Hedera HBAR: A decentralized security approach Based on Blockchain with NFT Transaction

Abstract:

Hedera is a public distributed ledger and governing body built from the ground-up to support to support new and existing applications running at web scale. Developers use distributed ledger technologies to build computational trust directly into their applications. This allows individuals and businesses who might not know or trust each other to quickly and inexpensively collaborate. Public distributed ledgers allow for creating and exchanging value, proving identity, verifying and authenticating important data and much more. Hedera is unique in that it achieves the same result as the most ubiquitous public blockchains (such as Bitcoin or Ethereum), But in a way that is faster, fairer and more energy efficient, scale, and secure – these advantages can be attributed to the underlying hash-graph consensus algorithm and the global enterprise governing body, which owns and operates Hedera today. [1]

Hedera is governed by the Hedera Governing Council: An expert council consisting of 39 leading global enterprises and organizations, distributed across up to 11 different industries and spanning a wide range of geographies. The Governing Council makes key decisions over software upgrades, network pricing, treasury management, and more. Governing Council members are term-limited and do not receive any profits from Hedera. The Hedera Governing Council is structured to best fulfill the desire for a decentralized, wise, stable governance in the long-term interests of the platform. All governing council members have all taken partial ownership of Hedera Hash-Graph LLC, by signing the agreement. This LLC agreement has been made available, in its entirely, at <https://www.hedera.com/council/>. [2] To the best of knowledge, this is first eminent study on the NFT Transaction in the blockchain methodology.

Keywords: Blockchain, NFT (Non-fungible Token), Security, Scalability, Authentication, Decentralized security, Hedera HBAR, Hedera Token Service.

Introduction:

Hedera is a proof-of-stake public distributed ledger which aims to use a combination of a “path to permissionless” (network nodes) and a “path to widespread coin distribution” (HBAR cryptocurrency) to keep the network secure, while working to achieve full decentralization. Let's focus on permissionless nodes and coin distribution, and the role they play in securely achieving and maintaining decentralization. [3]

**Public vs Private & Permissioned vs Permissionless**

Distributed ledgers are categorized as “private” or “public” and “permissioned” or “permissionless” — they can be any combination of the two. At open access of the Hedera main-net, the Hedera network is public permissioned. But to achieve full decentralization, Hedera believes it must transition to becoming a public permissionless network.

Private / Permissioned: This type of network offers no decentralization. The applications deployed in production, and the network nodes running those application, must be invited to join the network and meet certain criteria or provide a form of identification. Any party can also be removed without warning at any time.

Private / Permissionless: Requires that applications deployed in production be invited to join the network and can be removed without warning at any time. The nodes which constitute the network and run said applications can freely and anonymously join and contribute, typically in exchange for a network’s native cryptocurrency.

Public / Permissioned: Allows applications to be deployed in production or removed, without having to notify anyone, reveal their identity, or meet any application criteria requirements. The nodes which constitute the network and run said applications must be invited to join the network.

Public / Permissionless: This type of network is the most decentralized. Applications can be deployed in production or removed, without having to notify anyone, reveal their identity, or meet any application criteria requirements. Additionally, the nodes which constitute the network can freely and anonymously join and contribute, typically in exchange for a network’s native cryptocurrency.

Hedera is starting off at open access in the upper left quadrant, as a public permissioned network — the nodes which constitute the network will be operated by Hedera Governing Council members, which have been invited to join as network operators. As performance, security, stability, and incentives of the Hedera network mature, Hedera will open node operation to more entities and individuals, relaxing permissions.

The Hedera network will become public and fully permissionless — any individual or organization can run a node anonymously and earn HBAR cryptocurrency for assisting with network operation. This is the path Hedera will take, ensuring security at every point along the path, to fully realize its mission of becoming the most decentralized public permissionless ledger in the market.

Research Questions:

1. How to secure during the DDos attack?
2. How can they free up the carbon evaporation during the large block chain transaction?
3. What is Hedera consensus algorithm?
4. How to prevent from security breaches in Hedera Blockchain?
5. What are the advantages and disadvantages?

