NFT Trend And Security Issue and Market Manipulation

Kim Donghyun
dept. Information System
Hanyang Univ.
Seoul, Republic of Korea
lmkn5342@gmail.com

Mheen Kyoungwhan
dept. Information System
Hanyang Univ.
Seoul, Republic of Korea
kwheen@gmail.com

***Abstract*— In recent years, companies in South Korea have adopted NFTs to innovate in both virtual and offline environments. In the case of Lotte, they issued a belly bear as an NFT and held various events, and Shinsegae is planning a new business by utilizing the famous MetaCongz. However, it is necessary to consider whether the value of these NFTs is being properly evaluated. In the past, there was a time in medieval Europe when the price of a tulip was close to $100 million in today's dollars. This was because the seeds themselves were difficult to grow, and there was no way to know what kind of tulip would emerge from them. However, the value of tulip seedlings was soon recognized, and the price of tulips returned to normal. In the case of domestic NFTs, it is necessary to check whether they are not oversaturated. In this paper, we will compare MetaKongz, a famous domestic NFT, with overseas NFTs in the PFP category such as CryptoPunks and BEANZ, and analyze their characteristics, as well as analyze the NFT itself.**

I. Introduction

With the rise of non-fungible token (NFT), new opportunities and challenges have emerged in the digital asset market. While NFTs have brought a new level of excitement to the world of collectibles, art, and gaming, they have also exposed new security vulnerabilities that need to be addressed. This paper will explore two main security issues in NFT transactions: NFT phishing attacks and NFT double minting. We will discuss the causes of these issues, their potential impact on NFTs and their owners, and possible solutions to prevent them. By examining these security issues, we hope to raise awareness of the importance of securing NFT transactions and promote the development of safer NFT marketplaces.

II. Theoretical Background

A. Non-Fungible Token, NFT

NFT is a unit of data stored on blockchain that certifies a digital asset to be unique and therefore not interchangeable, while offering a unique digital certificate of ownership for the NFT. More broadly, an NFT allows to establish the “provenance” of the assigned digital oobject, offering indisputable answers to such questions as who owns, previously owned, and created the NFT, as well as which of the many copies is the original.[1]

[1] Matthieu Nadini, “Mapping the NFT revolution: market trends, trade networks, and visual features” PP.1, 2021

B. NFT Standard

1. Non-Fungible Token (NFT) Contract Address

In the context of blockchain technology, particularly within Ethereum-based systems, a Non-Fungible Token (NFT) Contract Address plays a vital role. This address is a unique identifier, serving as a specific location within the blockchain where the NFT's smart contract resides. This contract is a self-executing contract with the terms of the agreement directly written into code. Unlike cryptocurrency addresses, which are fungible and indistinguishable from each other, an NFT contract address points to a contract that verifies the provenance, ownership, and uniqueness of the NFT. Therefore, an NFT Contract Address is integral for transactions and interactions concerning a particular NFT.

2. NFT Gas

The term "gas" within the blockchain domain signifies the computational effort required to execute specific operations, including those involved in NFT transactions. Every operation that takes part in Ethereum, including the execution of smart contracts (which NFTs are part of), costs a certain amount of gas. Transacting with NFTs, whether it be minting (creating), buying, selling, or transferring, requires gas as a form of computational fee. This fee is paid in Ether (ETH), and the total amount of gas required varies based on the complexity of the contract, the size of the contract data, and network congestion. Thus, the concept of NFT Gas is a fundamental aspect of managing transaction costs and execution times within Ethereum's network.

3. Confirmations

In blockchain systems, confirmations refer to the number of blocks that have been added to the blockchain after the block containing a specific transaction. This term represents the number of times the network has confirmed the transaction, making it more secure and immutable. The larger the number of confirmations, the lower the risk of transaction reversal due to a fork in the blockchain. In the context of NFT transactions, this means that the ownership transfer of the NFT has been confirmed and permanently recorded on the blockchain. Therefore, confirmations are a crucial measure of

transaction security and finality within blockchain networks.

4. Smart Contract

A smart contract, first proposed by Nick Szabo in the 1990s, is a self-executing contract with the terms of the agreement directly written into code. They are stored on the blockchain and automatically execute when predetermined terms and conditions are met. Smart contracts not only define the rules and penalties related to an agreement in the same way a traditional contract does, but they can also automatically enforce those obligations. In the case of NFTs, a smart contract might define the rules for ownership transfer, ensure the uniqueness of the NFT, and handle the transaction's financial aspect. Therefore, smart contracts are foundational to the operation and trustless nature of blockchain-based systems, including NFT platforms.

C. *NFT Trade Flows*

1. NFT Creation: NFT creation is the process of transforming digital content into unique non-fungible tokens. Artists or creators choose an NFT platform and follow its guidelines to convert their digital assets into NFTs. NFTs are based on blockchain technology, with Ethereum being a prominent platform that utilizes ERC-721 and ERC-1155 standards. During NFT creation, information such as ownership, attributes, and metadata of the digital content is specified, and the generated NFT receives a unique identifier.

2. Listing NFTs for Sale: To sell an NFT, it needs to be listed on a marketplace. Artists or owners join their chosen NFT marketplace and complete a registration form, providing detailed information about the NFT and its selling conditions. Typically, the registration process involves supplying the NFT's image, title, description, price, royalties, and other relevant information. Once listed, the NFT becomes discoverable on the marketplace, allowing potential buyers to find and proceed with the purchase process.

