MONASH University

FIT5214: Blockchain

Assignment Project Exam Help

Lecture 6: Alternatives to PoW

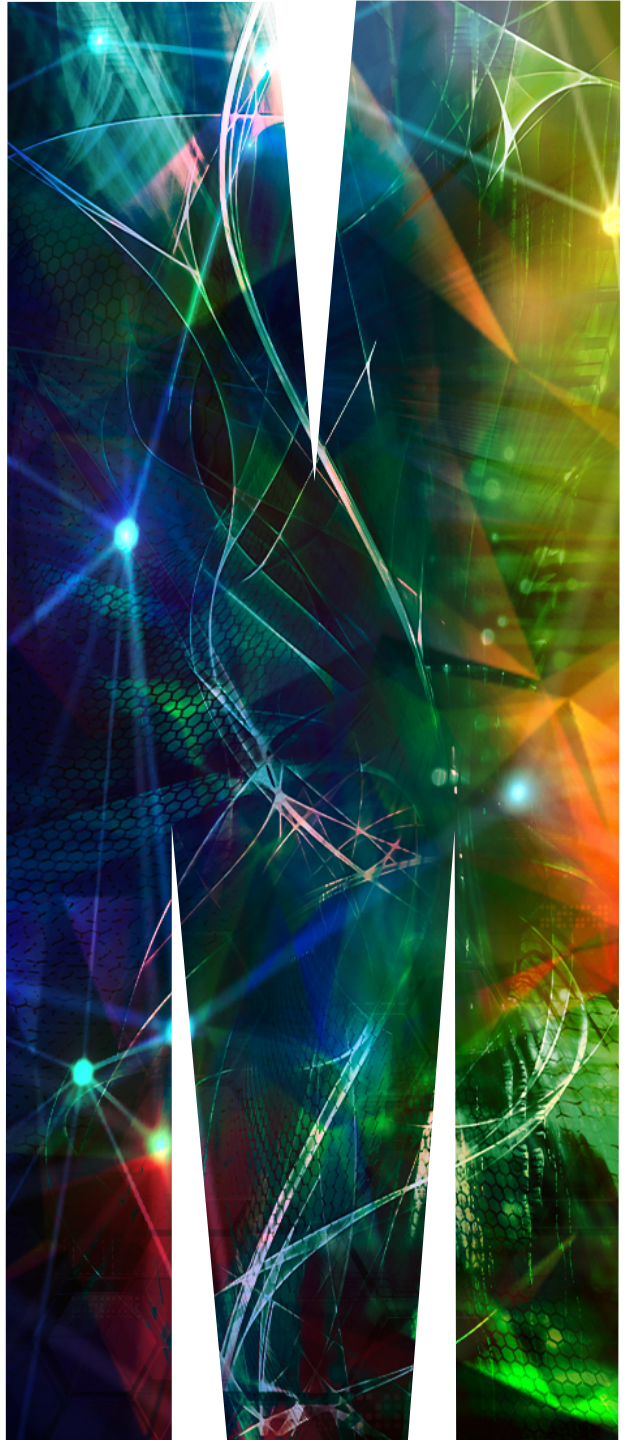
https://powcoder.com

Add WeChat powcoder

Lecturer: Rafael Dowsley

rafael.dowsley@monash.edu

https://dowsley.net



Unit Structure

- **Lecture 1: Introduction to Blockchain**
- **Lecture 2: Bitcoin**
- **Lecture 3: Ethereum and Smart Contracts**
- **Lecture 4: Proof-of-Work (PoW)**
- **Lecture 5: Attacks on Blockchains**
- **Lecture 6: Class Test/Alternatives to PoW**
- **Lecture 7: Proof-of-Stake (PoS)**
- **Lecture 8: Privacy**
- **Lecture 9: Byzantine Agreement**
- **Lecture 10: Blockchain Network**
- **Lecture 11: Payment Channels**
- **Lecture 12: Guest Lecture**

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

Unit Structure

- Lecture 1: Introduction to Blockchain
- Lecture 2: Bitcoin
- Lecture 3: Ethereum and Smart Contracts
- Lecture 4: Proof-of-Work (PoW)
- Lecture 5: Attacks on Blockchains
- Lecture 6: Class Test/Alternatives to PoW
- Lecture 7: Proof-of-Stake (PoS)
- Lecture 8: Privacy
- Lecture 9: Byzantine Agreement
- Lecture 10: Blockchain Network
- Lecture 11: Payment Channels
- Lecture 12: Guest Lecture

