Doge Protocol: The Vision

Authors: The Doge Protocol Community

Publication Date: September 2021

Revision : June 2023

Contents

Community Project

The Doge Protocol project is entirely community driven. All visions and projects in Doge Protocol are aspirational. There is no value attributed to anything. All Doge Protocol projects are community driven and there is no guarantee of delivery.

There is no centralized owner or entity that controls the development of the project. The community itself is open and decentralized. Anyone can contribute to the project. The development community itself is 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. Note that this is only a community vision and there is no guarantee that the projects listed in the vision will be developed. It is left up to the community to develop the projects. There is also no value attributed to any of these projects or coins or tokens or blockchain.

Background

We are in an age of decentralization, wherein previously centralized approaches in areas like domain name systems, 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.

Solving Real World Problems

Some of the pressing real-world problems that is a community aspiration to solve are:

1. Affordable Education
2. Affordable Healthcare
3. Affordable Clean Water
4. Affordable Clean Energy

The Doge Protocol Blockchain is only a base that can help solve these problems.

Doge Protocol

Doge Protocol is a combination of decentralized networks, smart contracts and decentralized apps (dapps), that form the backbone of this decentralization initiative. The primary component of Doge Protocol would be a quantum-resistant blockchain that supports smart contracts, satellite chains and is scalable in the number of transactions. Doge Protocol vision is also to be a combined multi-fork of Bitcoin, Ethereum, Doge Coin and DogeP tokens.

Doge Protocol Blockchain

A robust and scalable blockchain would be required to serve as the backbone for executing the vision of Doge Protocol, 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 Doge Coin are three of the largest and popular blockchains. They are vulnerable to quantum computers because of above reasons. One of the visions of the Doge Protocol 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, but from the current landscape, quantum computers are a viable threat to blockchains.

Hence the vision is to multi-fork Bitcoin, Ethereum, Doge Coin 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 woulbe 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 would be used to secure this blockchain while Kyber would be used to secure communication.

Consensus System

The blockchain would 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-Execution (PoE), Proof-of-Stake (PoS), Hybrid model (PoS + PoW) are being evaluated.

Decentralization

One of the important goals of the Doge Protocol blockchain ecosystem is that even if the current decentralized community stops contributing, the community should grow and contribute forever. There should be no single point of failure or ownership or control.

Satellite Chains

Satellite Chains are other blockchains of the protocol that support other use cases like gaming, VR/AR etc. Not to be confused with "side chains", these satellite chains would need to be loosely coupled with the main blockchain and expose a different set of capabilities. Satellite chains may also use a different coin but would need to integrate into the main chain. More on this in a follow-up whitepaper.

As part of the ecosystem, some more satellite chains ideas are:

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

Decentralized Classifieds

A simple use case for decentralization is classified ads, based on a bidding model using blockchain as an enabler.

Decentralized Book Database (ISBN)

Instead of ISBN, a decentralized approach to book identification would need to 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 Ads

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

About this paper

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

Appendix

1. Decentralization: https://en.wikipedia.org/wiki/Decentralization
2. ISBN: https://en.wikipedia.org/wiki/International_Standard_Book_Number
3. NIST Post Quantum Round 3 submissions: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions
4. Crystals Dilithium pq digital signature algorithm: https://pq-crystals.org/
5. Falcon pq digital signature algorithm: https://falcon-sign.info/
6. Ethereum: https://ethereum.org/en
7. ISBN: https://en.wikipedia.org/wiki/International_Standard_Book_Number
8. Doge Protocol: https://dogeprotocol.org/