ZVWS

by Ananth Kumar

Submission date: 06-Apr-2022 01:23AM (UTC-0400)
Submission ID: 1768136400
File name: Hedera_HBAR_-_Paper_-_Highlighted.docx (230.81K)
Word count: 3005
Character count: 16383

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. Distributed ledger technologies are used by developers to embed computational trust directly into their applications. Individuals and corporations who may not know or trust one other can work swiftly and cheaply as a result of this. 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.

Hedera is administered by the Hedera Governing Council, which consists of the following members: An expert committee made up of 39 of the world's most influential people has been formed. Global businesses and organizations, encompassing up to 11 industries and a diverse range of products and services. 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 designed to better satisfy the platform's long-term goals for decentralized, wise, and stable governance. All governing council members have all taken partial ownership of Hedera Hash-Graph LLC, by signing the agreement. In this article, we will undertake NFT transactions in a range of areas, including cryptography, banking, and financial transactions, using our hedera network. The study that supports NFT transactions in the hedera network phase of the three can be classified in the introductory section below. 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]

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 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.

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.

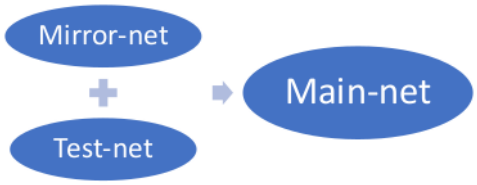
Research Questions:

1.

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.



[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.

Survey Report: Remove centralized control: Hala Systems

Storing data to a central database necessitates trust — faith that the database will be adequately secured and that the data will not be tampered with or erased.

after it has already been written Hala Systems was looking for a solution that could

act quickly.as an unbiased observer who is not influenced by them or a single party

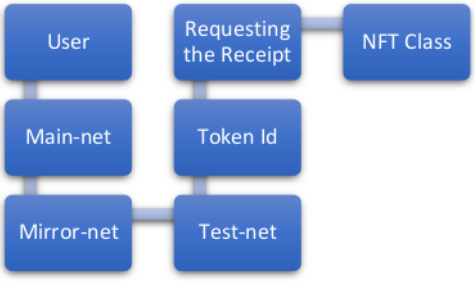
a single entity, but one that is dispersed and highly decentralized among several parties who are impartial. This distributed character, along with the fact that Multiple assurances are provided by its immutable nature. independent parties to determine who submitted the data and when it was received recorded, as well as the information it contains. Due to unauthorized access to Hala Systems' network domain, over 2 million people's accounts have been alerted. There were 140 warning messages sent to their clients about illegal access to their information. During the case study, 250k persons experienced less trauma as a result of using this service. Every Hedera network service uses the hashgraph consensus technique to establish distributed consensus.

Hashgraph proposed two innovative ideas to produce what may be the most mathematically efficient sort of consensus possible: gossip chatter and virtual voting. Hashgraph is not only efficient, but also secure; due to its asynchronous Byzantine fault tolerance, it has been found to be more robust in more conditions than rival consensus algorithms.

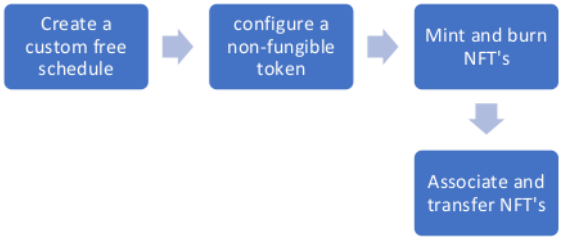
Proposed System:

Non-Fungible Transaction:

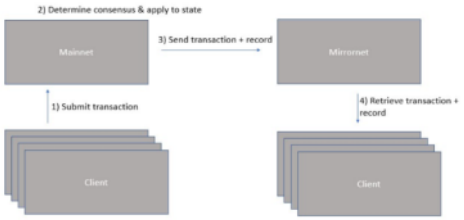
A non-fungible transaction is a type of cryptographic token technique is its attributes typically programmed into the NFT's issuing smart constructor are part of the initial native configuration of the NFT before issue are.



[Flow of NFT Transaction phases(a)]



[Flow of NFT Transaction phases(b)]



[Flow of NFT Transaction phases(c)]

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 bl ockchain transmit new information (called g ossip) about transactions, as well as gossip about gossip.