3. NFT Purchase: To purchase an NFT from an NFT marketplace, buyers explore the available NFTs and select their desired item. They review the NFT's details, price, and selling conditions before initiating the purchase request. Most marketplaces require buyers to pay the specified price for the NFT, usually in the form of cryptocurrency. Once the purchase is completed, the NFT is transferred to the buyer's wallet, and ownership is transferred accordingly.

4. Transfer and Ownership Changes: The transfer and ownership changes of NFTs occur through smart contracts on the blockchain. Owners can transfer NFTs to other individuals or accounts by providing the recipient's blockchain address or identifier. During the transfer process, the sender specifies the quantity of NFTs being transferred and any applicable fees. Following the transfer, ownership is transferred to the recipient. The transparency and immutability of the blockchain enable the tracking of ownership history.

D. *Wyvern protocol*

The Wyvern protocol is a protocol that implements a decentralized NFT exchange. It runs on top of the Ethereum blockchain. Wyvern works by brokering transactions between buyers and sellers: sellers list NFTs they want to sell, and buyers want to buy them. Wyvern brokers the transaction and transfers ownership of the NFTs to the buyer once the transaction is complete. In doing so, Wyvern earns a fee for brokering the transaction. Wyvern is one of the most prominent protocols implementing decentralized exchanges.

III. NFT Analysis

A. *MetaKongz*

MetaKongz is a domestic PFP project launched in December 2021. It was first developed based on the worldview that the bored gorillas in the circus are entering the sewer and developing an engine to reach Paradis. MetaKongz completed minting in December 2021 and launched a Discord channel and AMA-only channel.

B. *Compare Groups*

1. CryptoPunks

Cryptopunks is an NFT project launched by Larva Labs in 2017, centered around 100,000 unique digital characters existing on the blockchain. Each Punk, a 24x24 pixel art character, is algorithmically generated, offering a variety of features including accessories, hairstyles, and facial expressions. CryptoPunks have significantly influenced the NFT art scene and are often regarded as one of the earliest examples of NFTs. Notably, CryptoPunks completed their initial minting process for free, except for the cost of gas fees, providing an early model for subsequent NFT projects. Today, CryptoPunks are not just digital art pieces but have become valuable digital assets traded at remarkably high prices.

2. Bellygom World official

BELLYGOM NFT is a project created and developed from the partnership between Lotte Home Shopping and a FSN's affiliate, "FingerVerse." With a total of 10,000 PFPs, various experiences with the BELLYGOM IP such as shopping, hotels, exhibitions, and movies etc, are in store for you. We plan to design a new roadmap with the community members, to expand the

BELLYGOM Universe through private membership benefits and events such as renting the entire Lotte World just for our community.

3. BEANZ official
Beanz is a vibrant and unique NFT project that debuted in 2022. This project centers around 10,000 individual "Beanz" characters, each with its distinct traits, features, and backgrounds. Like many other NFT projects, the Beanz characters are algorithmically generated, resulting in a wide variety of combinations. Each Beanz character is not only a piece of digital art but also a part of a larger community-driven ecosystem. The Beanz project promotes active engagement from the community, hosting numerous events, contests, and giveaways. Unlike the early CryptoPunks project, Beanz were not minted for free, yet they've managed to attract a robust community due to their unique concept and the promise of utility within their ecosystem.

C. *Market Size Analytics*

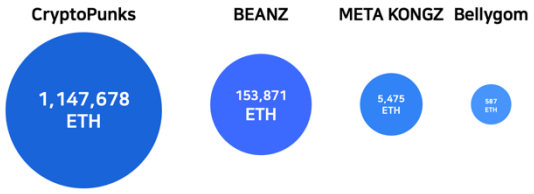


Figure 1. Size of NFT Markets. (Unit: ETH)

We measured the total size of each NFT collection. As of June 15, 2023, CryptoPunks has the largest NFT market size with 1,147,678 ETH. This is followed by BEANZ and MetaKongz with 153,871 ETH and 5,475 ETH respectively. Bellygom is the smallest with 6,536,457 KALY, which is about 547 ETH in Ethereum.

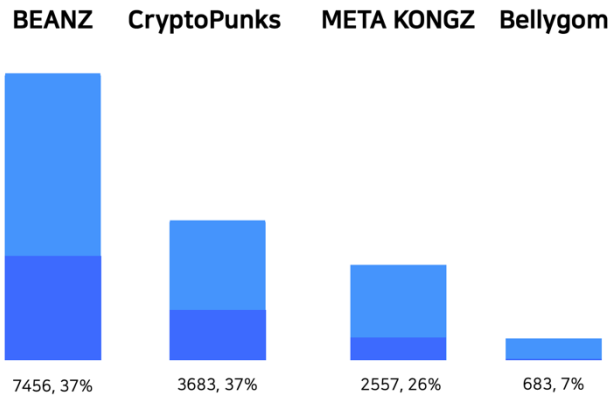


Figure 2. Bar graph of User and Unique User. (Unit: people)

On the other hand, if we look at the distribution of owners, we can see that for the rest of the NFTs except Bellygom, the number of unique owners (people who participated in the minting of the NFT) is in the 20-30% range, and for Bellygom, which was issued by a company as an event, the number of unique owners is 7%.
It is Beanz, not Cryptopunk, that has the most owners, and this may be due to the fact that BEANZ targeted the general public more than cryptopunk, and also built and minted an ecosystem in advance.