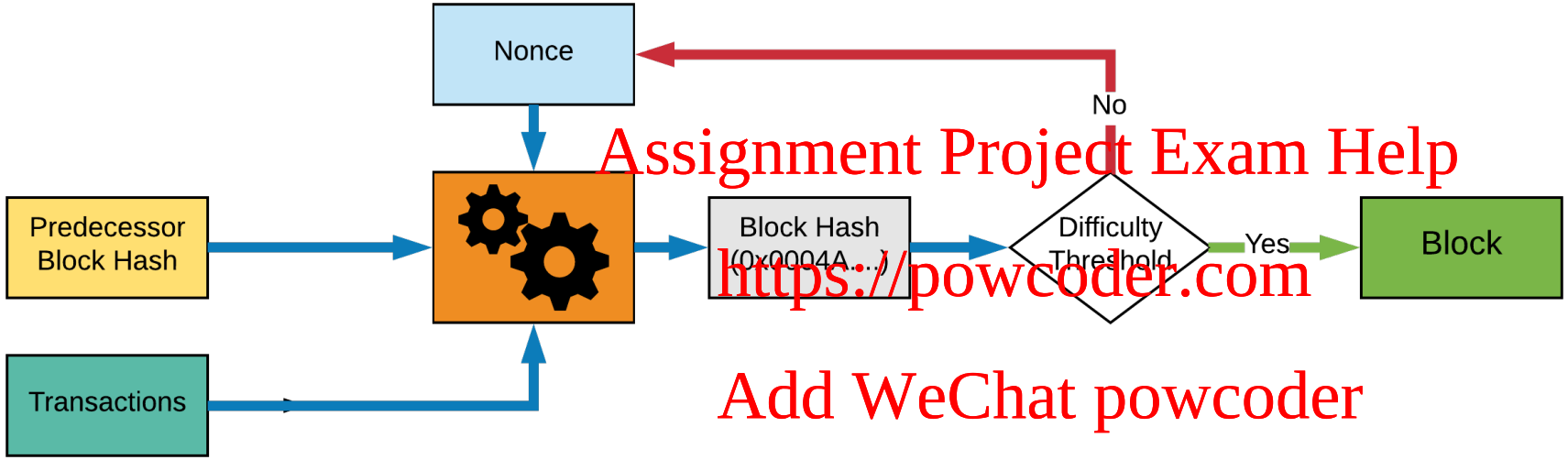
Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

Mini Research Project

- Groups of 3 persons officially from the same lab
- Each paper can only be selected by one group regardless of labs sessions. This is a first-come-first-serve model.
- Worth 30% of the unit marks
- Submission deadline: Tuesday, 18th of October, 16:30
- Presentations on the labs of Week 12
- Detailed instructions will be sent later today/further details also in the labs this week

