Aliens vs People
**Disclaimer**

The project is for the sale of **ART COLLECTIBLES** in the form of NFTs (non-fungible tokens) only.

This document is intended for **INFORMATION PURPOSES ONLY**, and may not be incorporated into any contract. Nothing herein constitutes legal, financial or investment advice. It is not a promise, binding agreement, or legal obligation to deliver any material, code, or functionality, and should not be relied upon in making purchase decisions. The development, release, and timing of any products, features or functionality is solely at our discretion, and subject to change.

Your NFTs should not be used for investment or speculative purposes.
# Table of Contents

**Part 1: Background**  
1

**Part 2: Technical Decisions**  
2
- Platform  
2
- Game Criteria  
2
- Game Type  
2
- WebRTC  
2
- Blockchain  
3

**Part 3: Legal Considerations**  
5
- Strategy  
5
- Rewards  
5
- Timeline  
5

**Part 4: The Game**  
6
- Gameplay  
6
- Conclusion  
7
Part 1: Background

Aliens vs. People spawned from a simple idea: NFTs shouldn’t just be functionless JPEGs. They should provide some utility. Some enjoyment. Something that keeps NFT holders coming back for more. Something that not only excites holders, but also motivates the entire blockchain community to build projects that offer more than just JPEGs.

Hence the decision to make a game. Preferably, an entirely on-chain game. A game that will be as timeless as Monopoly or Battleship. These games will be enjoyed by people hundreds of years from now, just as much as they were enjoyed by people almost a century ago. These classics have been played for generations for nothing more than the enjoyment they bring. Think of your favorite games. How many of them give you something of value beyond the enjoyment they bring? We want to build a game that is equally timeless. Not something you play just to earn rewards, but something that is so irresistibly fun that the game itself is the motivation to keep coming back.

Equally, the game should be enjoyable by everyone. From kids to their grandparents. By people from all walks of life. By people in every inch of the world. Blockchain is for all and inclusive; it knows no gender, race, geographic boundaries or age. If our game is to truly embrace the principles of blockchain, it too must be for all.

So, our criteria was simple:

1. The game should bring enjoyment in and of itself
2. The game should preferably be on-chain (but definitely decentralized, transparent and immutable)
3. The game should be playable by anyone and everyone

The answer?

Aliens and people are embroiled in an intergalactic war. In a Battleship-style game, the two sides must destroy each other’s fleet. Winner doesn’t go extinct, d’oh!

But before we get into specifics of the gameplay, let’s first discuss the technical and legal limitations that defined our decisions.
Part 2: Technical Decisions

Platform
Let’s start with why Solana.

If our goal is to make an on-chain game, we need fast transaction times, low gas fees and capacity for a large number of transactions per second. Solana hits the mark.

There are, of course, several other major benefits – but we won’t bore you with the geeky details that get us excited. Suffice is to say that we were impressed by Solana, and wanted to be an early part of its ecosystem.

Game Criteria
There are several technical criteria that our game would need to satisfy:
1. Secret State: Users must be able to submit their position (e.x. 100x80 on a grid) without it being readable by everyone else
2. Multiple Players: The game should be playable by thousands of NFT holders simultaneously
3. Transparent: Anyone should be able to view the raw gameplay and build their own frontend around it
4. Immutable: Developers and players cannot manipulate or falsify the gameplay
5. Decentralized: No central authority should be able to control any element of the game

Game Type
If we don’t use state channels, an MMORPG game would be a dreadful experience.

Imagine every action - every move, every kick, every punch - having to be pushed to the chain before it’s reflected in the gameplay. There couldn’t be real-time interaction between users.

If our best option is to be entirely on-chain, we would need a strategy-based game where waiting is the expectation and doesn’t detract from its enjoyment. Not something with a kick or punch that takes minutes, or even seconds, to reflect in the game.

So, is a game that uses state channels possible based on our criteria?

Let’s discuss.

WebRTC
One possibility in building a peer-to-peer game is skipping the blockchain altogether. Instead, using WebRTC, which permits direct communication between players. This is the approach many purported “blockchain” games have used.

Typically, a game server (assumedly ours) would be needed for signaling (to connect all parties), and
possibly serve as the single source of truth. Without it, each player would need to be the authority for their own moves, thereafter broadcasting it to everyone else and hoping they update the game states (even if they’re going to lose).

With the help of a hash (“Merkle”) tree, we could store the game state on the blockchain and prevent cheating. Using state channels would reduce the number of on-chain transactions, but there still remains a multitude of issues that make WebRTC an unideal solution for our needs.

Specifically:
1. The need for a central signaling server to connect the players
2. Peer connection limits. For example, Chrome has a soft limit of 256 simultaneous connections. That’s far too few for a game that will be enjoyed by thousands of players. Even if everyone could connect, the bandwidth requirements for a session that large would make the game unplayable for those with lower bandwidth
3. Privacy concerns, such as WebRTC leaking real IP addresses – which could then be linked to the players’ wallet addresses holding the NFTs

There are certainly benefits to using WebRTC and state channels. However, noting the issues above, it just wouldn’t work for us.

**Blockchain**
Before we can begin our on-chain game, we need to consider several caveats.

First, given the transparent nature of blockchain, players’ positions would be immediately readable by everyone. Woops!

What if users cryptographically hash their location with SHA256? Problem is, with a limited number of possible locations and SHA256’s deterministic output, one could easily determine the hashes of all possible points. So, a user’s position could be determined from simply looking at the corresponding hash. Ouch.

