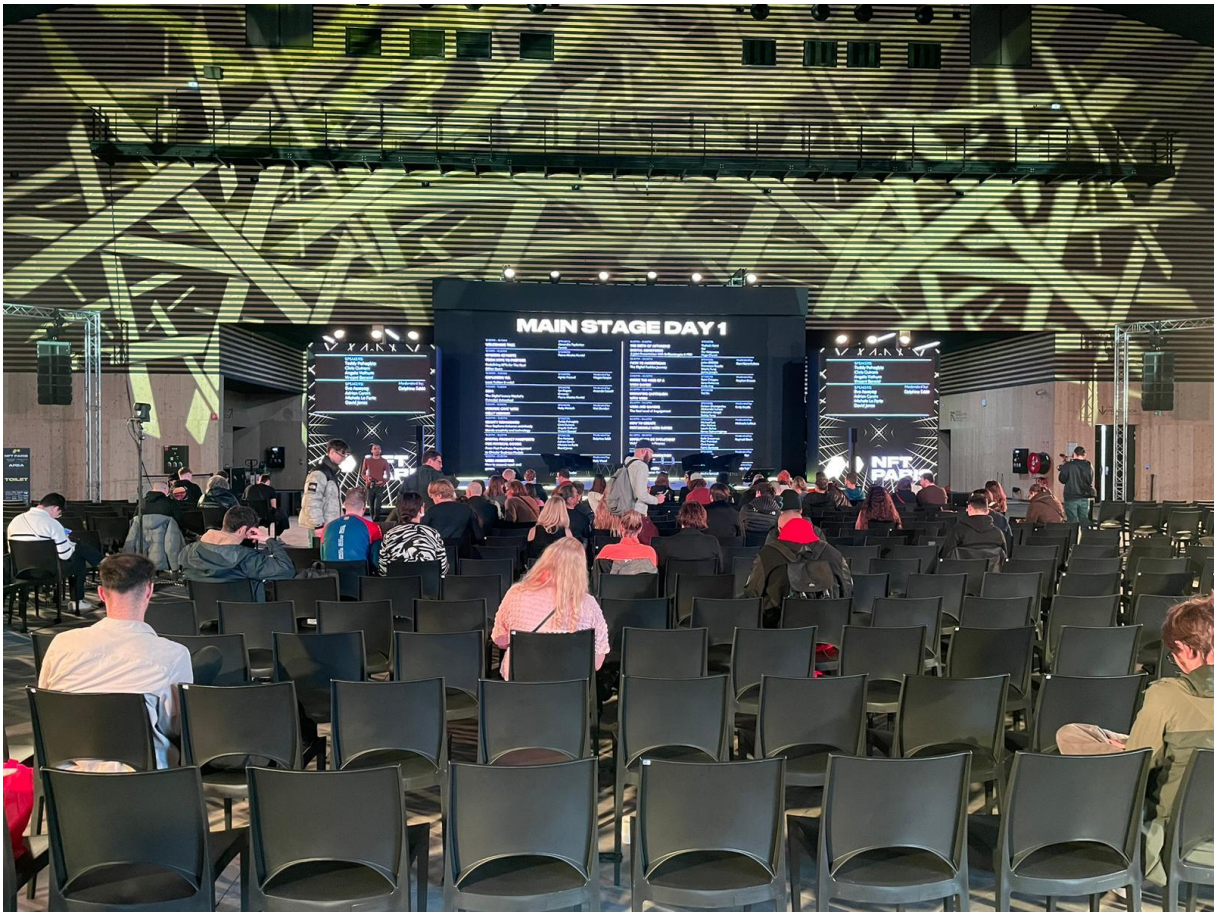
