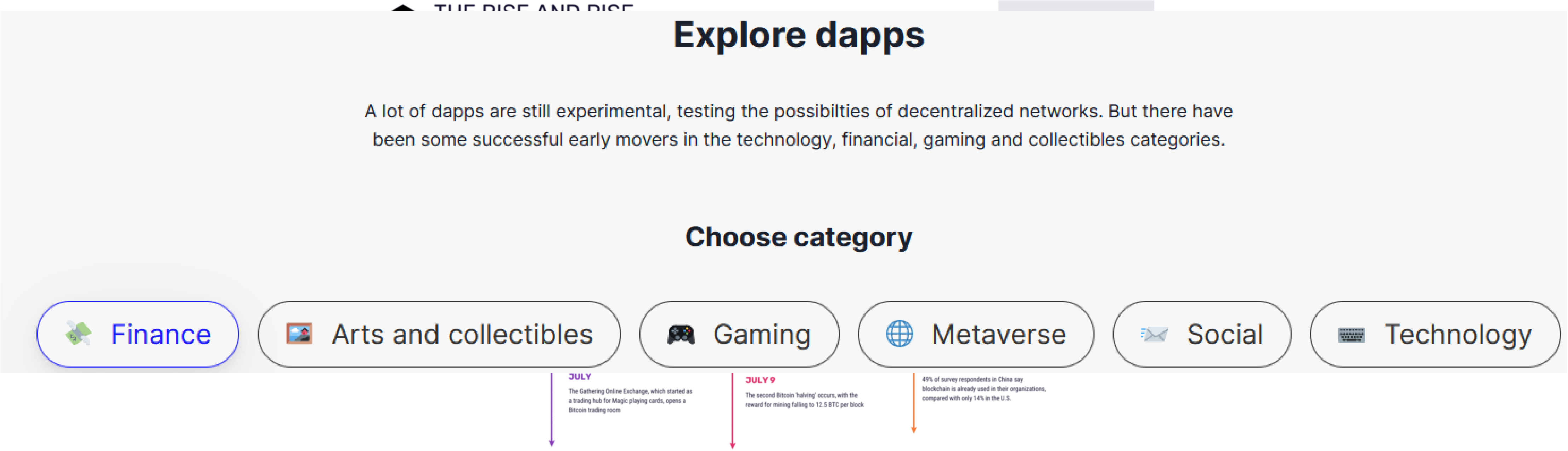
Ethereum Proof-of-Stake under Scrutiny

Ulysse Pavloff, **Yackolley Amoussou-Guenou**, Sara Tucci-Piergiovanni

Blockchain@X-OMI Workshop on Blockchain and Decentralized Finance
September 21-22, 2023 – France

Blockchains – Bitcoin to Ethereum

- Bitcoin appeared in 2008/9 as a distributed ledger for keeping balances and updating them to avoid double spending, etc.
- Ethereum came with the concept of smart contracts
  - Autonomous applications allowing many features and possibilities, such as DeFi



Explore dapps

A lot of dapps are still experimental, testing the possibilties of decentralized networks. But there have been some successful early movers in the technology, financial, gaming and collectibles categories.

Choose category

JULY

The Gathering Online Exchange, which started as a trading hub for Magic playing cards, opens a Bitcoin trading room

JULY 9

The second Bitcoin 'halving' occurs, with the reward for mining falling to 12.5 BTC per block

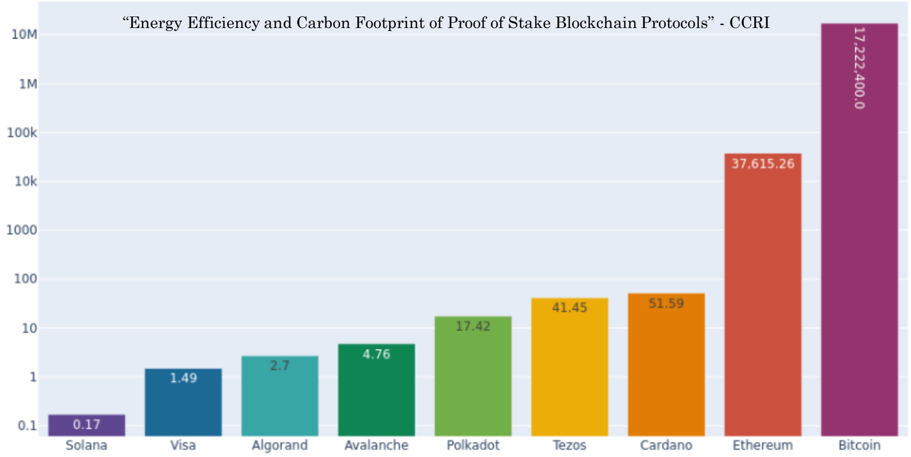
49% of survey respondents in China say blockchain is already used in their organizations, compared with only 14% in the U.S.

