Report Plan

Note Created: 2022-03-24 [[ReadMe Summary]]

Introduction

- Summary of the literature review capturing the key points as follows
    - Brief intro into browser based mining and its potential use as a monetisation method that is preferable to pre-existing methods i.e. subscription/freemium/ads
    - Current blockchain/cryptocurrency technology is not inducive to browser based mining due to its scalability issues (mining difficulty increases) when a currency user base grows. Blocking easy access to the mining system. **Hardware Inequality problem**.
    - Brief Description of some potential use cases (Educational platform, opensource project funding/attribution of ownership)
        - For these applications to be feasible the mining methods of cryptocurrencies need to be improved, to provide stability and increase scalability without restricting content access.
    - This report outline a dedicated decentralised cryptocurrency that is only minable via a permissioned pool... providing the stability and accessibility these applications require

A summary of the literature review and project spec (Part of markscheme)

- I will take the following sections?
    - Section 1.2 (cryptocurrencies and Browser based mining)
    - The summary section of consensus algorithms
    - Summary of mining pool section
    - Numbered table of the project goals (for reference in the evaluation section of the report)

WhitePaper section (Spec and Design Mark scheme Criteria)

Overview Of Design

- Review/State the purpose of the proposed solution
    - To support a browser based mining ecosystem(s) by allowing users to have access to content for "free" where the *price* paid is the mining of the cryptocurrency, which is rewarded directly to the content host.
- Open with an architecture image detailing:
    - The blockchain network (highly abstracted, just some nodes connected together)
    - The mining pool
    - The authentication server
    - Browser clients connected to the mining pool (perhaps noting different use cases)

- Description of how the components work together
    - Mention that I am using PoW

Mining Pool Details

- Mining pool is the key component which changed how my system works compared to typical blockchain infrastructures

Reward Function & mining Throttling

- In order to allow low powered devices to be able to feasibly "compete" in the POW mining process (and decouple the hardware from the rewards) The mining pool operates a custom reward Function
- Details of reward function (possibly some space for a mathematical formula here just to look clever haha)
    - Miners are able to mine in the pool until they submit a threshold number of shares (shares would hopefully be adequately explained in the lit review summary section)
    - Once that threshold has been reached they become eligible for the reward (of course this goes to the content creator so might need to find a better way of wording this)
        - Once this threshold has been met they will not receive any additional reward if they continue mining, thus there is no incentive to do so
    - The reward that the content creator receives is a proportion of the total block reward based on the number of users that mined "for them" during the block cycle
    - Once a miner submits a block solution to the pool, the pool verifies the hash and submits it to the blockchain, Receiving the block reward, which is then distributed according to the reward function (outlined above)
    - This decouples the hardware quality/power from the mining process as within any particular block cycle any one user is caped to the threshold
- This process allows PoW mining to be a measure of engagement, a proxy for a proof of time, with time spend mining = time spent using the resource.

Permissioned & authenticated (Security)

- This is only possible as the mining pools are controlled by a central authority and mining is only possible via those pools. This means PoW is not responsible for block consensus as that is the role of the "trusted" mining pool nodes
- This is what allows the alteration to the mining incentives
- Mining nodes can only be accessed when miners have been authenticated via a "typical" authentication server. This ensures that mining/rewards can be accurately used to monitor engagement as mining is only possible when engaging with content.(Via the authentication portal)

Network/Interaction Diagram (outlining how a user would interact with the system?)

- Scope to discuss the "protocol" that allows the system to function
    - Authentication via server
    - requests new connection from mining pool
    - miner uses the connection until mining is stopped.
    - **This would need formalising, which would be easier if the practical application was working**

    -

Security Concerns (Threat Modelling)

- Potentially talk about the Sybil attack/bot issue...
- With some proposed solution, Chain of trust, Network analysis

Implementation Section (If it ever f***ing works)

- Not sure about this section. I would like to talk about the difficulties associated with forking a cryptocurrency i.e. security through obscurity problems, and also detail the non-triviality/devops associated with hosting this platform.
- At the same time I'm not sure how to incorporate this yet, especially given the system is barely working
- In an Ideal world I will get over these implementation bottlenecks, quickly slap together a website and so some mining simulation stuff using the browser

Discussion about potential applications

- Detailed discussion about applications
    - Educational platform
    - Application to a tokenised internet (copyright attribution)
- Again not sure how I'm going to bring these together or how they really fit

Evaluation

Conclusion