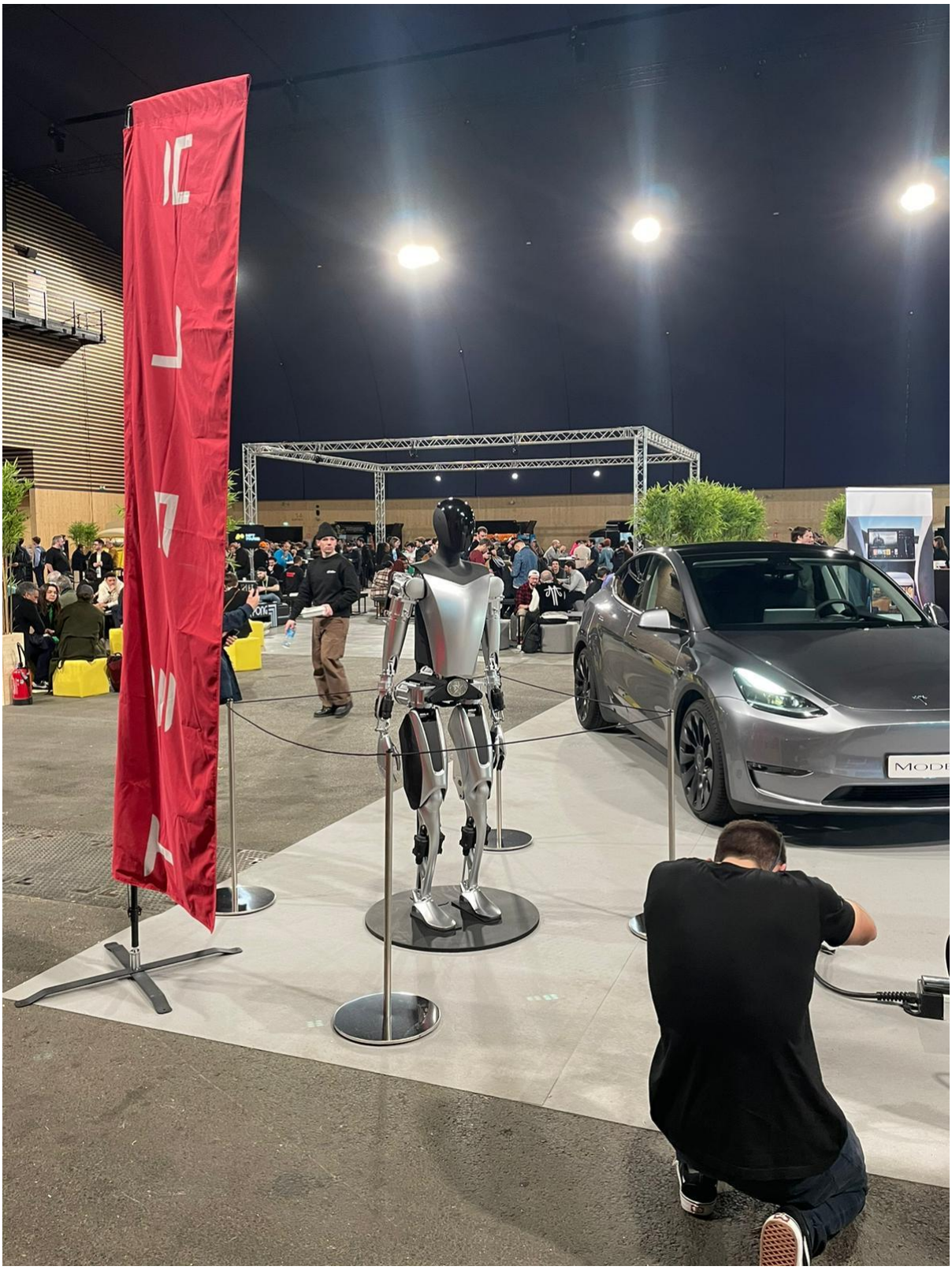
