Empera Blockchain (PoM). An ingenious blockchain that solves both PoS and PoW problems?

- https://empera.network/
  - Whitepaper: https://empera.network/files/EMPERA%20Whitepaper.pdf
  - Pitchdeck: https://empera.network/files/Empera_Presentation_Eng.pdf
  - Telegram channel: https://t.me/emperanetwork
- Proof of Stake (PoS) is positioned as our future, but it has some problems in it's design!
  - Proof of Stake overview
    - We are saving CPU/GPU and electricity
      - Producing new block is very cheap
        - In order to limit bad guys the miners should stack (reserve/freeze) their money
    - https://eth.wiki/en/concepts/proof-of-stake-faqs
  - Because mining is cheap there are two signigicant problems
    - Nothing at Stake
      - https://dlt-repo.net/nothing-at-stake-in-proof-of-stake-pos/
      - Bad guy can validate two blockchains (as it is cheap)
        - On one blockchain he will make a spending transaction
        - On another bockchain (a fake blockchain) he will not make such transaction
      - Later when the bad guy will become a miner he will change blockchains!
        - Other validators will validate it and continue to develop it
    - Centralization risk
      - Because of DeFi and derived financial instruments the issuers of such financial instruments have access to very big funds and they can use them to vote on blockchain
  - Ethereum PoS implementation offers solutions to these problems
    - fine when the miner was found validated two blockchains at the same time
    - fine when the miner was found validating wrong chain
    - fine is proportional to miner's stack size
    - HOWEVER
      - These solutions have not yet been tested in real life in the long term - they are just economic models
        - Some people believe that these solutions may cause huge problems in the future
        - Perhaps that is why the founders of Ethereum delayed the transition to PoS for so long.
- Instead of trying to solve PoS problems, can we just avoid the whole class of such problems?
  - Proof of Work (PoW) does not have such problems by it's nature!
    - Nothing at Stake
      - PoW does not have this problem, as it costs twice as much to mine two PoW blockchains.
    - Centralization risk
      - PoW does not have this problem as in order to increase voting power you should buy more hardware
  - But PoW has limitations in terms of scalability
- A better approach - Proof of Memory (PoM)
  - 1. We still need hardware like in PoW approach to AVOID PoS problems
    - We do need a hardware (RAM mostly in this case) and we do need to make math calculations on the hardware
      - So attacking the blockchain by changing it's past will still be very expensive
  - 2. In order to increase throughput we mine many different blockchains at the same time
    - There is a parameter L - number of blocks that are allowed to reuse the same generated Nonce (if it is good enough)
      - It allows to premine Nonces (for M blockchains for L blocks) in advance and store them in memory. And then quickly extract the best Nonce our of the memory
        - That's why this approach is called "Proof of Memory"
      - if L = 1 then POM is the same as POW. The higher L is the higher importance of memory size
        - ⚠️ Total hashrate = MIN((CPU/GPU hash rate * L), size of RAM)
        - ❓ The question is - how will the best value for L be defined?
    - Selecting next miner
      - 1. Miners only need LPowHash (hash of current block), and their PublicKey. They generate many Nonces and quickly calculate their NonceHashes
        - NonceHash = sha3(Nonce, PubKey, LPowHash)
      - 2. Miners store ALL generated Nonce-Hashes & Nonces IN MEMORY for next L blocks (and for all M blockchains it is mining for)
      - 3. When it's time to choose a miner for the next block on specific blockchain, all miners know the BlockNumber and PrevBlockHash and they quickly choose and share their best Nonces.
        - PowHash= XOR(sha3(BlockNum,PrevPowHash) , NonceHash)
          - The BEST Nonce is the one which NonceHash gives MORE leading 0s in PowHash
      - 4. So - miners submit their Nonces and together quickly determine the winner - who submitted Nonce that gives more leading 0s
        - To increase chances to win the miner should calculate and store in memory more NonceHashes and quickly chose the best one
    - Miners REUSE the same pre-generated NonceHashes & Nonces
      - They just select another Nonces to submit - the one that gives more leading 0s for the current block on specific blockchain
    - Miners CAN PARTICIPATE IN MINING multiple parallel blockchains!
      - This way we significantly increase performance (number of transac-tions per time)
        - Many blockchains run in paralel and have bridges to interoperate
      - Despite the fact that miner can mine many parallel blockchains he CANNOT CHANGE THE HISTORY - because changing the history is still very expensive as in PoW
        - The miner can try to create an alternate past, BUT there will be fewer 0s in the blocks of this past, so such a past will not be selected.
- Also
  - Transactions and calls to smart contracts are free!
    - BUT to fight spammers, the more money you hold, the more chance/ higher priority you have to process your transaction
    - Developers pay for smart contracts depending on the amount of data it need to store
  - JavaScript as a language for smart contracts
    - As it is much easier to find JS developers
    - Solidity will be or already is supported
  - Hosting of dApps including backend and frontend
    - 🔥WOW! That shoud increase trust in dApps!
    - ❓ Currently backend/frontend hosting it is centralized. Interesting how will be work in decentralized manner
  - Miners who are serving few blockchains can act is gates between those two blockchains
- My doubts
  - AFAIK, the founders of Ethereum have spent millions of US dollars on researches by top universities / experts to define and validate economic models as well as technical implementations.
    - It is quite unlikely that they didn't thought very well about their PoS implementation
    - And it is quite unlikely that few geniuses invented a better solution here
      - However after digging into details I now think that the core idea of PoM is ingenius 🔥
  - Personally, I believe in the future of PoS because the idea of not wasting CPU/RAM/hardware sounds more right.
    - ⚠️ Maybe there is a better way to protect the past while eliminate the need for hardware resources to become a miner?
  - if developers pay for smart contracts then it is not easy to organize stable coins
    - The more popular the stablecoin it, the more the developer has to pay
      - Because the developer does not collect any incentives (or he must explicitly program such a collection, which can be difficult)
        - ⚠️ I believe it would be better to built in ability to make both paid and unpaid transactions. Or to use SWIFT-like model with SHA/BEN/OUR instruc-tion