Consensus protocol

- Consensus protocol (especially in blockchains) are distributed algorithms used for the agents/nodes in a blockchain to agree on something, here, the next block to add to the chain

- As Bitcoin, Ethereum used the proof-of work – The more the agent/node has computing power, the more chances to be elected to add a new block

- However, PoW it too energy intensive



“Energy Efficiency and Carbon Footprint of Proof of Stake Blockchain Protocols” - CCRI

Figure 5: Electricity consumption [Wh] per transaction for Bitcoin, Ethereum, Visa, and all PoS systems. Logarithmic scale.

Transition to PoS

- It was a long process that took many years

- The beacon chain (for staking) started in 2020
  - But ideas of Ethereum being a PoS blockchain started the latest in **2016**

- Finally, the transition took place in September 2022 after many years of tests and patches

- This presentation will detail a bit the Ethereum’s Proof-of-Stake consensus protocol as launched in 2022

The Ethereum's PoS protocol (since 2022-09-15)

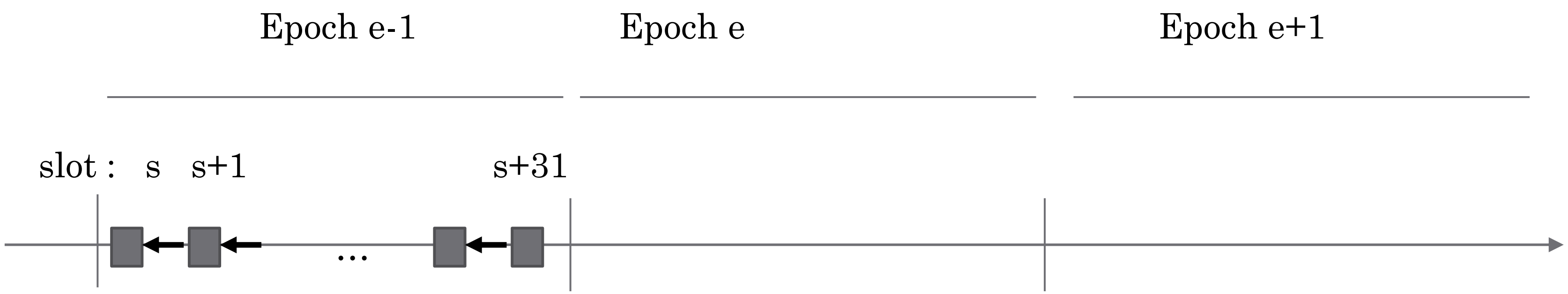
- The blockchain is maintained by *validators* (808 594 as of Sep, 20 2023)
  - One must **stake** 32 ethers to become a validator

- Validators, as miners, have the task to add blocks (1 each 12 seconds)
  - Newly minted Eth are given to validators as reward, according to their work