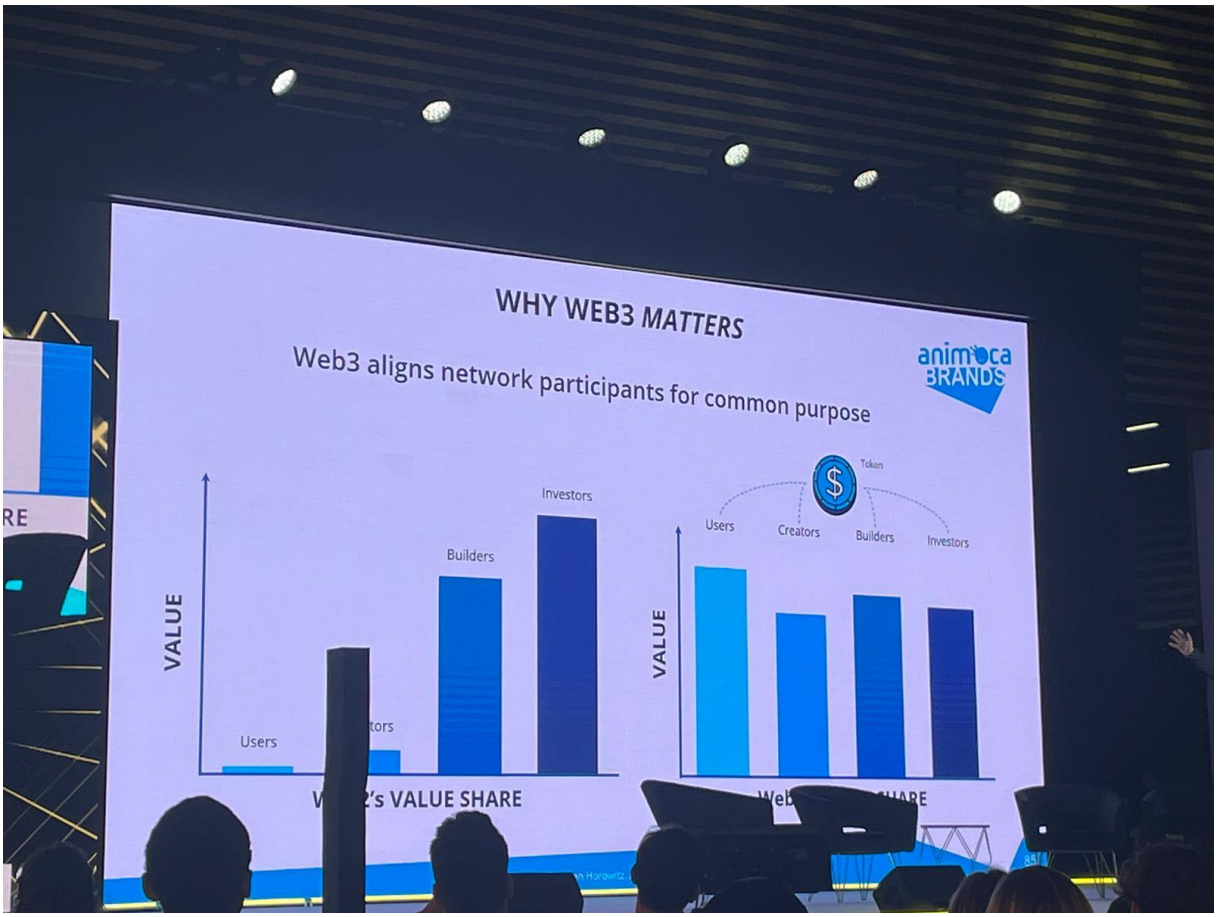
Homework 4

