Dark Forest:
Lessons from 3 years of on-chain gaming

gubsheep, 0xPARC
I’m gubsheep

○ Worked with the Ethereum Foundation since 2018 on education, community, and applied ZK R&D.

○ Created Dark Forest and spent 2019-2021 building it with Ivan Chub, Alan Luo, Brice Huang, Robert Cunningham, ...

○ Currently working on applied ZK R&D and other applied crypto experiments at ØxPARC.
Today’s Talk

What can projects like **Dark Forest** teach us about innovation in crypto broadly?
Dark Forest is a decentralized MMORTS game built with zkSNARKs on Ethereum.
Dark Forest is a decentralized MMORTS game built with zkSNARKs on Ethereum.
Today’s Talk

Dark Forest is a decentralized MMORTS game built with zkSNARKs on Ethereum.
Dark Forest started as a pie-in-the-sky experiment.

“Let’s build a ZK game where every WASD move triggers a transaction and a zkSNARK proof on-chain”
A lot has happened since!

- 10k+ players from around the world have participated in Dark Forest rounds, running entirely on-chain
- Trillions of gas used on Ropsten / xDAI / Gnosis Chain
- Rich developer ecosystem: plugins, alternate clients, GPU miners, player corporations, data marketplaces, chain analysis tools, and more
- Epic on-chain dramas featuring deception, betrayal, universe-wide alliances, ...
A lot has happened since!

@wilichang

Move over Star Wars.

What happened this past round of Dark Forest has to be the most epic space saga of all time.


Here’s the story.

dfdao and ordenGG have agreed to a diplomatic draw in Dark Forest v0.6.5.
A lot has happened since!

**Today:** a thriving ecosystem of “next-generation” application R&D, in the broader ØxPARC community.
QUESTION 1

Why build games on the **blockchain**?
**REASON:** Permissionless Interoperability

Dark Forest is an Ethereum **smart contract**, which anyone (player, bot, or smart contract) can interact with programmatically.
Client-side plugins

Towards Center
When you choose one planet, you can make it towards center.

Scoring Planets
See the top scoring planets within your vision.

Tiny Leaderboard
Shows a tiny leaderboard with timer.

Remote Snarker
Speed up snark computation using servers.

Heatmap
Highlight territories around you!
Third-party client implementations
Automations and bots

nick.eth @nicksdjohnson · Aug 16
Weekend project: A @darkforest_eth AI.

So far it attacks planets, distributes silver, upgrades planets, and prospects and finds artefacts.

Still on the todo list is distributing energy. Figuring out how to allocate and use artefacts will be tricky though.

<table>
<thead>
<tr>
<th>Name</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rose Sleepy (L4R0)</td>
<td>Sending 27000 silver to Oatmeal Breathe (L5R0)</td>
</tr>
<tr>
<td>Six Hiss (L4R0)</td>
<td>Sending 14250 silver to Oatmeal Breathe (L5R0)</td>
</tr>
<tr>
<td>Fog Resell (L4R0)</td>
<td>Sending 25471 silver to Onerous Jaded (L5R2)</td>
</tr>
<tr>
<td>Jail Amuck (L4R0)</td>
<td>5% to prospect</td>
</tr>
<tr>
<td>Changeable Ludicrous (L4R0)</td>
<td>Capturing Redo Convince (L5R0) with 28125</td>
</tr>
<tr>
<td>Measly Depend (L4R0)</td>
<td>12% to attack Redo Convince (L5R0)</td>
</tr>
<tr>
<td>Daffy Sneeze (L4R0)</td>
<td>10% energy to send silver to Fold Rapid (L3R0)</td>
</tr>
<tr>
<td>Otter Button (L4R0)</td>
<td>30% energy to send silver to Fold Rapid (L3R0)</td>
</tr>
<tr>
<td>Harbor Country (L4R1)</td>
<td>89% to attack Redo Convince (L5R0)</td>
</tr>
<tr>
<td>Bridge Convince (L4R0)</td>
<td>34% to attack Redo Convince (L5R0)</td>
</tr>
<tr>
<td>Lose Jail (L4R0)</td>
<td>Capturing Rhythm Snap (L4R0) with 34771</td>
</tr>
<tr>
<td>Childhood Partake (L4R2)</td>
<td>91% to attack Rhythm Snap (L4R0)</td>
</tr>
</tbody>
</table>
New core gameplay features

Project Sophon

Broadcast Market

Forget refilling across the xDai Bridge. Play to Earn with Sophon.

Each player only gets one Planet Broadcast per day—don’t waste it, you could be getting paid to play!