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

Recap: PoW

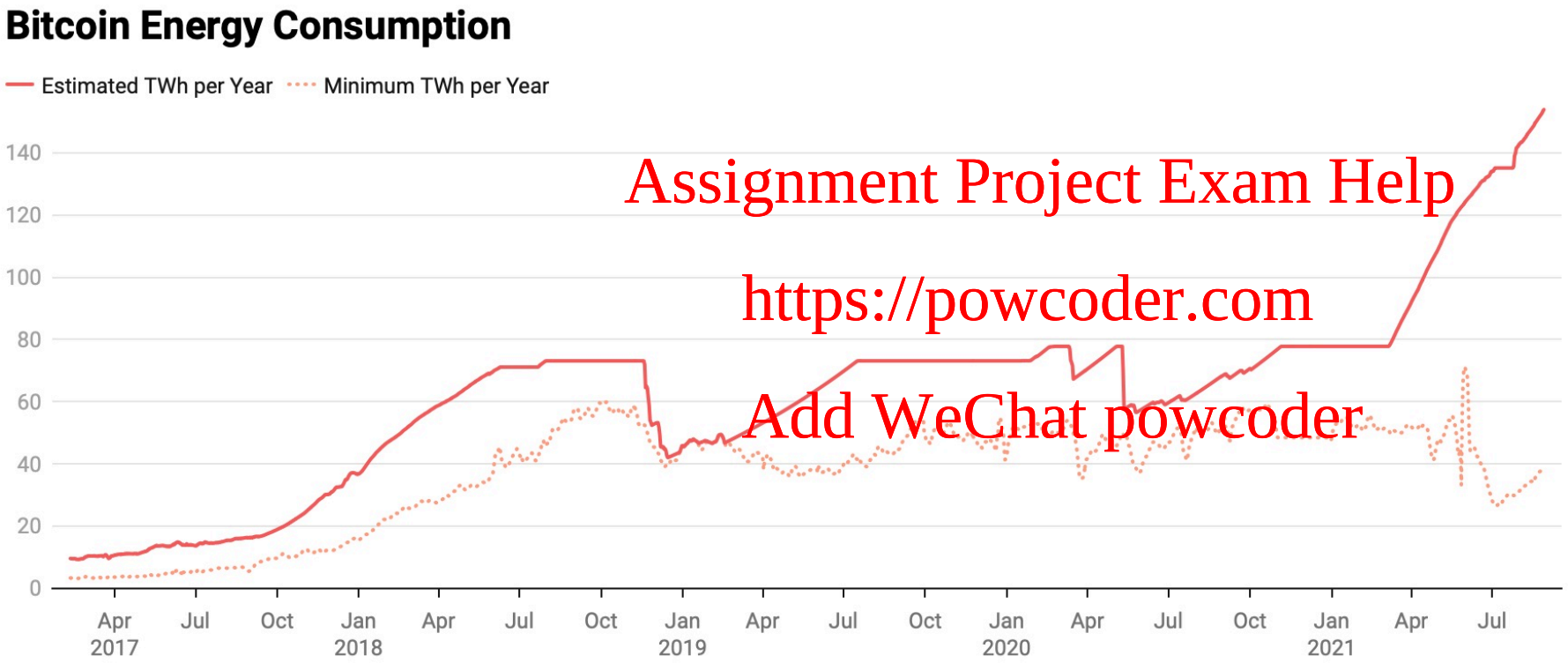


Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

Weakness:

1. solving puzzles requires *A LOT* of computing power, and electricity;
2. the throughput is limited

Bitcoin Energy Consumption



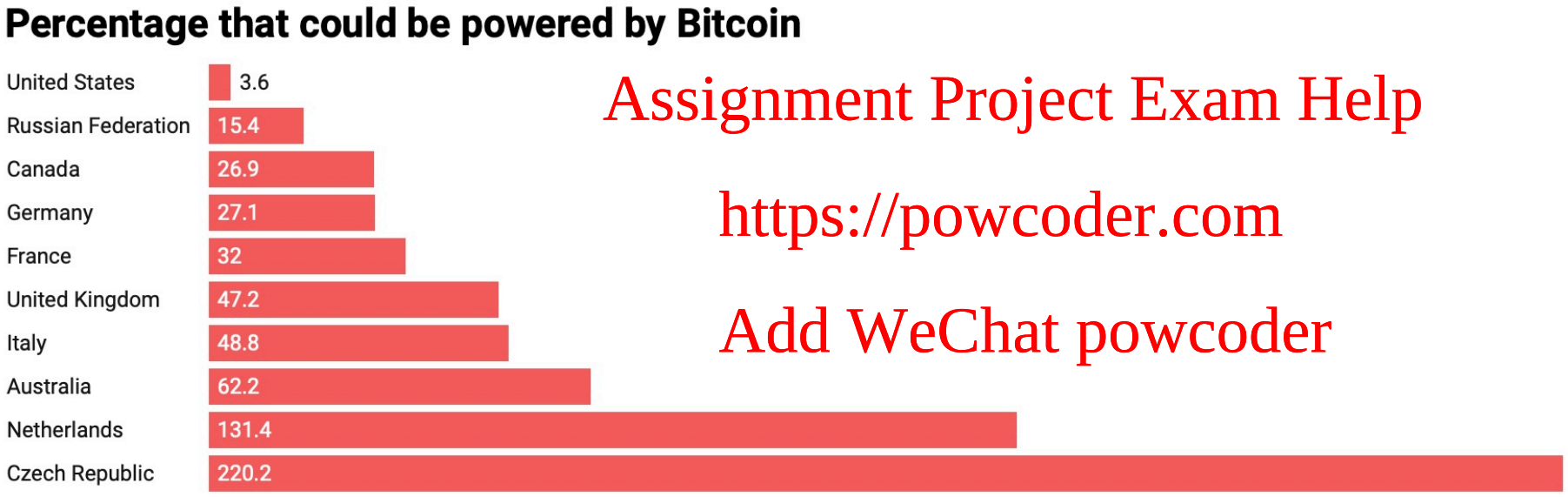
Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