D. *Contract Address Analytics*

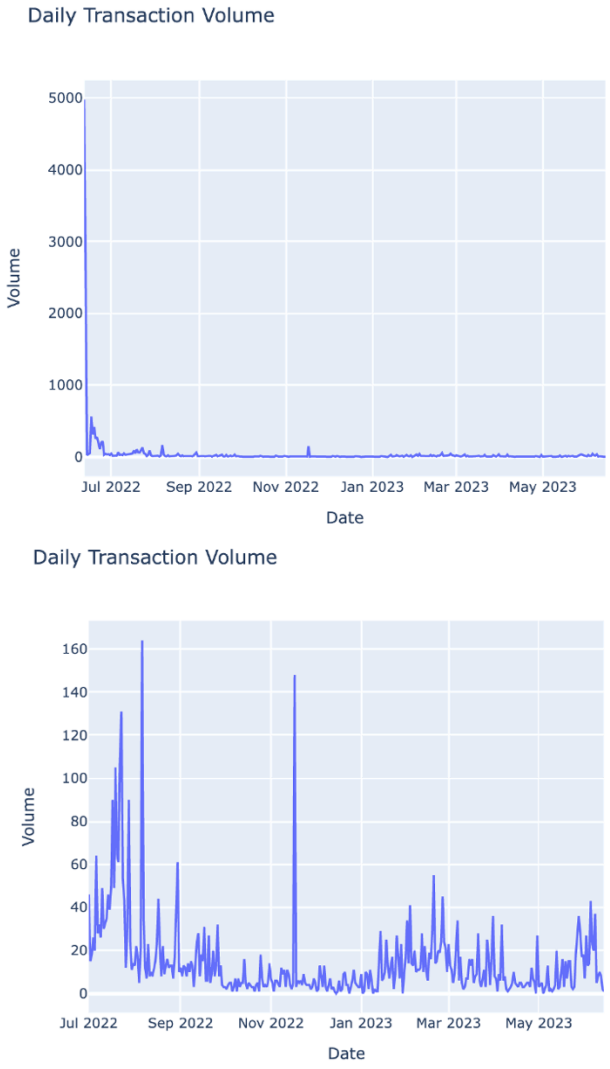


Figure 3. Daily Transaction Volume Graph. (upper) Transaction of MetaKongz Contract Address since first minting **(lower)** Transaction of MetaKongz Contract Address after initial large-scale minting

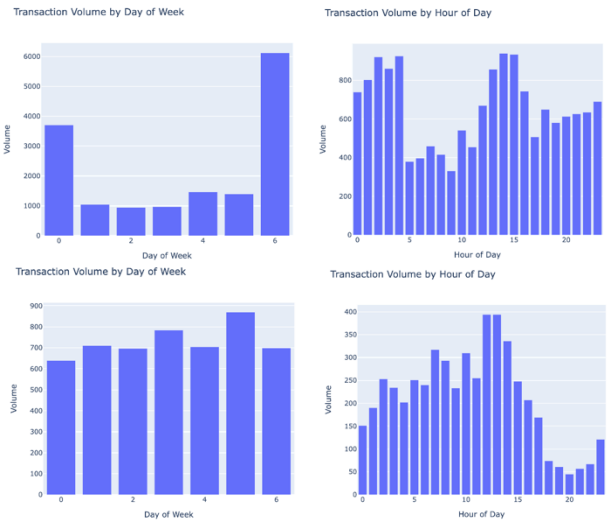


Figure 4. Distribution differences before and after filtering data (upper and lower)

In the figure 4, we can see the difference between the time series data before and after filtering. In the case of a week's worth of data, you can see that the distribution is more evenly distributed after filtering, instead of being concentrated on Sunday and Monday. In the case of MetaKongz, which is mainly used in South Korea, the first graph of Transaction is uneven, but when we exclude the records when changing the main exchange, the time distribution is more or less even.

In the figure 3, we analyzed MetaKongz's daily transaction history. MetaKongz abandoned Klaytn in June 2022 and moved to Eth, so there is a lot of early minting data. If you exclude the early minting data, it looks like a lower graph. On average, there are about 14 transactions per day, and the highest number of transactions per day was 164.
Since 26% of the transactions occurred in the early days of the blockchain platform move, this can skew and misinterpret the data in time series analysis, so the time series analysis that follows is limited to records after the platform move.

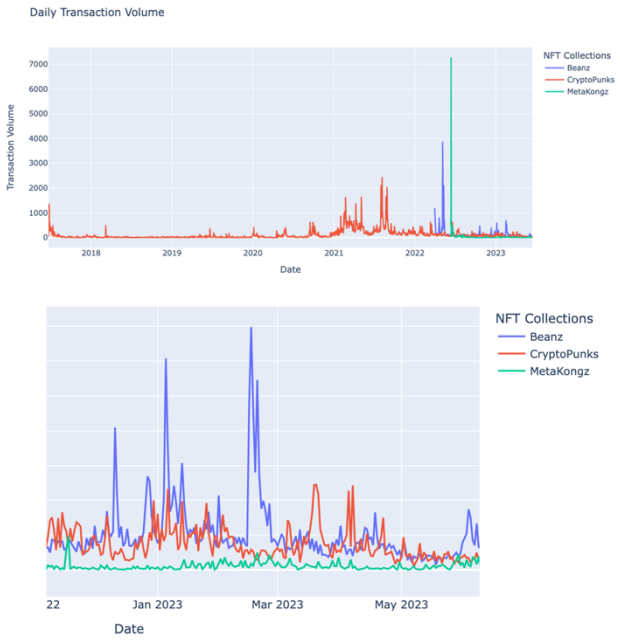


Figure 5. Daily Transaction Volume of Three NFTs. **(upper)** Total Transaction History of BEANZ, CryptoPunks, MetaKongz **(lower)** Transaction History of three NFTs. Especially filtered 2023's history

In addition to MetaKongz, we've shown two more NFTs, BEANZ and CryptoPunks. CryptoPunks is the oldest of the three, with a release date of 2017. The average number of daily trades is 122 for CryptoPunks, 131 for BEANZ, and 42 for MetaKongz, with MetaKongz being about three times less active than other NFTs in its category. (upper) Looking at the history of 2023 alone, we can get a sense of the overall trading activity, with BEANZ > CryptoPunks > MetaKongz.