Just create a new plugin containing:

```javascript
1 export { default } from "https://play2earn.projectssophon.com"
```
1. (offline) I verify that
   a. Seller’s LIST proof is valid
   b. Publicly committed values are valid
2. I order listing(s) by depositing my money in the escrow smart contract
3. I preemptively declare how the final sale should be encrypted
   a. $\text{ecdh(MY PRIVKEY, SELLER PUBLKEY)}$
   b. $\text{hash(SHARED KEY)} \rightarrow \text{publish}$

Constraint
- \( \text{hash(PLANET_X/Y, PLANET HASH KEY)} \)
- \( \text{perlin(PLANET_X/Y, BIOMASS KEY)} \)
- \( \text{poseidon encode check(CIPHERTEXT, PLANET ADDR, KEY)} \)
- \( \text{hash(KEN)} \)
- \( \text{SELLER ADDR \& SELLER ADDR} \)

Publicly Verifiable Value
- A valid planet hash
- The correct biomebase
- Valid ciphertext using KEY
- KEY won’t change later
- Watermark proof to Seller
<table>
<thead>
<tr>
<th>Rank</th>
<th>Player</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>The Astral Colossus (Rank 34: 76528735)</td>
<td>76528735</td>
</tr>
<tr>
<td>1</td>
<td>@TheVelorum (Rank 189: 505491)</td>
<td>17700133</td>
</tr>
<tr>
<td>2</td>
<td>@davidryan59 (Rank 100: 5275290)</td>
<td>13898245</td>
</tr>
<tr>
<td>3</td>
<td>@scotato (Rank 228: 260000)</td>
<td>7979795</td>
</tr>
<tr>
<td>4</td>
<td>@tofu4956 (Rank 91: 8120164)</td>
<td>3747725</td>
</tr>
<tr>
<td>5</td>
<td>@jojozzas (Rank 117: 2958284)</td>
<td>3477702</td>
</tr>
<tr>
<td>6</td>
<td>@orden_gg (Rank 1: 77777777)</td>
<td>3461902</td>
</tr>
<tr>
<td>7</td>
<td>@MJ659600 (Rank 70: 38316438)</td>
<td>3347518</td>
</tr>
<tr>
<td>8</td>
<td>@xJunshen (Rank 68: 34673145)</td>
<td>3165856</td>
</tr>
<tr>
<td>9</td>
<td>0xcF0cc... (Rank 221: 281000)</td>
<td>3081000</td>
</tr>
<tr>
<td>10</td>
<td>@CryptoPriest6 (Rank 61: 48465292)</td>
<td>2822434</td>
</tr>
<tr>
<td>11</td>
<td>0x2616B... (Rank 10: 154472935)</td>
<td>2734149</td>
</tr>
<tr>
<td>12</td>
<td>@thelegendoftin1 (Rank 184: 592176)</td>
<td>2073140</td>
</tr>
<tr>
<td>13</td>
<td>@vjotav (Rank 72: 26777836)</td>
<td>1650000</td>
</tr>
<tr>
<td>14</td>
<td>@rchld123 (ex. Cassian)</td>
<td>1176701</td>
</tr>
<tr>
<td>Plugin Library</td>
<td>help</td>
<td>minimize</td>
</tr>
<tr>
<td>----------------------</td>
<td>------</td>
<td>----------</td>
</tr>
<tr>
<td>Claim Game Mode</td>
<td>edit</td>
<td>del</td>
</tr>
<tr>
<td>Artifact Shards</td>
<td>edit</td>
<td>del</td>
</tr>
<tr>
<td>Oil and Uranium R...</td>
<td>edit</td>
<td>del</td>
</tr>
<tr>
<td>Sattelites</td>
<td>edit</td>
<td>del</td>
</tr>
<tr>
<td>Add Plugin</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What does permissionless interoperability mean?

Permissionless interoperability means that players can build the game experience, not just core developers.

It means that other games can hook into your game to share assets, identity systems, mechanics, and more. No “support team” or “BD team” needed.

Marketplaces, player corporations, nested games inside games, new resources and mechanics, automations, alternate clients, interoperable assets and stats, shared reputation systems, and more...
QUESTION 1

Why build games on the blockchain?
QUESTION 2

Why build games on the blockchain?
QUESTION 2

Why build anything which we don’t have an obvious practical use case for on the blockchain?
REASON 1

Games are a technically demanding yet low-stakes environment. They allow us to rapidly push infrastructure forwards without putting massive amounts of financial value at risk.
Deleted Account
My main thing was making sure you all knew df v.05 was going to...

We have pretty big improvements on Nethermind nodes which we profiled with their team on DF after the end of the game. Will scale up infrastructure before the launch. If you have an idea how can we make a smoke test before the play test I am very interested in it

Diamonds in Projects
- Smart Contracts as Apps - EIP-2535 Diamonds and the feasibility of a DAO Operating System
- Dark Forest & the Diamond Standard - Dark Forest project moves to and discusses diamonds.
- The Diamond Standard: A new paradigm for upgradeability - DerivaDEX on diamonds.
- We like the (EIP-2535) Diamonds - Premia Finance talks about their use of diamonds.
- Why Getchvault is upgrading to the Diamond standard - How to upgrade an existing proxy contract to EIP2535 Diamonds.
- Handling multiple tokens, with a modern solidity architecture via Diamonds & ERC1155
- Smart contract packages — upgradeability for normal people