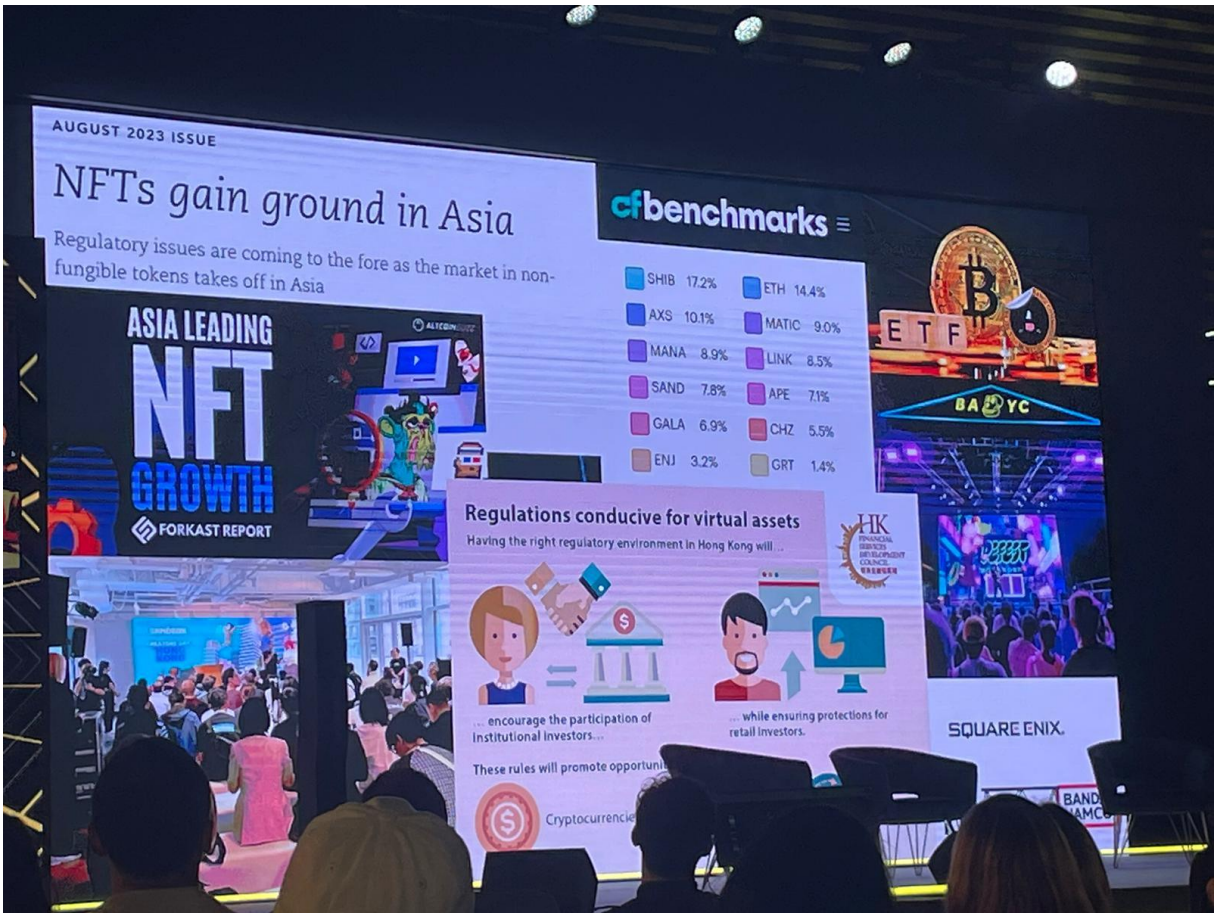
Bonus point exercise – NFT Paris Week

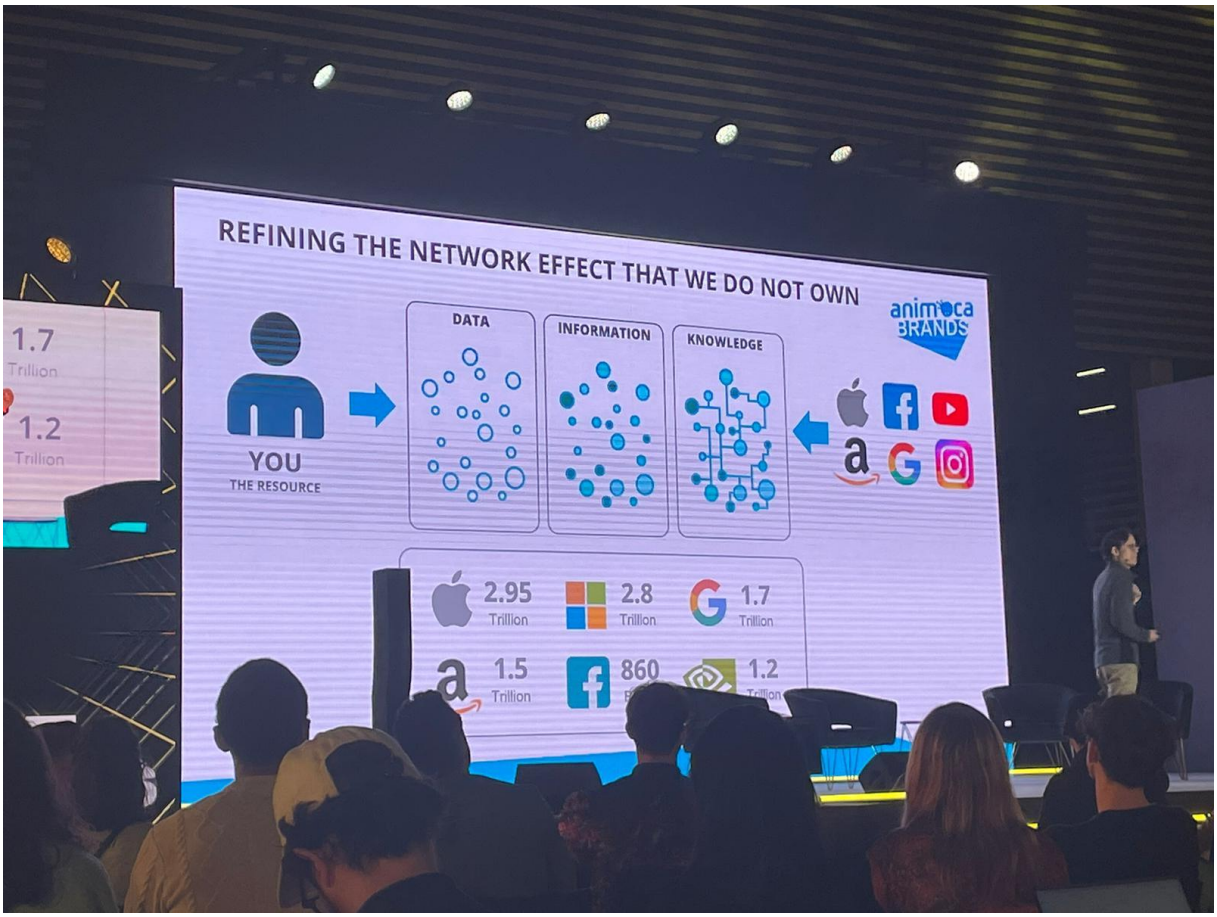
Pictures






WHY WEB3 MATTERS
Web3 aligns network participants for common purpose
animoca BRANDS
VALUE
Users
Builders
Investors
Token
Users
Creators
Builders
Investors
VALUE


AUGUST 2023 ISSUE
NFTs gain ground in Asia
Regulatory issues are coming to the fore as the market in non-fungible tokens takes off in Asia
cfbenchmarks
SHIB 17.2%
ETH 14.4%
AXS 10.1%
MATIC 9.0%
MANA 8.9%
LINK 8.5%
SAND 7.8%
APE 7.1%
GALA 6.9%
CHZ 5.5%
ENJ 3.2%
GRT 1.4%
ASIA LEADING
NFT
GROWTH
FORKAST REPORT
Regulations conducive for virtual assets
Having the right regulatory environment in Hong Kong will ...
... encourage the participation of institutional investors...
... while ensuring protections for retail investors.
These rules will promote opportuni
Cryptocurrencie
ETF
BAYC
SQUARE ENIX.