https://digiconomist.net/bitcoin-energy-consumption

Bitcoin Energy Consumption



Assignment Project Exam Help

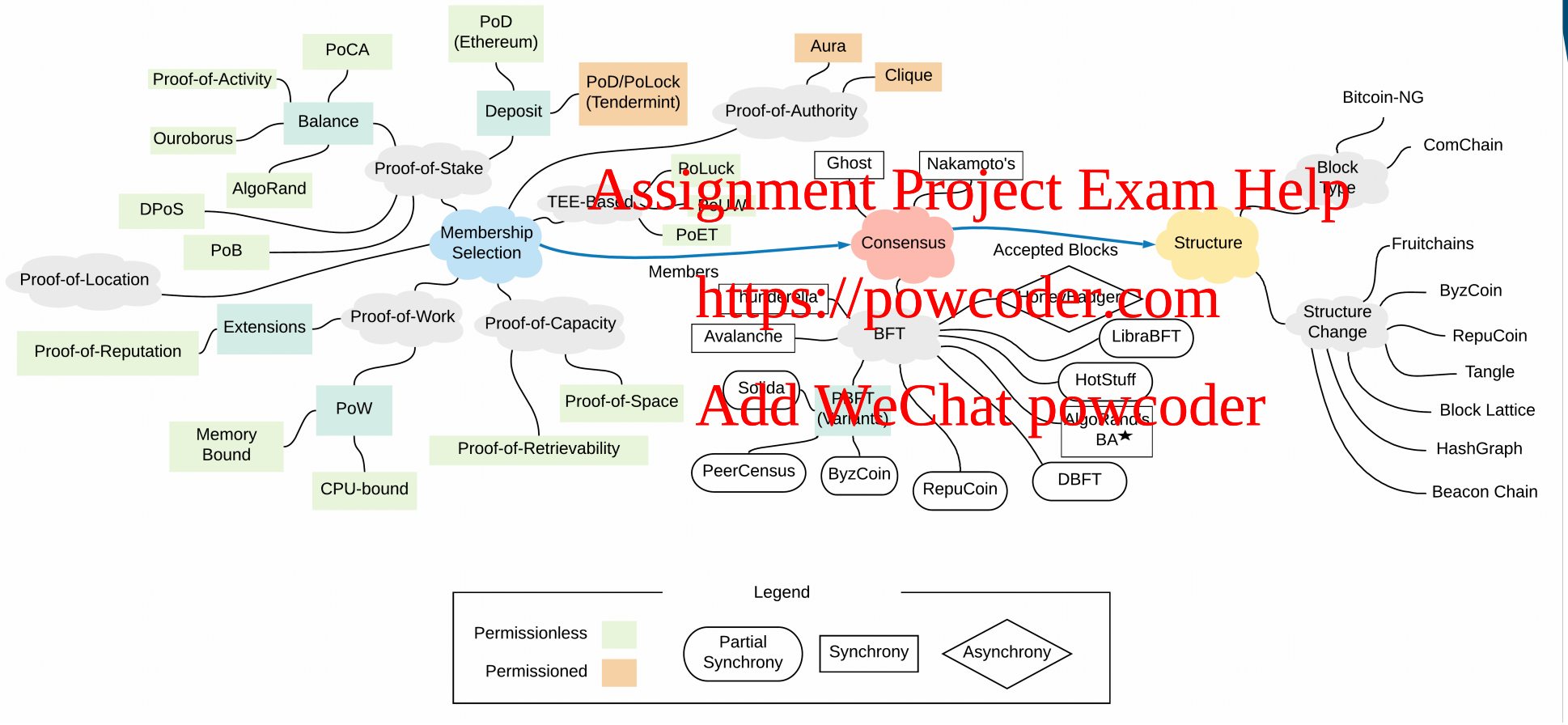
https://powcoder.com

Add WeChat powcoder

https://digiconomist.net/bitcoin-energy-consumption

MONASH University

Landscape



Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

https://arxiv.org/pdf/1908.08316.pdf

MONASH University

Membership selection and consensus

Most proof-of-* are ways to choose members to run consensus algorithms, such as

- Nakamoto consensus: the longest chain wins
- GHOST consensus: the heaviest subtree wins
- BFT protocols (week 9)
  - A (small) group of nodes run a consensus algorithm to agree on a proposal