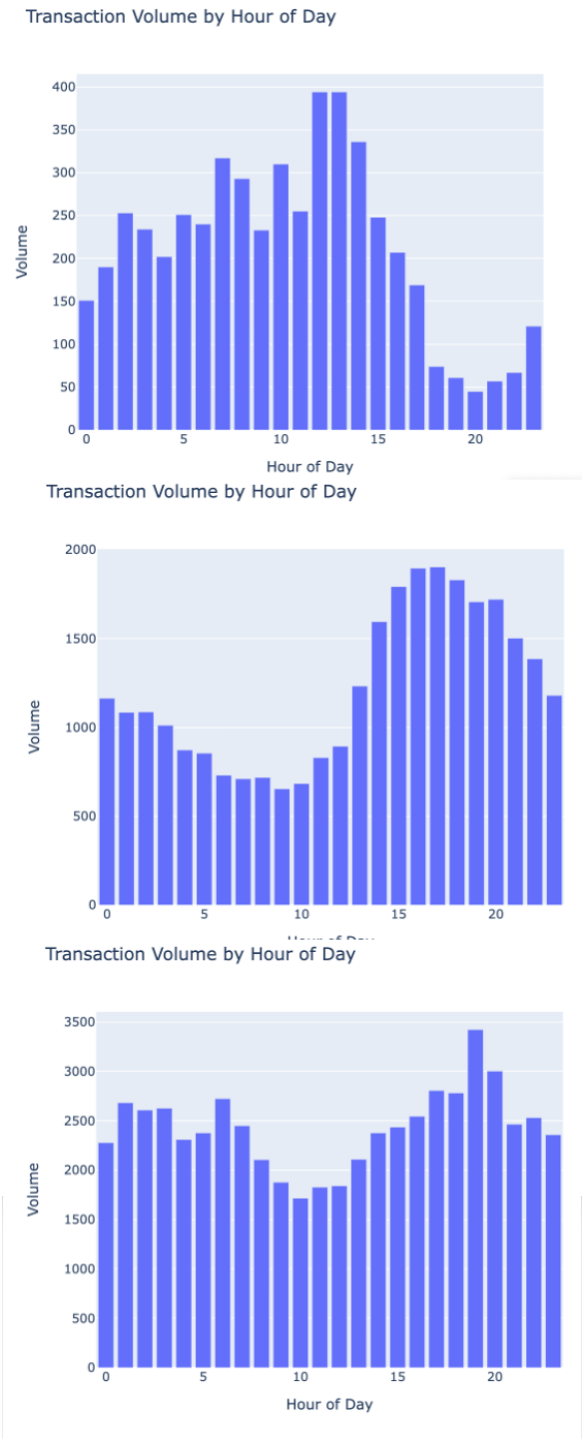


Figure 6. Transaction Volume by Hour of Day. (first) Time Series of MetaKongz **(second)** Time Series of CryptoPunks **(third)** Time Series of BEANZ

In the graph above, you can see the most frequent trading hours for each collection. Due to the global nature of the Ethereum blockchain network, the date and time data returned by the Etherscan API is based on UTC (Coordinated Universal Time). MetaKongz has the highest volume of transactions at 20-21pm KST, while CryptoPunks and BEANZ have the most transactions between 04:00 and 02:00-03:00, respectively. Assuming that traders have similar consumption patterns, we were able to estimate that a large number of traders are located in the U.S. (mainly in PST and HST, e.g. the western U.S.).

IV. NFT Security Issue

A. NFT Phishing

An NFT phishing attack is when a hacker creates a phishing site with the intention of acquiring NFTs and stealing the NFT owner's personal and wallet information. These attacks can result in the theft of NFT owners' assets, and victims can lose both their wealth and personal information. NFT phishing attacks are usually introduced via email, messenger, social media, etc. Hackers send fake emails using the same email domain as the NFT owner and direct them to a phishing site. The phishing site is usually pretending to be an NFT exchange or wallet site to trick you into logging into the site and stealing your wallet information and personal data. For example, Opensea was recently hacked. The hacker sent an email impersonating Opensea's mail domain and directed the user to a phishing site. The site stole Opensea wallet information and personal data.

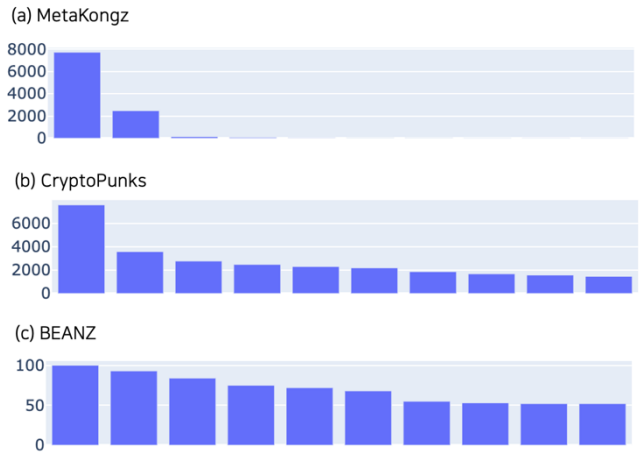


Figure 7. Top 10 holders of NFTs.