REFINING THE NETWORK EFFECT THAT WE DO NOT OWN
animoca BRANDS
DATA
INFORMATION
KNOWLEDGE
YOU
THE RESOURCE
1.7
Trillion
1.2
Trillion
2.95
Trillion
2.8
Trillion
1.7
Trillion
1.5
Trillion
860
1.2
Trillion


Web3 gives people property rights:
the ability to own a piece of the network
Web1
Read
Web2
Read
Write
Web3
Write
Own
Own

I attented the NFT Paris Week on Friday afternoon, and I mostly listened to four different conferences. Here are 6 pictures that I took during the event, the first one being the schedule for the conferences (Sadly, the picture isn't cleared enough to see the schedule). I attended to 4 first of the afternoon, which were on the following topics (I sadly don't remember the names of the speakers, but I remember the name of some companies and people:

- Digital Fashion going mainstream: Someone from DressX, CybrMagazine and from CuteCircuit (the person in question used to work for a big fashion brand) were there ;
- Web3 Game : Founder of CrossTheGaesTCG, AlienWorld, and someone from a company that, if I understood well, invests in Web3 ideas ;
- Another Web3 gaming conference, but I don't remember much about it ;
- AnimocaBrands : the founder of it.

Besides the conferences, I looked at what was going on around; there was a stand for Tesla (which may not be that surprising knowing Elon Musk seems quite invested in Cryptocurrencies), a stand for AnimocaBrands, a few physical creation with NFTs proving ownership (some kinds of lights as art pieces). One stand was proposing to transform NFT image into real world "painting". Eventually, there was also a big "stand" with fashion shows going on, and, although it was not that interesting to me, I think it was about digital fashion.

From the conferences, I learnt a lot about digital fashion, and I had absolutely no idea about it. I definitely think this is something with potential, particularly if some kind of metaverse was to actually exist. CuteCircuit made a big collaboration with Katy Perry, which is a first step to get recognized; the goal of them is to get into the Fashion Week, similarly to other "physician" fashion brands. They talked about the use of IA to "dress" online characters, or even a picture of yourself, in order to see how a new dress/shirt… would fit on you, without having to physically wear it.

About Web3 games, as I like video games, I was very interested to discover this world; this is not something mainstream yet, but I found some good ideas, and the use of NFTs makes much more sense to me in this case (for example, the game CrossTheAges proposes cards that are actually NFTs, so you own your cards). From what I've understood, they would really like that a big player (like Epic Games) enter the Web3 experience, such that many new gamers would join the game (they believe gamers would, afterwards, prefer Web3-based games, due to their incentives, than old games). This is an aspect of Web3 that I definitely want to take a look at, and I even downloaded CrossTheAges, as it reminds me of HearthStone, another cards-game.

Eventually, the most interesting conference was held by the founder of AnimocaBrands; he talked about Web3 in general, and the DeFi. The pictures of slides I took were part of his presentation, which was very clear and showed the great opportunities, changes and solutions that Web3 gives to the world.

Exercise 2 – Writing Technical Specifications

To integrate EIP-4337 into the NFT project for Boonty, and create a Technical Specification that outlines the upgrade process and its benefits, I'll follow a structured approach similar to that of official Ethereum Improvement Proposals (EIPs). EIP-4337, also known as Account Abstraction (AA), allows for a more user-friendly experience.

Technical Specification for EIP-4337 Integration in Boonty's NFT Project

1. Abstract

The implementation of EIP-4337 will involve deploying your smart contracts in a way that operate within the new paradigm of account abstraction on Ethereum. The implementation of this proposal will allow users to use smart contracts wallets containing arbitrary verification logic instead of EOAs as their primary account, making it easier for non-frequent users of web3.0 technology. This proposal avoids Ethereum consensus change, increasing the chance of faster adoption by the community. Moreover, it can change a lot the way transaction fees are dealt with.