- Misbehaving validators caught in the act are slashed – reduction the stakes

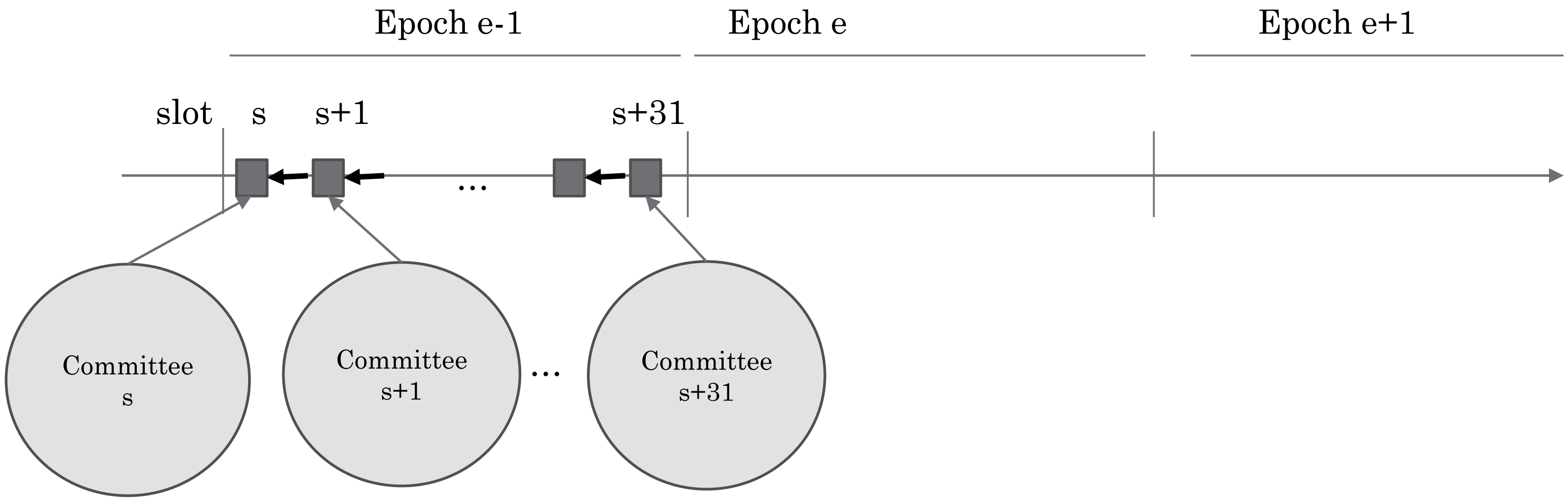
Slots and epochs

- 1 slot lasts 12 secondes
  - Ideally, there should be 1 block per slot
- 1 epoch = 32 slots = 6 minutes 24 seconds