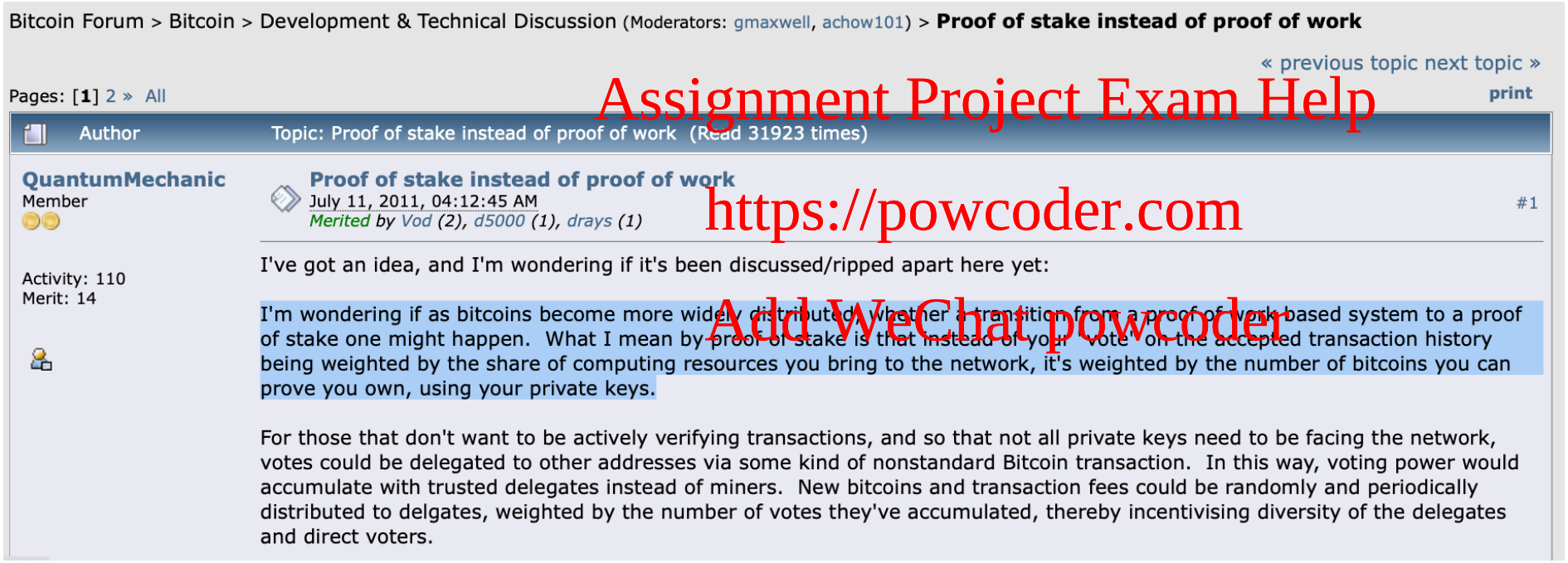
Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

Proof-of-Stake (PoS)

The concept was first proposed in a Bitcoin community forum on 11 July 2011.



Bitcoin Forum > Bitcoin > Development & Technical Discussion (Moderators: gmaxwell, achow101) > **Proof of stake instead of proof of work**

« previous topic next topic »

Pages: [**1**] 2 » All

print

Assignment Project Exam Help

Author	Topic: Proof of stake instead of proof of work (Read 31923 times)

https://powcoder.com

QuantumMechanic
Member

Activity: 110
Merit: 14

Proof of stake instead of proof of work
July 11, 2011, 04:12:45 AM
Merited by Vod (2), d5000 (1), drays (1)

#1

Add WeChat powcoder

I've got an idea, and I'm wondering if it's been discussed/ripped apart here yet:

I'm wondering if as bitcoins become more widely distributed whether a transition from a proof of work based system to a proof of stake one might happen. What I mean by proof of stake is that instead of your "vote" on the accepted transaction history being weighted by the share of computing resources you bring to the network, it's weighted by the number of bitcoins you can prove you own, using your private keys.