2. **Motivation**

The current user experience for interacting with Ethereum-based NFTs requires users to have a funded wallet to cover gas fees. Particularly, as web 2.5 company, Boonty may not be only used by web 3.0 enthusiasts, which would make some people lost in this new paradigm; some would have to create a wallet, fund it with the ERC20 token necessary for gas fees, and mint the rewards. For new users, or people that would only use that for these specific NFT rewards, this may be unattractive. This barrier can deter potential users unfamiliar with cryptocurrency from participating in Boonty's NFT loyalty program. By implementing EIP-4337, we aim to, we solve this problem, allowing Boonty to touch a wider population. Moreover, thanks to EIP-4337, we can build privacy-preserving applications, that can deal effectively with atomic multi-operations, and, most importantly for Boonty, a huge change can be brought for transaction fees; firstly, they can be paid with ERC-20 tokens, letting people a wide choice and some liberty to choose the token they want and/or have easily access to. Secondly, developers can pay fees for their users, meaning they can sponsor their transactions. These two particularities can be of interest for Boonty and the companies dealing with it, as they can pay for the fees when minting rewards, which is the pure definition of a reward; something free that you deserved.

3. Specification

3.1 Definitions

3.2 User Operation, EntryPoint, and Paymaster Contracts

- **UserOperation** : An ABI-encoded struct which avoids Ethereum consensus changes. Users put the action they want their wallet to take inside the UserOperation (for instance, minting an NFT). It includes information on the sender, the nonce, the data to be called, gas… and, importantly, this is where you can specify if the transaction is sponsored by a "paymaster". "UserOperation" objects are then brought to the user operation mempool, in which bundlers will create bundle transactions (bag of multiple UserOperation call to a pre-published global entry point contract).

- **EntryPoint** : Serves as the network's gateway for processing UserOperations. It validates operations, manages execution, and, in our case, support paymasters that can sponsor transactions. The entry point itself creates wallets.

- **Paymaster** : A contract that agrees to sponsor gas fees for specific UserOperations. It contains logic to verify whether it will sponsor an operation based on predefined criteria.

To implement EIP-4337, you'll have to create a contract for the wallet, and for the paymaster.

3.3 NFT Contract Interaction with Paymaster

The NFT contract will be modified to construct `UserOperation` instances for actions like minting and evolving NFTs. These operations will specify the Paymaster contract as the gas fee sponsor, abstracting the gas fee management from the users.

4. Rationale

EIP-4337's account abstraction provides a flexible and user-friendly approach to managing blockchain interactions. By abstracting the complexities of gas management and transaction signing, we can offer a seamless experience for users participating in the loyalty program.

Incorporating a Paymaster provides a flexible mechanism for managing gas fee sponsorship. It allows Boonty to define specific criteria for sponsorship, such as sponsoring only the first minting operation of a new user or special promotions, thereby optimizing engagement costs and incentivizing desired user behaviors.

6. Technical Implementation

-**Implement a smart wallet contract** for each user, that acts on behalf of them

-**Deploy Paymaster Contract**: Deploy a Paymaster contract on Ethereum that implements the `IPaymaster` interface. This contract should be capable of deciding which operations to sponsor based on the logic defined by Boonty.

-**Integration with EntryPoint**: Ensure that the EntryPoint contract can interact with the deployed Paymaster, allowing UserOperations to specify the Paymaster as their sponsor. The NFT contracts deployed by Boonty should recognize calls from smart wallets.

-**Modify NFT Contracts**: Update the NFT contract to prepare `UserOperation` instances for user actions, specifying the Paymaster as the gas fee sponsor. This will likely involve creating a function that constructs and signs `UserOperation` instances on behalf of users. Ensure also that contract's functions that require user identification or permission checks are compatible with calls made by smart wallet contracts on behalf of users.

-**Relayer Network**: Implement or integrate with a relayer network capable of forwarding UserOperations to the EntryPoint. The relayer will need to handle the submission of operations and manage the reimbursement from the Paymaster.

-**Monitoring and Management Tools**: Develop tools for monitoring transactions, managing the Paymaster's balance, and adjusting sponsorship policies as needed to ensure the sustainability of the sponsorship model.