- Rewards are given at the end of each epoch

A committee-based protocol

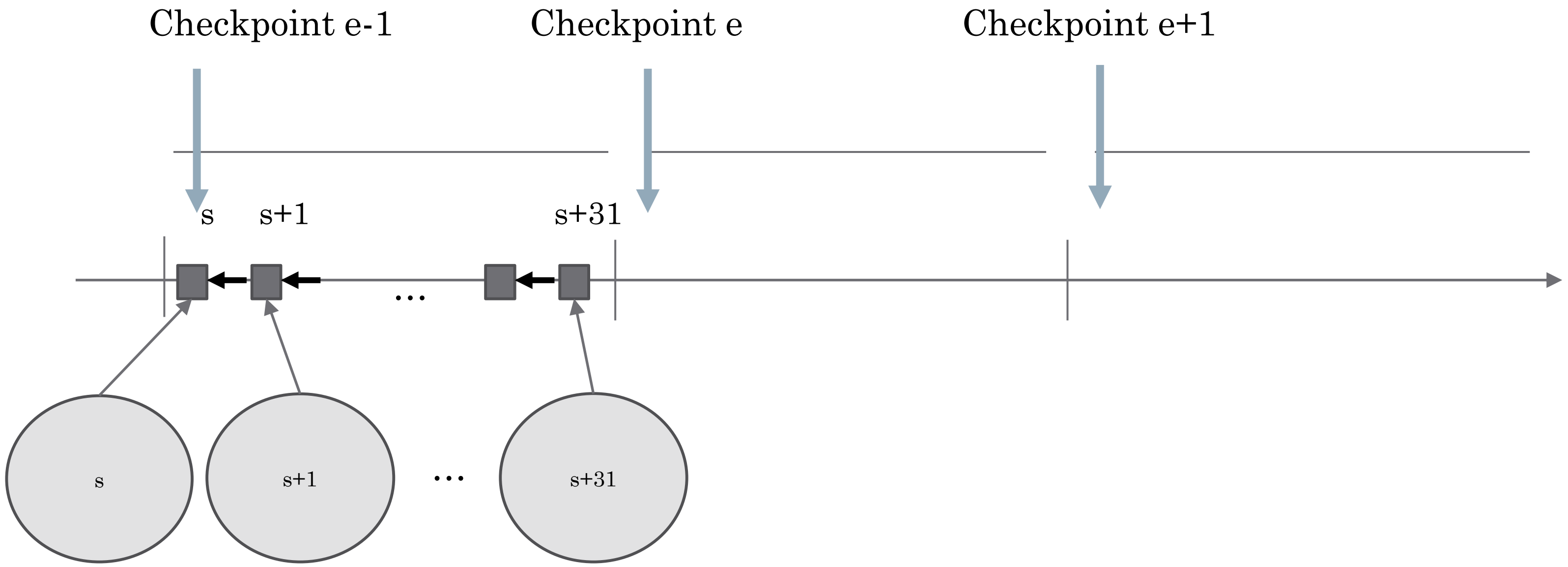


- Each committee is a set of validators. Committees form a partition of validators per epoch

- For each committee/slot, 1 validator is selected proposer (at random) and must propose a block within the slot time

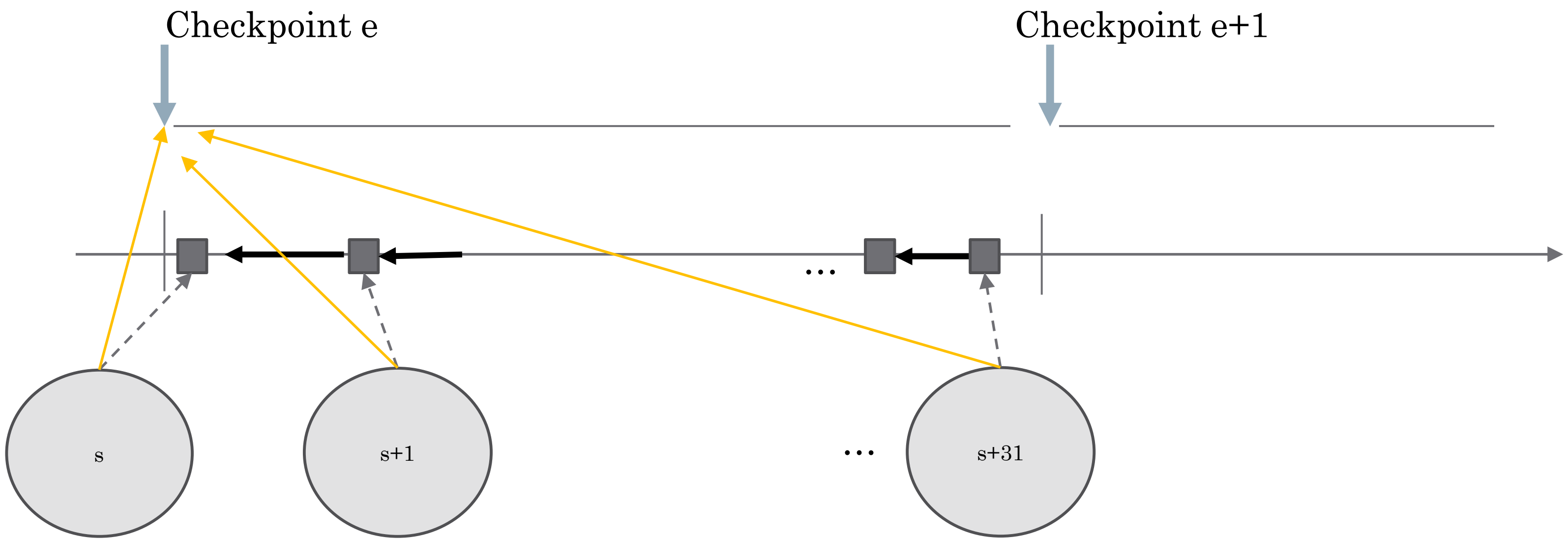
- Committee members "attest" the proposed block by a vote. They follow a fork choice rule