For those that don't want to be actively verifying transactions, and so that not all private keys need to be facing the network, votes could be delegated to other addresses via some kind of nonstandard Bitcoin transaction. In this way, voting power would accumulate with trusted delegates instead of miners. New bitcoins and transaction fees could be randomly and periodically distributed to delgates, weighted by the number of votes they've accumulated, thereby incentivising diversity of the delegates and direct voters.

https://bitcointalk.org/index.php?topic=27787.0

MONASH University

Proof-of-Stake (PoS)

PoW: vote by comparing power — more computing power, more votes
PoS: vote by number of coins — more coins, more votes

Assignment Project Exam Help

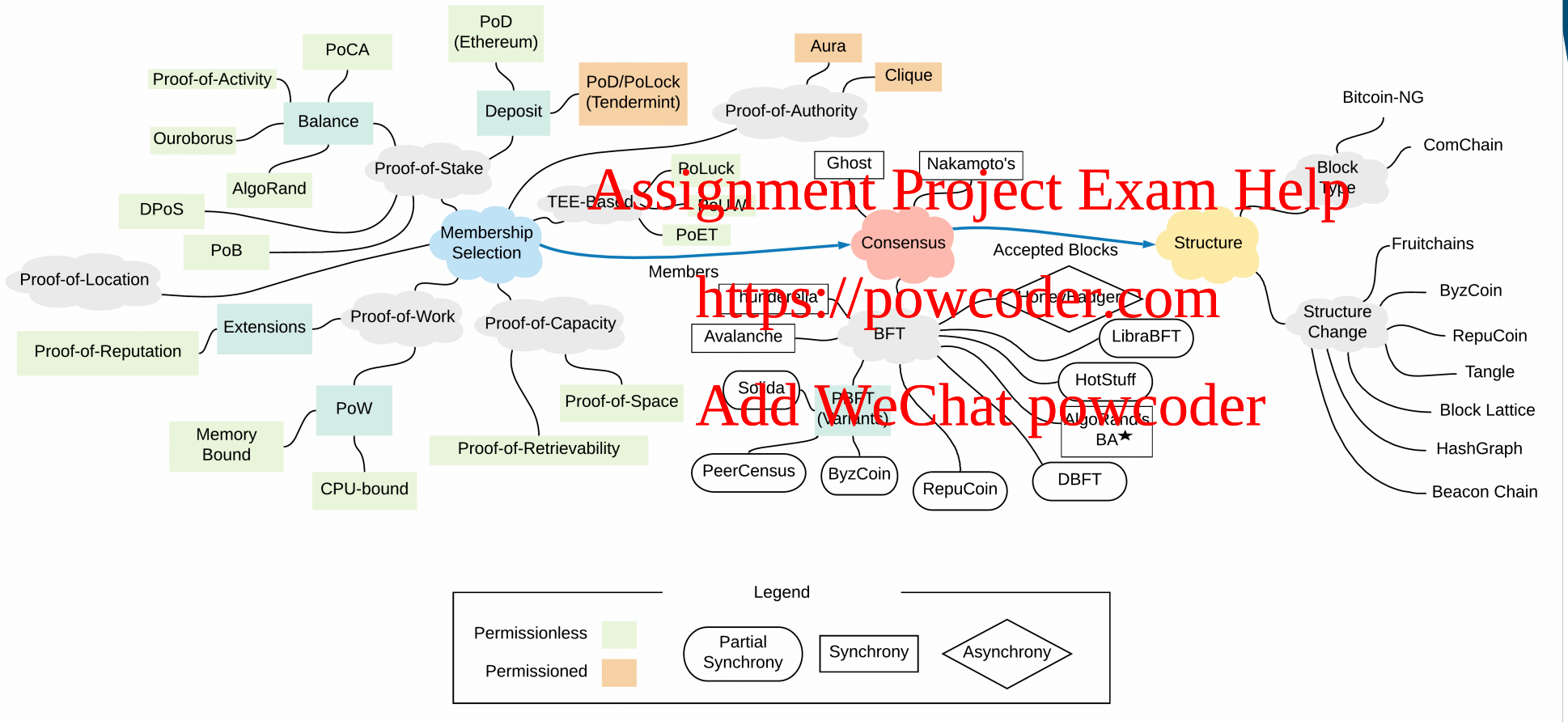
https://powcoder.com

With **PoW**, the one with **51% computing power** controls the system
With **PoS**, the one with **51% coins** controls the system