What if we add a “salt” to the hash? Basically a secret user-generated key, which is coupled with their position to generate the hash. But, this secret key would still need to be sent to the smart contract to decrypt the position. When sent on the blockchain, this secret key would then be known to all participants. You can see the issue.

What if we let users submit their hashed position with a secret key, followed by their guesses about others’ positions, and then the original secret key to decrypt their own position? The smart contract can then determine the users’ original positions, while, already having the guesses so that they can’t be changed. This is called a “commit/reveal” scheme. Now we’re on to something.

We of course need to add other game mechanics to prevent cheaters. This includes setting time limits to disqualify users who don’t share their secret keys (because they know someone got their position), or
those who try to submit their strikes after the secret keys have already been revealed.

There are some better methodologies, such as zero-knowledge proofs (“ZKPs”), as well as its adaptations in the form of zk-SNARKs and zk-STARKs. Here, a user would be able to prove their position, without actually revealing it. However, no implementations of ZKPs exist on the Solana blockchain yet.

Finally, we could use a data oracle in the smart contract, but this would require a trusted third-party and alleviate from our goal of being a strictly on-chain game. Plus, trusted solutions like Chainlink only offer price feeds for the Solana network at this time.

In conclusion, we decided on a strategy-based game that operates on the Solana blockchain, using a commit/reveal scheme.
Part 3: Legal Considerations
We want our game to be accessible by everyone.

To ensure this, there are several considerations that went into the gameplay.

Strategy
Our game should be based on strategy and not just pure luck. Plus, what fun is pure luck anyway?

To incorporate strategy, the game would have multiple rounds. You would not be able to place your avatar in a previously struck position, but it would nonetheless be strike-able again by the opposing team.

There would also be a chat room, accessible to only those on the same side. This way, teams can collaborate on where to strategically position their avatars. Imagine all team members colluding to place their avatars on the exact same position on the grid, so the opposing team has a tough time finding it. Or, a naughty team member secretly placing their own avatar elsewhere, so that when the entire team gets struck – they are the only ones who survive. The possibilities are endless.

Rewards
Initially, we contemplated modifying NFTs to decorate them with their wins. But, this isn’t ideal, since first and foremost – our NFTs are art collectibles. Some people simply want their NFTs as such without any intention of participating in the game. They would justifiably be upset if others’ NFTs are decorated with medals, while theirs are not, simply due to their disinterest in participating in the game. Instead, we opted to award in-game and Discord rankings based on wins.

This also alleviates another concern, which is, that the reward should not be something of value. If we gave away something of value, validators may avoid publishing blocks that don’t serve their interests. It may also make our project into a security, since the won NFTs could be treated as dividends of an initial investment (being the purchase of NFTs). Regardless, if users were only playing our game for rewards, we didn’t do something right. Since the idea of our game was always to be a timeless classic that users play for the game’s enjoyment in and of itself.

Timeline
No empty future promises.

Our game would be ready and playable as soon as you have your NFTs to participate. This allows you to attribute a value based on our delivery at the time of mint, and, holds us accountable to deliver everything before you spend a penny.
Part 4: The Game

It all starts with a fascinating storyline:

The year is 2100.

Mars is colonized. Solana is the defacto currency. People have found neighboring aliens. And, we all surprisingly get along.

Until one day, a mysterious disease wipes fertility in all the universes. Early research shows that a distant planet may hold the ingredients to restart it. But, there's only enough juice there for one civilization. The other, will go extinct.

It will take scientists on both sides time to build robots capable of getting to the planet fast enough. But, neither side wants to wait. They cannot afford to wait. Their survival depends on it. As much as they like each other, the war must begin now. They must destroy each other for their own survival.

Hence begins the ultimate battle of the cosmos. The best warriors on each side have already volunteered. They must be found and destroyed at all costs.

So warriors, we ask you:

ARE YOU READY?

Gameplay

1. Players are either an alien or people depending on their NFT
2. Players have 24 hours to select where they want to place themselves on a 100x100 grid, i.e. 80x40
3. Players select a {secret key} that is only known to them. A unique secret key should be used by each player every time they pick a position for their avatar
4. Players submit where they want to be in the grid by sending a transaction to the game’s smart contract. Their position is stated in the transaction description in this format:

   \( \text{game #}-\text{round #}-\text{sha256(secret key,position)} \)

   Where:
   - \{game #\} is the current or future game # for which the position is being selected
   - \{round #\} is the current or future round # for which the position is being selected
   - sha256(secret key,position) is the hash of your \{secret key\} and grid position

5. Players then have another 24 hours to submit their secret key, along with where they want to “strike” the opposing team on the grid. The transaction description is formatted as such:

   \( \text{secret key}-\text{guess} \)

   Where:
- {secret key} is the unencrypted nonce used to hash their original position on the grid
- {guess} is the point on the opposing team’s grid where they want to strike, i.e. 100x20

6. Players whose positions were hit are removed from the game. Those who did not submit their {secret key}, or submitted invalid ones, lose a rank as a penalty
7. Survivors repeat steps 2-6, except, avatars cannot be placed on previously “struck” points (although, you can still strike them again)
8. Once everyone on the opposing team are eliminated, the winners are crowned

Other rules:
- If a player doesn’t submit their {secret key}, they lose a rank as penalty
- If both sides’ players get eliminated in a round, those with the most remaining players at the commencement of the round are crowned winners

**Conclusion**
At the end, we have an entirely on-chain game that meets all of our requirements. Anyone can interact with the gameplay directly from the blockchain. They can build their own use interfaces (“UIs”) if they want. The game is entirely on-chain, decentralized, immutable and can be played by all the NFT holders simultaneously.