Checkpoints



- Ideally, the first block of an epoch is called **checkpoint**
- Checkpoints are what validators aim to “finalise”
  - By using attestations

Attestations



- When their turn, attesters of a slot cast 2 different votes
- One for the checkpoint of the current epoch. Here in orange
- One for the best block seen, ideally their slot's. Here dashed
- Rewards are given based on attestations stored on chain

Justification: a step toward finalisation

- If a checkpoint received a fraction of 2/3 of attestations among all validators of an epoch, such checkpoint is considered *justified*

- A checkpoint being justified can be seen as a candidate block for finalisation

- When a checkpoint is justified, validators will have a preference building on top of it

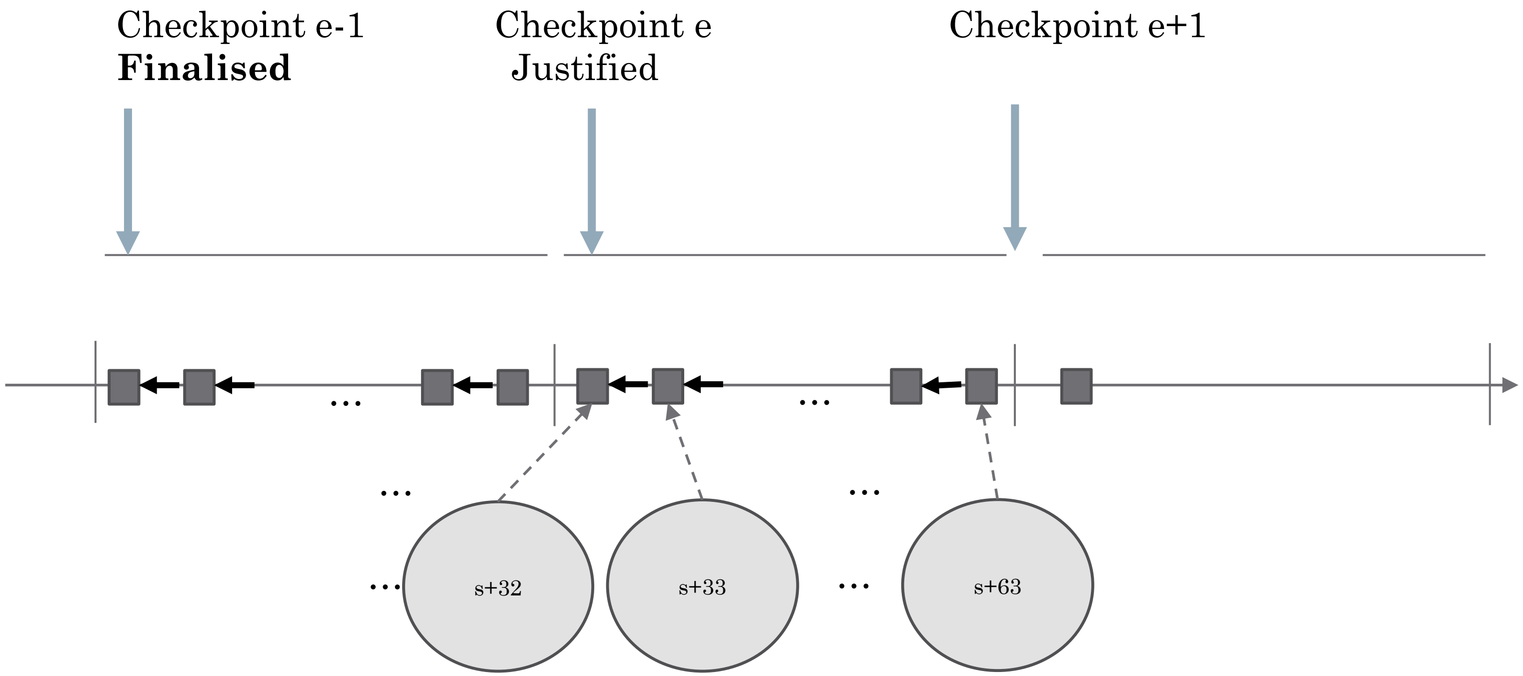
Finalisation

- A checkpoint being finalised is done in two successive epochs. The general case is the following:
  - If the checkpoints of two epochs e and e+1 are justified, then the checkpoint of epoch e is said to be *finalised*