Hashgraph:

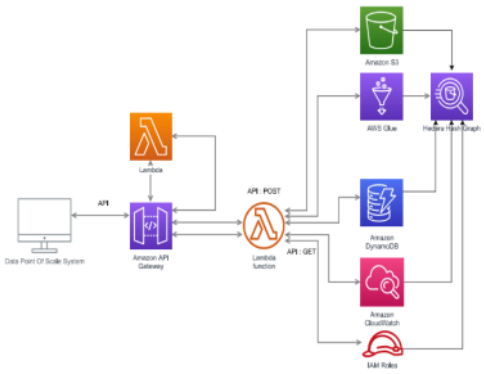
Hedera Hashgraph employs its own consensus method and data structure called hashgraph to perform 100x more transactions per second than blockchain-based alternatives. Hashgraph is incredibly efficient thanks to two features: virtual voting and chatter about gossip. On hashgraph, each event has the following information: Self-parent, Other-parent; Transactions, Timestamp, Signature on a computer.

The table about the consensus algorithm components:

SNO	Item	Description
1.	Timestamp	The timestamp of when the member created the event commemorating the gossip sync
2.	Transaction	The event can hold zero or more transactions
3.	Hash 1:	Self-parent hash
4.	Hash 2:	Other-parent hash
5.	Digital Signature	Cryptographically signed by the creator of the event

Consensus Algorithm [In Gossip Protocol]:

Grasping the concept of gossip is the history of how these occurrences are connected to one other through their parent hashes. This history is represented as a directed acyclic graph (DAG), a hashgraph, or a graph of hashes.



Each allowed party can get data from the controlled API and check Hedera directly to validate the information and integrity of the state of a coupon. The information for the applicable coupon can be obtained through the API, and the hash can be recalculated by the partner application. The transaction ID can be checked on a Hedera mirror node to ensure it was recorded appropriately on the public ledger once the hash is confirmed to match.

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 G$\hbar$ = 1,000,000,000 $\hbar$

1 Megabar = 1 M $\hbar$ = 1,000,000 $\hbar$

1 Kilobar = 1 K $\hbar$ = 1000 $\hbar$

1 Hbar = 1 $\hbar$ = 1 $\hbar$

1 Millibar = 1000 m $\hbar$= 1 $\hbar$

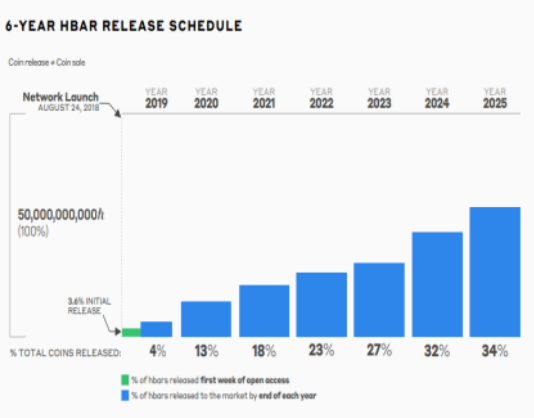
1 Microbar = 1,000,000 $\mu\hbar$ = 1 $\hbar$

1 Tinybar = 100,000,000 t$\hbar$ = 1 t$\hbar$

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:

Each function in the hedera solidity programming, which is already pre-defined set of costs, was assigned in the numerous processes conducted by the hedera consensus network.



To ensure that the Hedera network is secure under a permissionless design, the network's currencies must be broadly distributed.

Coins represent the "stake" of voting power in Hedera's proof-of-stake consensus process – more coins equal more voting power over consensus. To ensure network security, HBARS must be widely distributed, with no single attacker or group of attackers holding more than one-third of the coins. Hedera's goal is to combine a "road to permissionless" with a "path to widespread coin distribution" in order to maintain the network secure while also pushing toward more decentralization.

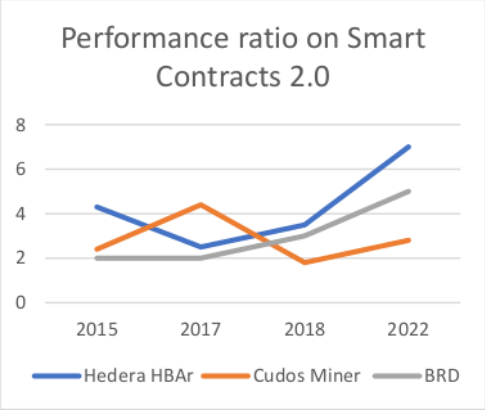
First, until enough coins are released, Hedera will remain a permissioned network. The network will remain permissioned for the sake of network security until the total value of all circulating coins reaches a point where a hostile user (or group of users) would be unable to purchase a third of them to carry out an assault. The amount of HBARS that can be proxy-staked to a single node will be limited once proxy-staking is introduced.