The graph above shows the top 10 holders of NFTs. Using a similar calculation to the Gini coefficient, which calculates the degree of inequality, MetaKongz is the most unequally distributed, followed by CryptoPunks and BEANZ. MetaKognz is more unequal than BEANZ by a large percentage, but is very similar to CryptoPunks.

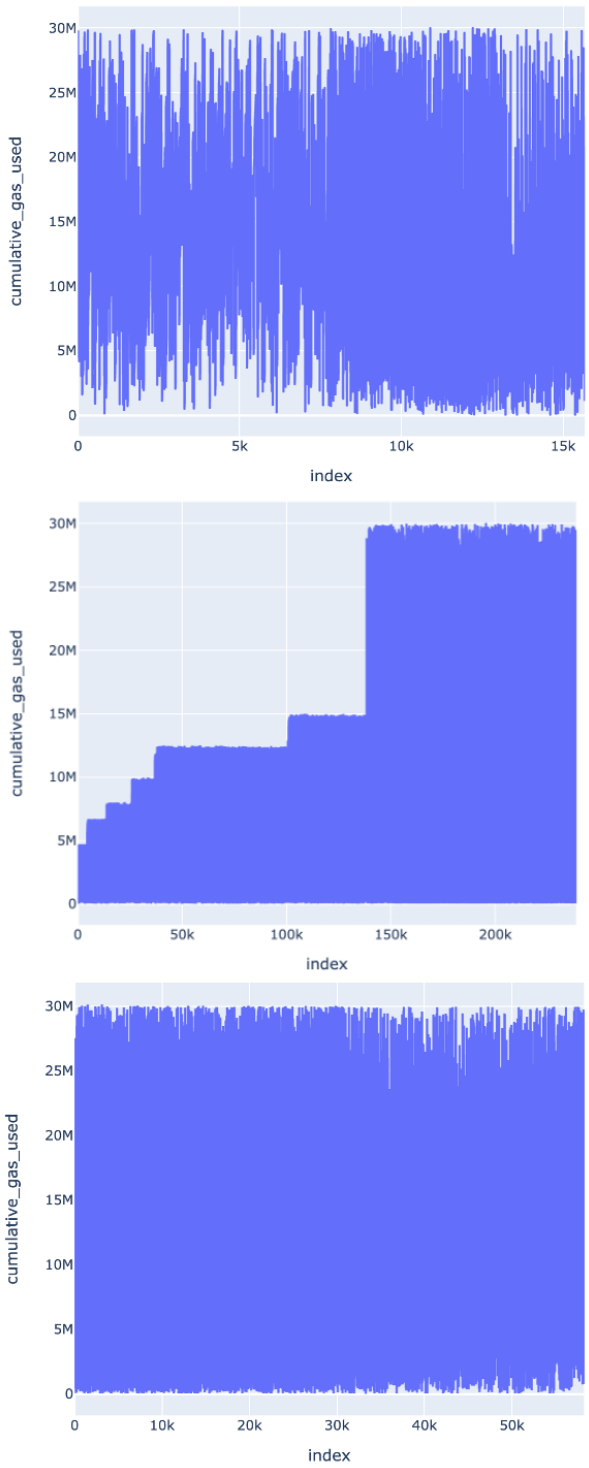


Figure 8. Graph shows Congestion of NFTs Network.
From top to bottom, MetaKongz, CryptooPunks, and BEANZ

The graph above shows the cumulative gas usage by Transaction Index. Transactions on the blockchain require a gas fee, and since there is a maximum amount of gas that a block can store, there comes a moment when the gas fee is emptied as transactions are repeated. In other words, the more frequently transactions occur, the more congested the network is.

Comparing MetaKongz and BEANZ, we can see that BEANZ is traded much more frequently, which means that the cumulative gas is replaced much more frequently.

In the case of CryptoPunks, we can see that the total amount of cumulative gas has increased like a staircase, and we can deduce the following factors. First, the price of gas required to process a transaction on a blockchain network varies depending on the time of day and the congestion of the network, and this variability can cause the gas cost of a transaction to increase or decrease over time. Second, as the network becomes more congested and transactions with higher prices are included in blocks, the cost of gas can increase. Finally, the more complex the operation a transaction performs, the higher the gas cost. None of this is certain, as this is all generalized reasoning, but it's usually assumed for these reasons.

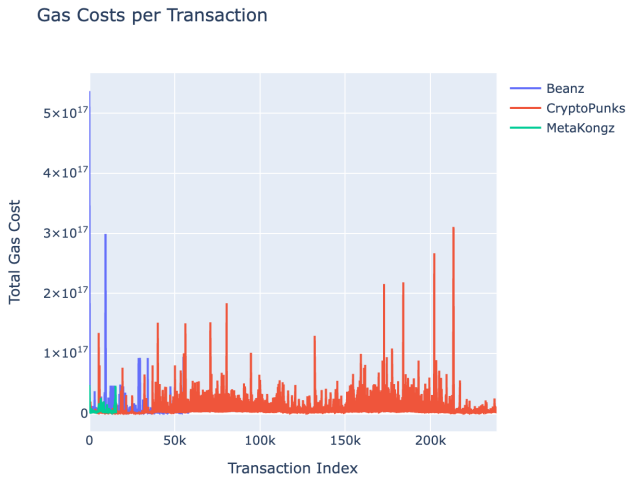
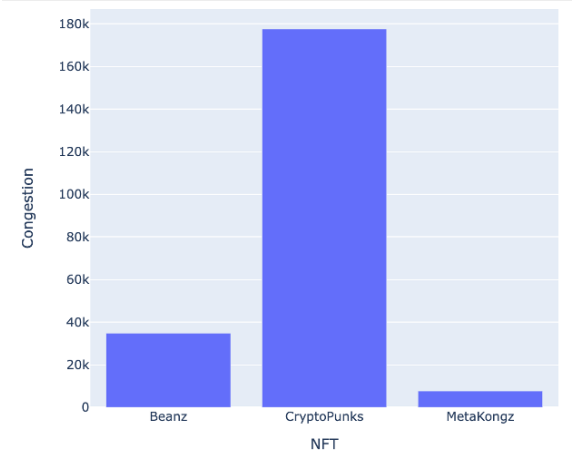