Literature Survey:

Survey Report: On Hedera Token service

In Hedera token service, which consists of 3 phases are Main-net, Mirror-net, Test-net which is used to implement the NFT Transaction in Hedera Network. In Main-net phase, it contains Main-net nodes, Mirror nodes, Network services and support. In Mirror-net Phase, which contains the information about community mirror nodes, Hedera ETL, Hedera Mirror node, One-Click Node Deployment, Run your own Beta mirror node. The Beta version can implement only if the NFT Transaction phase should before the deployment to Main-net phase. In Test-net phase which contains Testnet nodes, Mirror nodes, Network services and support. The Network services consists of cryptocurrency, consensus, tokens, files and smart contracts. [1]

[Transaction Phase of Hedera HBAR Network]

Survey Report: On Main-net Access

A Main-net phase, which should have Hedera main-net account to interact with and pay for any of the network services (cryptocurrency, consensus, tokens, files and smart contracts). Hedera Account is what holds balance of HBAR to be used for transfer accounts or payments for network

services.[2]

Proposed System:

**Non-Fungible Transaction:**

A non-fungible transaction is a type of cryptographic token technique is its attributes typically programmed into the NFT’s issuing smart constructor are part of the initial native configuration of the NFT before issue are.

[Flow of NFT Transaction phases(a)]

**Blockchain Methodology:**

As the word is used in the blockchain world, the hashgraph is 100 percent efficient. Work is occasionally lost in blockchain mining a block that is subsequently deemed old and abandoned by the community. The equivalent of a "block" in hashgraph never grows stale. Hashgraph makes good use of

bandwidth as well. Hashgraph adds just a little cost above and above the amount of bandwidth necessary simply to tell all nodes about a particular transaction (even without obtaining consensus on a timestamp for such transaction).

**Gossip Protocol:**

A gossip protocol, also known as an epidemic protocol, is a computer peer-to-peer communication mechanism or process based on how epidemics propagate. To guarantee that data is delivered to all members of a group, numerous distributed methods utilize peer-to-peer gossip. This is the technique that allows all transactions to commit their transactions via the gossip protocol. This can resolve the error in multicast broadcasting communication by itself.

Participants in the gossip protocol on the blockchain transmit new information (called gossip) about transactions, as well as gossip about gossip.

[Flow of NFT Transaction phases(b)]

Performance Evaluation:

This is a report of the Hedera Smart Contract service's performance. A smart contract service that enables blockchain nodes to connect with unknown parties in order to transfer wallet balance from one to another at the same time. It uses Decentralized systems approach to securely commit transactions in multi-cast way. This adds solidity between transactions, acting as a bridge between each user throughout the transaction phase.

Transaction cost Denomination of Hedera Network:

1 Gigabar = 1 Gℏ = 1,000,000,000 ℏ

1 Megabar = 1 M ℏ = 1,000,000 ℏ

1 Kilobar = 1 K ℏ = 1000 ℏ

1 Hbar = 1 ℏ = 1 ℏ

1 Millibar = 1000 m ℏ= 1 ℏ

1 Microbar = 1,000,000 μℏ = 1 ℏ

1 Tinybar = 100,000,000 tℏ = 1 tℏ

On the Blockchain transaction charge, these are the transaction fees for the Hedera Token service. The Hedera Block chain NFT Transaction fee denominations can divide bulk transactions into these transaction denominations. It assigns a transaction charge to each Tinybar. We can transact the amount of millions of transactions at low cost, low predictable gas fee, low carbon burn.

Transaction cost of Hedera Network on Blockchain NFT:

|  |  |  |  |
| --- | --- | --- | --- |
| **S.NO** | **Operation** | **Cost** | **Other Site Cost** |
| 1 | CryptoCreate | $0.0001 | $.0.0010 |

Discussion:

Conclusion:

The hashgraph consensus technique allows developers using Smart Contracts 2.0 to charge reasonable, predictable gas prices. Hedera can handle up to 15 million gas per second, which is the same as Ethereum's target for a single block. Hedera's high transfer speeds and security standards assist Smart Contracts 2.0 transactions as well. The Hedera network uses hashgraph to achieve Asynchronous Byzantine Fault Tolerance (ABFT), the greatest level of security for a distributed ledger, which implies that no one person or group can prevent the algorithm from achieving agreement. The Hedera Smart Contract Service is compatible with the EVM (Ethereum Virtual Machine) and runs Solidity, a programming language utilized by 30% of all Web3 developers. With the Hedera Token Service, Hedera's Smart Contracts 2.0 blends Solidity and EVM compliant smart contracts with the versatility of Hedera's tokenization infrastructure by supporting native Hedera tokens and NFTs. This gives consumers more options, allowing developers to evaluate the usability of smart contracts and add hashgraph-based tokenization capabilities into their programs.

References:

[1] Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges - Qin Wang, Rujia Li, Qi Wang, Shiping Chen Southern University of Science and Technology Swinburne University of Technology, University of Birmingham.

[2] Smart Contracts 2.0: Live on Main-net - Feb 07, 2022 by **Gehrig Kunz** Product Marketing at Hedera Hashgraph

[3]