Second, Hedera has a slow and deliberate release timetable, with only 34% of all HBARS scheduled to be released before 2025. This delayed release plan is designed to ensure that the network grows in a stable and orderly manner, allowing it to scale without losing the security required for a really useful and pervasive network that delivers on the promise of creating a trusted, empowering, and secure online world.

The below table (a) shows the service charges acquired by Hedera Network NFT Transactions, such as Cryptocurrency service, Consensus service, Token service, Schedule service, Contract service, and so on. Hedera charges a moderate miscellaneous fee for all operations when compared to the cost of other network providers.

SNO	Service	Cost ($)	Others ($)
1	Cryptocurrency Service Sum*	0.026	0.030
2	Consensus Service*	0.02	0.10
3	Token Service *	3.16	3.8
4	Schedule Fee*	0.01	0.0102
5	Contract Service*	1.16	1.5
6	Miscellaneous Fee*	0.00	0.10

[Table contains the information about Hedera Network service cost (a)]



[Performance ratio on Smart Contracts 2.0]

Discussion:

The account balances are updated simultaneously for each transaction and its related fee payments. The account's HBAR are only accessible to the person who holds the private key.

The 2021 NFT boom proves that blockchains can: 1) solve real-world problems, 2) be quickly deployed, and 3) generate wealth for both users and underlying networks. There are other competing blockchains that use different consensus algorithms than Ethereum. Venture into NFT technology with the goal of enhancing transaction speed and decreasing fees. The goal is to increase market valuations and expand the user base. NFT sales volume in August 2021. Close to $4 billion was spent on the OpenSea marketplace in February, up from only $8 million in January. 202117, a jump of 50,000%. This highlights the industry's massive revenue potential. On top of existing blockchains, NFT economics is constructed.

Various current blockchains began to include NFT as a result of the excess demand curve.

As a result of the surplus demand curve, various current blockchains began incorporating NFT infrastructure that enables NFT minting, trading, auctioning, mining, staking, and other operations. It seems reasonable to assume that the NFT craze sparked a significant increase in blockchain adoption, which is an important step toward blockchain technology's eventual revolution of commerce and financial services. Et al. Paul Madesen, take out a single trustworthy node at a time with a DDoS attack. Other nodes are unable to sync with a DDoSed node. It also controlled over a limited number of malicious nodes (less than 1/3), who are aware of what is going on and may be able to help me guide the attack to alternate which node is DDoSed. For as long as the attack continues, ability to shut down the network. This is a DDoS attack (Distributed Denial of Service). The attacker has gained access to a large number of machines on the internet, which

he can use to flood a single computer with so many packets that it shuts down for the duration of the attack. When it comes to choosing a DDoS target, it doesn't matter how intelligent the attacker is. It makes no difference if the attacker uses a malicious node as a spy to assist in the selection of the victim. The attack is still ruled out. An attacker cannot freeze the network for as long as the attack continues unless every pair of honest nodes eventually syncs, and more than 2/3 of the nodes are honest nodes. Because if it went on indefinitely, all four Conditions would hold true, but the Results would not. The ABFT proof rules this out. As a result, the ABFT proof declares this type of liveness attack impossible, and the claim must be incorrect. the Leader attack may even contain a mathematical proof that it is ABFT. However, it cannot have an ABFT proof because an ABFT proof would ensure that it is immune to that assault. This is one of the key ways in which ABFT outperforms ABFT. A protocol with a ABFT proof is guaranteed correct, but if the evidence can be updated to an ABFT proof, the correctness guarantee can be increased to provide liveness guarantees as well.

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] HALA SYSTEMS Seeking Justice with Tamper-Proof Evidence on Hedera Hashgraph, @2020 Hedera Hashgraph, Global.

[4] Non-Fungible Tokens (NFT). The Analysis of Risk and Return - Mieszko Mazur, IESEG School of Management

[5] ABFT for Correctness and Liveness – Feb 07, 2020 – Paul Madesen

[6] Hbar Economics A deep dive into the dual role of HBARS & detailed release schedule – Hedera LLC.

ZVWS

ORIGINALITY REPORT

33%	32%	1%	9%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	hedera.com Internet Source	26%
2	www.portlavacawave.com Internet Source	3%
3	docs.hedera.com Internet Source	1%
4	Submitted to University of Hertfordshire Student Paper	1%
5	en.wikipedia.org Internet Source	1%
6	arxiv.org Internet Source	<1%
7	fortsattageb.com Internet Source	<1%
8	Dejan Dolenc, Jan Turk, Matevz Pustisek. "Distributed Ledger Technologies for IoT and Business DApps", 2020 International Conference on Broadband Communications	<1%

for Next Generation Networks and Multimedia Applications (CoBCom), 2020
Publication

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		