Figure 9. Gas Costs per Transaction of NFTs

Figure 9 tracks the change in the cost of gas, isolating it based on the transaction where the cost of gas starts to drop. We calculated the rate of change, a common method, to find the inflection point.



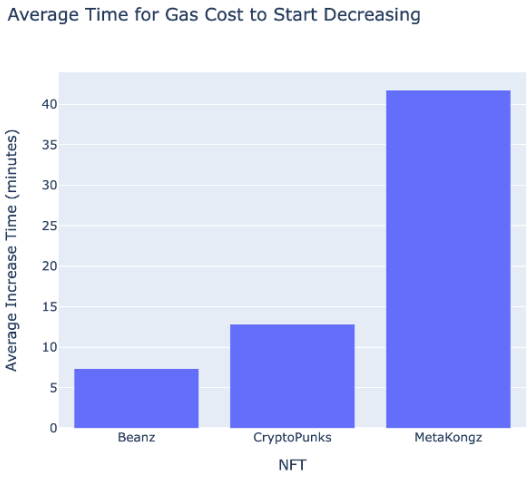
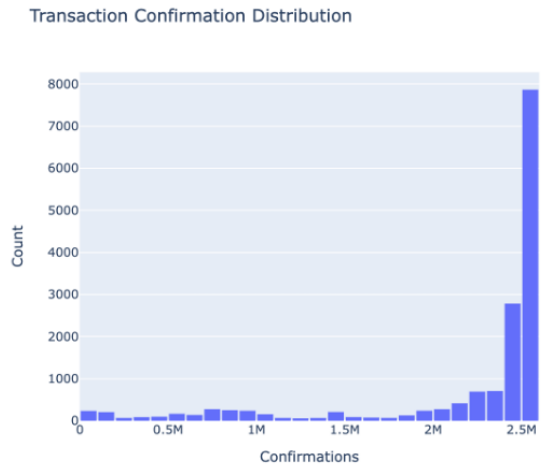


Figure 10. The number of congestion (top) and time (bottom) it takes for Cumulative Gas to initialize once

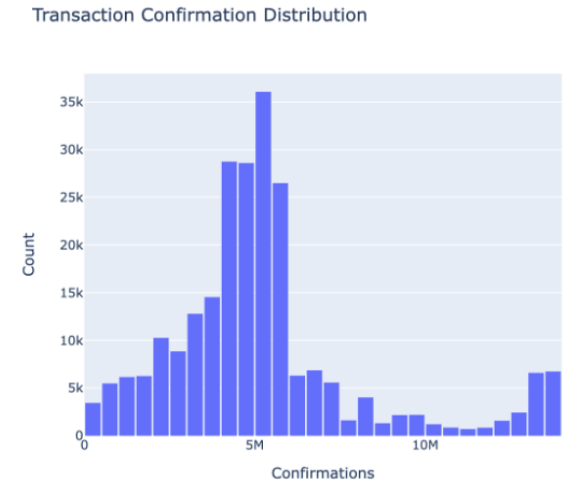
Figure 10 was created to calculate the complexity of the network. We first wanted to estimate the distribution of the data by counting the number of sharp changes. We calculated the percentage change in gas costs and defined the keyword "congestion" by defining a "sharp change" as when the percentage change exceeds a certain threshold. We set the threshold at 0.1 (defining a "sharp change" as a change in gas cost of more than 10% compared to the previous transaction).

The bottom of Figure 10 is a graph of the time it took for the actual block to become oversaturated and for gas to be reset. MetaKongz took 41.74 minutes to initialize gas, compared to comparable times of 7.34 minutes and 12.82 minutes for BEANZ and CryptoPunks, respectively. This suggests that MEtaKongz is not being traded as frequently as the previous two NFTs.

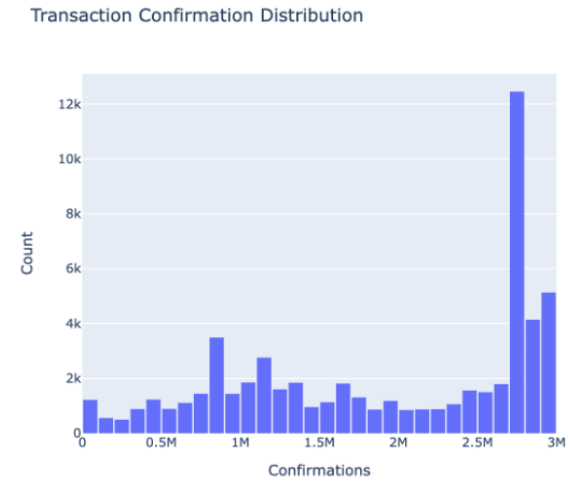
To compare each numerical metric, the average transaction cost (product of gas_price and gas_used) for MetaKongz is 2451454382389797.5 wei, for CryptoPunks it is 4499089528345068.5 wei, and for BEANZ it is 2115223046293041.5 wei.




```
Min Confirmations: 243
Max Confirmations: 2525291
Mean Confirmations: 2182510.36912666
```




```
Min Confirmations: 212
Max Confirmations: 13565366
Mean Confirmations: 5273799.605805809
```




```
Min Confirmations: 149
Max Confirmations: 2987287
Mean Confirmations: 1910258.0412925158
```