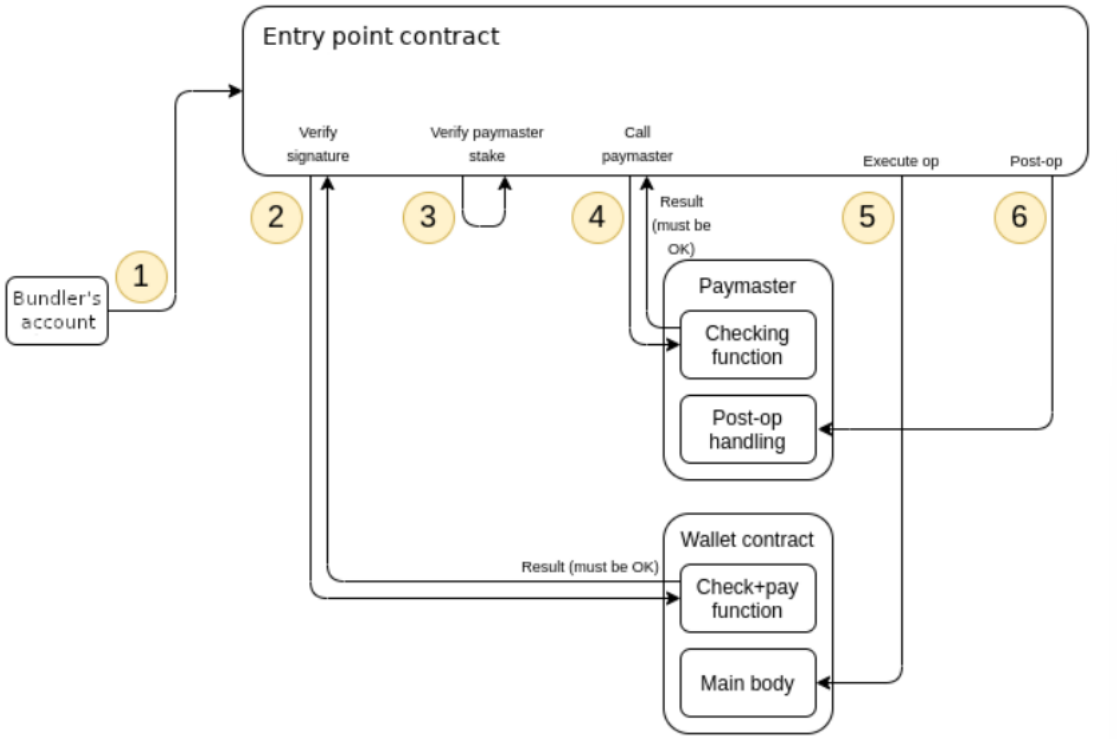
7. Benefits

- **User-Friendly**: Eliminates the learning curve associated with Ethereum gas fees and wallet management.

- **Increased Engagement**: Lowers the barrier to entry, encouraging more users to participate in the loyalty program.

- **Cost Efficiency**: Allows Boonty to sponsor gas fees for specific interactions, optimizing engagement costs.

8. Architectural Diagram



9. Conclusion

By integrating EIP-4337 with the addition of a Paymaster into Boonty's NFT project, we significantly enhance the platform's usability and accessibility. This approach not only simplifies the user experience but also provides Boonty with a powerful tool to manage engagement costs and incentivize user participation through sponsored transactions.

Pseudo-Code

Wallet interface

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;


interface IWallet {
   function validateUserOp(
      address user,
      uint256 nonce,
      bytes calldata signature,
      bytes calldata callData
   ) external view returns (bool isValid);


   function executeUserOp(
      address user,
      uint256 nonce,
      bytes calldata signature,
      bytes calldata callData,
      uint256 callGas,
      uint256 verificationGas,
      uint256 preVerificationGas,
      uint256 maxFeePerGas,
      uint256 maxPriorityFeePerGas,
      address feeToken,
      uint256 feeAmount
   ) external payable;
}
```

You would need **to** implement the IWallet interface in a Smart Contract Wallet, for a smart contract wallet with EIP-4337 compliance.