Presentation Guide

Note Created: 2022-01-28

- Recap the purpose of the project
    - Proposing a mining in the browser solution
    - Which will act as an alternative to traditional monetisation
    - Which are flawed, Ads -> privacy concerns, Freemium -> require content creators to reach critical mass
    - My system allows users to directly fund content creators whilst they consume the content **Next Slide**
- The current State of cryptocurrency cannot support browser based mining
    - External Volatility greatly impacts the profitability
    - Whilst mining difficulty drives an increased need for more powerful hardware.
    - This causes a hardware inequality where only powerful (and thus expensive) hardware are able to feasibily compete in the mining market.
- In order for pay-as-you-go mining model to work, hardware power must be disconnected from the proof of work system.

Next Slide

- In enters my proposal
- where all miners are rewarded equally regardless of the amount of work they performed
- This is made possible by having users connect to a centralised mining pool
- Centralising the pool allows the mining process to be decoupled from the consensus problem as consensus of the chain is ensured by the centrally controlled pool.
- This is important as it allows the reward structure to be changed as it is no longer necessary for incentivising against bad actors.
- This means that instead of rewarding users based on the amount of work they put in (favouring powerful hardware) it can instead reward all users that meet a minimum work threshold.
- Essentially users will submit valid shares to the pool, until the threshold is met and then no further work will be necessary.

Next Slide

- Rewards are then distributed equally.
- Each new block added to the chain will have a fixed reward (much like bitcoin)
- But instead of rewarding a single user (in a single miner example) or distributing to users in the pool based on the amount of work they performed all users will receive the same amount. (a proportion of the reward based on the current number of miners)
- So if there are 5 miners that meet the work threshold and the block reward is 5 coins then each gets a coin

Next Slide

- In the pay-as-you-go monetisation method instead of the these coins being sent to the miners they are instead directly sent to the content creators.

- This means that content that is being more heavily consumed or utilised receive greater rewards
- This information could also be stored as part of the blockchains ledger itself
- In order for this system wo work effectively the mining difficulty or the pool threshold will need to be adjusted based on the mining capability of lower powered device, thus allowing them to partake in the mining process.

Next Slide

- The proposed system has several key problems which must be overcome
- Botting or sybil attacks will be easier to commit due to the reduced cost of proof of work
  - There are several possible solutions to the problem, Requiring strict authentication of users when they sign up
  - Closely monitor user activity
  - Captcha/are you still watching mechanic
- Although ownership of content can be attributed to users (which is great for open source) there is nothing to control the theft/piracy of content
  - A problem currently plaguing NFT's

Next Slide

- Plan was to become a monero mining pool with the reward distribution set up
- Several hurdles got in the way
  - Becoming a full monero node. (SDD full / block corruption + the long sync time)
  - Deploying the first pool system failed (outdated interaction with the monero deamon)
  - Tried moving to an RPI but have had little success
- **Current Position**
  - I am currently a full monero mode (with the ability to mine as a user)
  - The pool software I have chosen is still having some issues connecting to the deamon
  - I know/have planned the changes to the pool reward function but have yet to implement it.

Theoretical Advancements A possible solution to the sybil attack is to have different pool with different potential rewards. Users are assigned to pools based on their account age. Therefore a rapid bot attack would have little profitability.

- Problem is that you still need to be able to detect bots.

Talking Points

[[Theoretical Advancements]]