 Quantum Coin vision is to work with existing DEFI systems like Aave, Compound etc. and have them run on the Quantum Coin blockchain. Note that this is only a vision at this point and there has been no communication with any of the Aave or Compound community or team.

Decentralized Exchanges (DEX)

Decentralized Exchanges provide a way to swap token created on the blockchains, in a decentralized fashion. Similar to the DEFI vision, the Quantum Coin vision for DEX is to work with popular DEX communities like SushiSwap, UniSwap and have them run on the Quantum Coin blockchain. Note that this is only a vision at this point and there has been no communication with any of the SushiSwap or UniSwap community or team.

About this paper

This paper details the vision of the Quantum Coin community. While we strongly believe the community will execute this vision on time, there is no guarantee of execution or time of execution of any of the items called out in this vision document. Quantum Coin is a community-driven initiative. Follow-up whitepapers will provide technical details when items called out in this document are being executed.

Addendum

"Quantum Coin" and "Quantum Coin Community" were previously known under the monikers "Doge Protocol" and "Doge Protocol Community" respectively.

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. NIST Post Quantum Round 3 submissions: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions
5. Crystals Dilithium pq digital signature algorithm: https://pq-crystals.org/
6. Falcon pq digital signature algorithm: https://falcon-sign.info/
7. Rainbow pq digital signature algorithm: https://www.pqcrainbow.org/
8. Ethereum: https://ethereum.org/en
9. DEX: https://en.wikipedia.org/wiki/Decentralized_exchange
10. ISBN: https://en.wikipedia.org/wiki/International_Standard_Book_Number
11. Aave: https://aave.com/
12. Compound: https://compound.finance/
13. SushiSwap: https://sushi.com/

14. UniSwap: https://uniswap.org/

15.Quantum Coin: https://QuantumCoin.org/