(Gnosis, Erigon, Lattice) Fast EVM chain for Dark Forest and on-chain games

A project, is working on better programming models and better infrastructure. We are investing heavily in a protocol and infra lab. The protocol lab would be programming models (we currently have an EVM EOS system) and better clients (= software), while the infra lab would work on better execution layers (= test both labs to work freely with the rest of the ecosystem (Gnosis, Erigon, OP), the software. Having them in-house with us makes it easier for them to "build what want" given we have products in production today that require much better hardware.

core: subtract deposit gas from pool, so other txs do not use the same gas #35

proto lambda wants to merge 1 commit into tx-pool-fix from deposit-gas-pool-fix

ethereal-optimism / reference-optimistic-geth

core/types: deposits do not tip, avoid basefee subtraction #37

# Closed proto lambda wants to merge 1 commit into optimise-prototype from effective-gas-tip-cap

speed up UC 100x :))

# gameboy

nalinbhardwaj committed on Aug 26

i can't ca30(()133; commit 3b292ddec5f37d47bf
REASON 2

Games are a leading social indicator in technology.

How players interact with new affordances in games gives us insight into how users will interact with digital systems of the future.
The Crypto Gaming Governance Thesis

why we’re building dfdao

dfdao experiments

As a leader of dfdao, I fully recognize the opportunity that we have for DeGov exploration. Our goal is to strive for victory in Dark Forest while using a variety of cooperative mechanisms. We hope that some of these mechanisms will be applicable to other blockchain games and eventually other DAO structures at large.
REASON 3

Games are inherently playful.

A thriving indie game community can help “bridge the gap” between technologists and creatives, artists, writers, and thinkers — introducing greater intellectual diversity to the ecosystem.
Okay, the day has finally come.

I am forced to grudgingly admit that I have found a blockchain game that legitimately does something with Blockchain that is genuinely new, innovative, and that you can't do with a centralized service.

That game is Dark Forest.
What does it mean to build for the future?
Fuck around and find out
“The Alto aimed to be not a machine of its time, but of the future... The governing principle of [Xerox] PARC was that the place existed to give their employer that ten-year head start on the future. They even contrived a shorthand phrase to explain the concept. The Alto, they said, was a time machine.”

_Dealers of Lightning_ by Michael Hiltzik
Dark Forest started as a pie-in-the-sky experiment

“Let’s build a game where every WASD move triggers a transaction and a ZK proof on-chain”
Today: a thriving ecosystem of “next-generation” application R&D, in the broader ØxPARC community
Systems vs tools
NEW EXPANSION

Brave the Beyond in Shadowlands – Buy Now

journey beyond the veil, discover five otherworldly realms of wonder and horror, gain incredible powers — and save Azeroth from all-consuming darkness.

Shop now

NEWS

Slay monstrosities in Torghast’s twisting corridors

NEWS

Jump Into This Week’s PvP Brawl: Arathi Blizzard

NEWS

Level anew with the new Threads of Fate game mode
Client-side plugins

Towards Center
when you choose one planet, you can make it towards center.

Scoring Planets
See the top scoring planets within your vision.

Tiny Leaderboard
Shows a tiny leaderboard with timer.

Remote Snarker
Speed up snark computation using servers.

Heatmap
Highlight territories around you!
@projectsonphonic/df-plugin-dev-server

An ESBuild server for Dark Forest plugin development.

Installation

You can install the command globally using:

```
npm i -g @projectsonphonic/df-plugin-dev-server
```

Usage

Once installed, you should have access to the command:

```
df-plugin-dev-server
```

You can see the supported flags by running:

```
df-plugin-dev-server
```

Start a Dark Forest plugin development server.

Options:

- `--help` Show help
- `--version` Show version number
- `--dir` The directory to load
  - [deprecated: use `--glob` instead]
  - [string]
  - [optional]
- `--glob` The glob to load
  - [string]
  - [optional]
**Light Forest - Custom Dark Forest Arena Rounds**

Light Forest is the simplest way to create a custom branded Dark Forest Arena round for your own community. It creates a website and game client for you automatically so you can focus on building your perfect game.

**Requirements**

- Install `node >= 14` (Consider using nvm)
- Install Yarn

**Install**

Click the link below to create a new repo from the Light Forest template.

https://github.com/dfdao/lightforest/generate

Or, if you have the GitHub CLI:

```
gh repo create <new-repo-name> --template=dfsdao/lightforest
```

Clone that new repo to your local machine.

**Setting up a round**

1. Visit `arena.dfdao.xyz/arena` and create a map. Once the map is created, you will get a unique hash of the map’s configuration. Copy this value and save it for later.
Dark Forest Arena: Grand Prix

One month ago, we launched a public play test for Dark Forest Arena, a short, action-packed version of Dark Forest.
Systems vs tools
Playing the infinite game
“There are at least two kinds of games: finite and infinite”
“A finite game is played for the purpose of winning, an infinite game for the purpose of continuing the play.”
“To play Dark Forest is to build on Dark Forest.”

- DFDAO
An Evening in the Dark Forest - Tuesday 4:30PM - 8PM
Autonomous Worlds Arcade - Wednesday 4PM - 7PM
Applied ZK SLS - Thursday 10AM - 6PM
Autonomous Worlds SLS - Friday 10AM - 3:30PM
ZK Community Hub - Continuous, Tuesday through Friday