Figure 11. Min/Max/Ave confrimation and their counts
From top to bottom, MetaKongz, CryptooPunks, and BEANZ

The distribution of each confrimation can be used to characterize the NFT market. In the case of MetaKongz,

we can see that there are only a few very heavily traded NFTs, the market is not active, and there are only a few main trading lists. On the other hand, in cryptoPunks, we can see that the trading frequency is low, but it happens for many items, and the volume is much higher than in MetaKongz. BEANZ has a similar distribution to MetaKongz, but the peak transaction volume is about 1.5 times higher than MetaKongz, and the overall distribution is also more even.

B. Cause of NFT Phishing And Protocol Vulunerability

1. *Why was opensea attacked? :* The Opensea case above was caused by a vulnerability in the Wyvern protocol used by Opensea. When the user pressed the button in the email, a function called "atomicMatch_" was triggered, sending all the NFTs to the attacker. "atomicMatch_" is responsible for all transactions on OpenSea with minimal trust and is passed to Project Wyvern Exchange because Atomic allows transactions to occur if all parameters of the transaction are met. This means that one poorly placed button click through a phishing site could result in all NFTs being stolen.

```
function hsashToSign(Order memory order)
     internal
     pure
     returns (bytes32)
{
     /* Calculate signature */
    return keccak256("\\x19Ethereum Signed
Message:\\n32", hashOrder(order));
}
```

The above code takes a structure and signs it with a function called hsashToSign in Wyvern Exchange version 1. The `\x19Ethereum Signed Message"\n32` in the code above is there to recognize the calculated signature as an Ethereum signature. This ensures that the signature cannot be used outside of Ethereum. And 32 means the length of the message, and the hashed message has a length of 32 bytes. It is then hashed with keccak256 along with the hashOrder value corresponding to the message, and finally signed with the private key. However, this code makes it difficult to verify the uniqueness of the message, because it does not imply that the sender of the message is the same as the signer of the message. Therefore, a Signature Replay Attack can occur where a user's signature for that message is used by another user for a different contract. Signature Replay Attack is an attack that allows a contract to be executed repeatedly despite the fact that it has been authorized. This allows you to construct an attack contract that steals the user's NFTs after obtaining their signature. And `\\x19Ethereum Signed Message:\\n32` mean that the EIP191 signature was used. The disadvantage of eip191 signature is that the user cannot see information about the signature. Therefore, even if a hacker changes or adds part of the message, the user does not know. Using the above Signature Replay Attack, hackers can continue to use the signatures based on validation previously signed by the user.

Version byte	EIP	Description
0x00	191	Data with intended validator

2. Possible attack routes for protocol vulnerabilities

```
/*Transfer ether with valid signature*/
  function transfer(address _to, uint
_amount, bytes[2] memory _sigs)
    external
  {
    byte32 txHash = getTxHash(_to,
_amount);
    require(_checkSigs(_sigs, txHash),
"invalid sig");

    (bool sent, ) = _to.call{value:
amount}("");
    require(sent, "Failed to send Ether");
  }
```

To invoke the transfer function, you need three input values: _to, which is the address to send the ETH, _amount, which is the amount of ETH to send, and signature _sigs. And signatures are required as many as the number of owners. Transfer hashes _to and _amount using getTxHash functions. Use the checksigs function to verify that the signer and owner match for each signature. If matched, the transaction is considered valid and the ETH is sent to the _to address. The reason why this contract is vulnerable to Signature Reply Attack is that once the user running the contract has someone else's signature, the transfer function can be called as many times as you want, which checks the signer and owner, not the sender, so the signature is considered valid.

3. How to resolve security vulnerabilities

```
/*Transfer ether with valid signature*/
  function transfer(address _to, uint
_amount, uint _nonce, bytes[2] memory
_sigs)
    external
  {
    byte32 txHash = getTxHash(_to,
_amount, _nonce);
```

```
    require(!executed[txHash], "tx
executed");
    require(_checkSigs(_sigs, txHash),
"invalid sig");

    executed[txHash] = true;

    (bool sent, ) = _to.call{value:
amount}("");
    require(sent, "Failed to send Ether");

  }
```

You can use nonce to improve the problem of not distinguishing invalid signatures. Nonce is an arbitrary number that is issued so that it cannot be reused. In the above code, hash together using _nonce as the input value of the getTxhash function. You also use _nonce as an input to the transfer function. This allows you to create a unique transaction hash by adding a nonce. Add an executed mapping and indicate that the transaction hash with the transfer function is used through the require syntax to prevent Signature Replay Attacks on the same contract.

```
/**
 * Increment a particular maker's nonce,
thereby invalidating all orders that were
not signed
 * with the original nonce.
 */
function incrementNonce() external {
    uint newNonce = ++nonces[msg.sender];
    emit NonceIncremented(msg.sender,
newNonce);
}
```

Similar to the above, opensea conducted an update to Wyvern Exchange version 2, which adds a nonce variable that can identify the track section. In addition, ERC712 was applied to ensure data transparency. In Wyvern Exchange version 2, information signed by the user can be directly checked in the form of a structure.

