Project Briefing — Blockchain for Video Game Distribution

Thomas Smith (tcs1g20)
Supervisor: Leonardo Aniello

Video game developers often rely on a third party to help sell and distribute their games on PC. By taking Steam as an example, we can show how developers would benefit from a decentralised distribution network:

Issue	Steam	Decentralised Distribution
Cost to distribute	A 30% cut on all sales made on Steam.	Initial infrastructure to distribute to the first set of nodes. Users can be rewarded for contributing through in-game rewards, which have minimal cost.
Censorship	Steam has control over what games are on their platform. Steam can ban users, who will lose access to their entire games library. The Chinese version of Steam is heavily restricted due to the Chinese government.	As a public network, any developer can upload games and seed themselves. Users are a resource to the network and won't be banned permanently. No central party means that governments cannot restrict access.
Availability	Large infrastructure means great availability for users to access games. If Steam goes down, then all users are affected and cannot access services.	Distribution comes down to demand for game and the quality of rewards for contributing. The network can still function even if some nodes go offline.

In our case, a node is used to refer to the underlying software that performs actions on behalf of the user. Whereas the term "user" is used to imply some form of human-computer interaction.

Filecoin offers cloud storage to users who "rent" storage space off nodes in the network. Estuary is a web application that uses Filecoin as a way of storing public data and allows any user to verify that a piece of data is stored on it. In contract, this project is specifically tailored towards sharing software and its subsequent updates and being able to identify specific node's contributions on sharing a given piece of software.

Goals:
The goal of this application is to create a video game distribution platform, which allows developers to independently release their games whilst being able to offer high availability and be immune to censorship from larger bodies *(like governments)*. Blockchain technology should enable this through its trustless property and means that users can trust the software they receive through the network and be able to use public key infrastructure to verify the uploader of the software.

An important aspect to the success of this project is for users to have a way of paying for software and then having to show that proof before being allowed to download and distribute the software. On top of this, users who do contribute to the distribution will need a way to prove that they have; I believe implementing a proof of space time algorithm (like the one used by Filecoin) could enable this.

Scope:
For this project to be functionally successful, it should at minimum:

- Distribute software between nodes by sharing fixed length shards of data.
- Store metadata about software on the blockchain including a Merkle Tree and a root hash to assist in the identification and verification of the software.
- Allow developers to publish games to the blockchain. It should also allow them to publish updates by referencing previous blocks in the blockchain.
- Use proof algorithms to determine a node's contribution.
- Use encryption techniques to help with the secure sharing of shards between nodes.
- Offer a command line interface for users to interact with the network.
- Use digital signatures to verify the identity of uploaders.
- Support a proof of purchase method to be called before downloading.

This project will not:

- Offer a graphical user interface for users to locate software.
- Implement the ability to pay for games through the network, although strategies may be discussed.