CS6858 Distributed Trust Blockchain: Write-Up Assignment

Prasanna Bartakke
EE19B106

Dogecoin 

Governance model

Open-source Community Mode.

Dogecoin is an open-source project. Many organizational contributors and individuals form the direction of the various projects of the Dogecoin blockchain and ecosystem.

Access and Control Layer

Public Blockchain

No one or no corporate entity owns the Dogecoin blockchain; it is open-source, permissionless, decentralized and peer-to-peer. The Dogecoin network is controlled by the network of nodes through which it operates, and anyone can run a node. Some nodes also mine Dogecoin to confirm the transactions up to the next block and add the next block.

Network Topology

Decentralized (a distributed P2P network which enables direct transactions between every node within the network)

Dogecoin nodes function via a decentralized consensus mechanism to prevent malicious actors from gaining control over the network. This decentralized control via the nodes ensures that Dogecoin transactions are securely processed peer-to-peer without the need of a central controlling party.

Consensus Mechanism

Proof of Work

Dogecoin is based on the code of Bitcoin, the first cryptocurrency. Dogecoin is a hard fork of the now-defunct Luckycoin, a hard fork of Litecoin (LTC). It uses a Scrypt-based

consensus mechanism like Litecoin. Dogecoin's implementation differs from Litecoin by several parameters. Dogecoin's block time is 1 minute compared to 2.5 minutes for Litecoin. Scrypt is used in Dogecoin's Proof-of-Work algorithms, which prevents miners from using ASICs, the specialized equipment used in Bitcoin mining.

The network participants of Dogecoin use their computing power to secure the network and enable block creation while verifying transactions similar to Bitcoin. The difference is that Dogecoin has a light architecture, enabling DOGE to process transactions at a faster rate than Bitcoin. Dogecoin is mined with computational power used by the network participants to generate new blocks and validate the transactions by solving mathematical puzzles. The block generation reward received by miners is 10,000 DOGE.

Cryptocurrency: Native Assets

Only native cryptocurrency

Dogecoin is primarily an online blockchain-based currency for payments and instant transactions. Users can send and receive DOGE with their Dogecoin (DOGE) wallets within seconds and with minimal transaction fees. The block reward given to miners is 10000 DOGE per block.

Tokenisation

No Tokenisation present

Tokenization refers to the process of converting tangible and non-physical assets into blockchain tokens. This is not supported by Dogecoin.

Asset Supply Management

Unlimited - Deterministic

Initially, Dogecoin's supply was limited to 100 billion DOGE. However, the developers changed the monetary policy of Dogecoin shortly after the initial release of DOGE. The limit on the amount of DOGE was removed, creating an infinitely inflationary supply.

It is estimated that the circulating supply will double in 26 years, and currently, there is no hard limit to the total supply. The inflation rate of Dogecoin decreases compared to the total supply. It has a diminished inflation rate because it has a fixed yearly issuance of 5 billion coins. This property makes Dogecoin the perfect candidate to be used as a currency.

Dogecoin is not meant to be hoarded; hoarding is a significant barrier to a cryptocurrency being used as an actual currency. Dogecoin will have a much more valuable and practical place in the economy than other cryptocurrencies, as most other cryptocurrencies remain unspent.

Transaction Capabilities – Transaction Model

UTXO – Unspent Transaction Output

A UTXO chain is a blockchain using the unspent transaction output accounting method. UTXO is the original form of cryptocurrency blockchain, first introduced in the Bitcoin whitepaper by Satoshi Nakamoto. In a UTXO-based ledger, there are no accounts or wallets, at least not at the protocol layer.

Instead, transactions are composed of inputs and outputs, and the coins are stored as a list of unspent transaction outputs (UTXOs).

Security & Privacy – Data Privacy

No data obfuscation

Every transaction on the blockchain is public. Given a public wallet address, anyone can see any Dogecoin transaction that has ever been made from the address. Thus it is necessary not to claim a public address to remain anonymous.

If one has a hardware wallet, it is recommended to use new randomized public addresses for each transaction for anonymity and privacy reasons.

The Dogecoin network relies on the miners to secure the blockchain and validate transactions. PoW rules are enforced through full nodes, and miners use computational power to solve mathematical equations. Solving mathematical puzzles generates a new block, verifying and permanently recording transactions. Miners are rewarded if they publish the correct block.

Is it programmable?

No, Dogecoin does not support smart contracts.

Dogecoin cannot interact with smart contracts directly. Given that it operates on its own chain, the coins can be wrapped so that they can be locked into a state that is interoperable with a contract until it is later released. The Ren Project has enabled Dogecoin (renDOGE) to be used on the Ethereum blockchain and access the Defi network.

Give your assessment on the potential of the platform.

The Dogecoin crypto network is a popular starting point for new investors entering the wide cryptocurrency world. Dogecoin has developed a large online following and a

significant market capitalization. Dogecoin presents itself as a fun and friendly cryptocurrency. Its leading role in popularizing meme coins has helped develop a marketplace for assets driven by and for the internet culture. Dogecoin was increasingly transacted in online cryptocurrency marketplaces by people looking for an unconventional currency for their portfolios. Initially, Dogecoin experienced explosive growth resulting in it briefly exceeding the combined trading volume of all other cryptocurrencies, including Bitcoin, in Jan 2014. While the project may have been launched as a joke, it proves that the value of memes is an intimidating proposition for the emerging digital economy.

Dogecoin has emerged as a popular method for tipping online content creators with micro-donations and supporting charitable organizations rather than being used as a store of value or as a platform for building blockchain-based applications. The Dogecoin Foundation is a non-profit company through which the Dogecoin community has historically carried out charitable campaigns.

Pros:

1. Faster confirmation time for completed transactions.
2. Minimal transaction fee.
3. Network of a devoted and friendly community of creators and followers,
4. Low value helps in micro tipping and as a gaming currency.
5. Widely accepted and endorsed by famous people like Elon Musk on Twitter.

Cons:

1. The mining of Dogecoin is non-profitable because the value of the mining reward is relatively low.
2. An inflationary currency which limits the potential of Dogecoin.
3. No support for smart contracts resulting in limited functionality.
4. Considered less secure than other popular cryptocurrencies.

Dogecoin is not intended to be an investment or store of value. Instead, Dogecoin's primary practical function has been as a form of tipping (especially in online settings). People donate DOGE to online content creators for funny, informative, or otherwise noteworthy content. Tipping content creators on Reddit, Twitter, and Twitch is another example of cryptocurrency's entanglement with social media and widespread internet culture.

References:

1. https://dogecoin.com/dogepedia/#documentation
2. Dogecoin - Wikipedia. https://en.wikipedia.org/wiki/Dogecoin
3. What is Dogecoin? And how does DOGE work? (2022 edition) - Kriptomat. https://kriptomat.io/cryptocurrencies/dogecoin/what-is-dogecoin/
4. What Is Dogecoin? The DOGE Crypto Network | Gemini. https://www.gemini.com/cryptopedia/what-is-dogecoin-mining-doge-crypto