C. *Countermeasures against NFT phishing attacks*

When logging into an NFT exchange or wallet site, NFT owners should always verify that the site is legitimate. It's important to verify the email domain and enter the URL address correctly, and when you receive a message like an email, it's best to go directly to the site and log in without clicking on the link. It's also important to take full advantage of security features on NFT exchanges and wallet sites. You can use two-factor authentication, biometrics, security programs, and more to protect your personal and wallet information. Finally, when trading NFTs, it's important to trade on a legitimate exchange. By trading on a legitimate exchange, you can avoid phishing sites and ensure the safety of your NFT transactions.

V. References

[1] 정세희 and 이창무, "국내 NFT 거래의 보안 위협요소에 관한 연구", 2022

[2] "How to Steal User's Signature in NFT Phishing Attacks", Medium Blog, last modified Jun 14. 2022, accessed Jun 8. 2023, https://medium.com/@Beosin_com/how-to-steal-users-signature-in-nft-phishing-attacks-13d7e7580dc5

[3] "[Hacking Series] #04 Signature Replay", Medium Blog, last modified Jan 19. 2023, accessed Jun 8. 2023, https://medium.com/decipher-media/hacking-series-04-signature-replay-41f4d2f8146c

[4] "Signature Replay", Solidity by Example, accessed Jun 8. 2023, https://solidity-by-example.org/hacks/signature-replay/

[5] "ERC-191:Signed Data Standard", Etuereum Improvement Proposals, last modified Jan 20. 2016, accessed Jun 8. 2023, https://eips.ethereum.org/EIPS/eip-191

[6] "ERC-712: Typed structured data hasing and signing", last modified Sep 12. 2017, accessed Jun 8. 2023, https://eips.ethereum.org/EIPS/eip-712

[7] "Opensea: Wyvern Exchage v1", Etherscan, accessed Jun 8. 2023, https://etherscan.io/address/0x7be8076f4ea4a4ad08075c2508e481d6c946d12b#code

[8] "Opensea: Wyvern Exchage v2", Etherscan, accessed Jun 8. 2023, https://etherscan.io/address/0x7f268357a8c2552623316e2562d90e642bb538e5#code

[9] "Wyvern Protocol in Opensea NFT Marketplace", Medium Blog, last modified Mar 6. 2022, accessed Jun 8. 2023, https://victoryeo-62924.medium.com/wyvern-protocol-in-opensea-nft-marketplace-b0cef9a9143a

[10] Ben Luke, A. S. & Stoilas, H. WTF are NFTs? Why crypto is dominating the Art market. (2021). https://www.theartnewspaper.com/podcast/wtf-nfts. (Accessed 4 May 2021). (The Art Newspaper).

[11] Team, N. Non-fungible tokens quarterly report Q1 2021. (2021). https://nonfungible.com/subscribe/nft-report-q1-2021. (Accessed4 May 2021). (NonFungible Corporation).

[12] Evans, T. M. Cryptokitties, cryptography, and copyright. AIPLA QJ 47, 219-247 (2019).

[13] Lounge, T. W. Choosing the right blockchain for your NFT. (2020). https://medium.com/phantasticphantasma/choosing-the-right-blockchain-for-your-nft-didf2bebae91. (Accessed 4 May 2021). (Medium).

[14] Team, C. (2021). CryptoKitties: Collect and breed furrever friends. https://www.cryptokitties.co/. (Accessed 4 May 2021). (Cryptokitties).

[15] Wong, J. I. The Ethereum network is getting jammed up because people are rushing to buy cartoon cats on its blockchain. (2017). https://qz.com/1145833/cryptokitties-is-causing-ethereum-network-congestion/. (Accessed 4 May 2021). (Quartz).

[16] Tepper, E. People have spent over \$1 m buying virtual cats on the Ethereum blockchain. (2017). https://techcrunch.com/2017/12/03/people-have-spent-over-1m-buying-virtual-cats-on-the-ethereum-blockchain/. (Accessed 4 May 2021). (TechCrunch).

[17] Riegelhaupt, R. Results: Beeple's purely digital NFT-based work of Art achieves \$69.3 million at Christie's. (2021). https://www.christies.com/about-us/press-archive/details?PressReleaseID=9970&lid=1.(Accessed 4 May 2021). (Christie's Press Release).

[18] Reyburn, S. JPG file sells for \$69 million, as "NFT mania" gathers pace. (2021). https://www.nytimes.com/2021/03/11/arts/design/ nft-auction-christies-beeple.html. (Accessed 4 May 2021). (The New York Times).

[19] Phillips, D. The 10 most expensive NFTs ever sold. (2021). https://decrypt.co/62898/the- 10-most-expensive-nfts-ever-sold. (Accessed 20 May 2021). (Decrypt).

[20] Howcroft, E. "Cryptopunk" NFT sells for \$11.8 million at Sotheby's. (2021). https://www.reuters.com/technology/cryptopunk-nft-sells-118-million-sothebys-2021-06-10/. (Accessed 25 June 2021). (Reuters).

[21] Devlin, J. The "insane" money in trading collectible cards. (2021). https://www.bbc.co.uk/news/business-56413186. (Accessed 20 May 2021). (BBC).

[22] Matthieu Nadini “Mapping the NFT revolution: market trends, trade networks, and visual features”