- Intuitively, the idea is that in such a situation, everybody saw the first checkpoint and is considering it in the local chain

- That checkpoint will forever be in the blockchain

Finalisation



Selection of validators

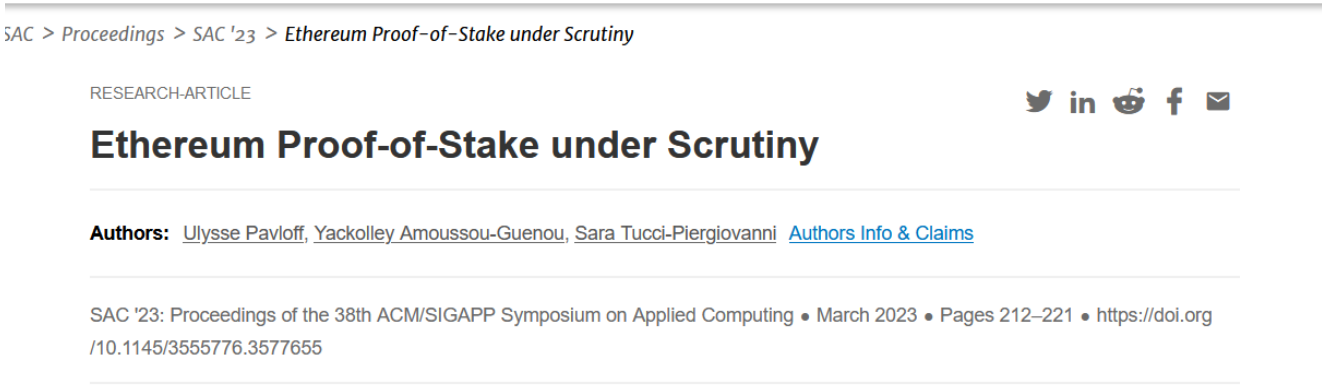
- Being a validator is “simple” it suffices to stake 32 Eth
  - Being a committee-member is the exact same thing

- However, being proposer is more random. That election is based on the amount of stake of the agents/nodes. The more an agent has staked (capped at 32), the higher the chance to be proposer at a slot

- Some pseudo random values are inserted in each block. Those value for an entire epoch forms a seed. That seed is what is used for the pseudo random selection of proposers, and even the repartition of agents in committees

The protocol has some vulnerabilities

- “When a checkpoint is justified, validators will have a preference building on top of it”



SAC > *Proceedings* > *SAC '23* > *Ethereum Proof-of-Stake under Scrutiny*

RESEARCH-ARTICLE

Ethereum Proof-of-Stake under Scrutiny

Authors: Ulysse Pavloff, Yackolley Amoussou-Guenou, Sara Tucci-Piergiovanni Authors Info & Claims

SAC '23: Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing • March 2023 • Pages 212–221 • https://doi.org/10.1145/3555776.3577655

- This preference can be manipulated, by malicious agents, to cause delays in checkpoints finalisation

https://hal.science/hal-03821290v2

Ethereum’s Proof-of-Stake

- A BFT-consensus blockchain which is some situation may be considered a particular mix between Nakamoto-style consensus and BFT consensus

- There are some issues regarding the liveness of the finalisation, but most importantly, there is no study yet understanding the impact of the “incentive mechanisms” implemented

- The protocol is still analysed a lot, both by researchers and developpers from the Ethereum’s Fundation. Moreover, the protocol may evolve in the future

- “… the Merge reduces the electricity consumption and carbon emissions of the Ethereum network by 99.988 % and 99.992 %, respectively.” in *Implications on the Electricity Consumption and Carbon Footprint of the Ethereum Network* by the Crypto Carbon Ratings Institute (CCRI)

Futures directions on Ethereum PoS

- (Incentive) analysis of the protocol, considering rewards, penalties, slashing…

- Is Ethereum proof-of-stake more or less decentralized than the PoW version?

- …

Merci | Thank you