Add WeChat powcoder

Next Week

Landscape



Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

https://arxiv.org/pdf/1908.08316.pdf

MONASH University

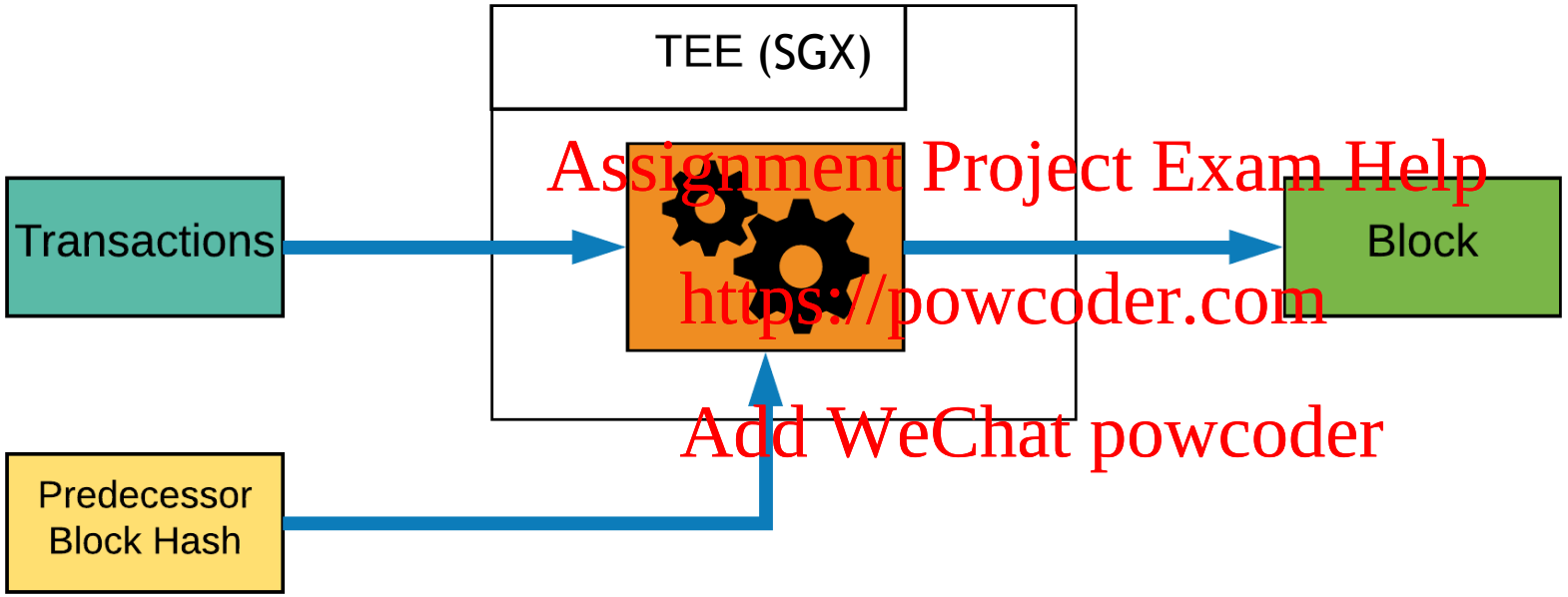
Proof-of-Elapsed-Time (PoET)

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

https://sawtooth.hyperledger.org/examples/

MONASH University

Proof-of-Elapsed-Time (PoET)



Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

MONASH
University

Intel Software Guard Extensions (SGX)

It is an extension to Intel processors allowing:

- **Enclaves (an isolated environment):**
  Running code securely on an untrusted environment
  (e.g. running code on Windows)

  So you can protect your secret in the presence of malware on your machine.

- **Attestation:**
  Provide verifiable proofs to local/external systems that the code was running in the enclave

  So code can be run securely on a remote machine.

- **Minimum Trusted Computing Base:**
  Only need to trust the hardware processor. No need to trust DRAM, OS, etc.

  So the attack surface is very small, but you need to trust the hardware, so the manufacturer, i.e., Intel

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

How PoET works?

New participants joining the network

1. Each participant needs to have at least one SGX-enabled machine
2. A new participant downloads the PoET trusted code and run it in an enclave
3. The trusted code creates a new key pair
4. The participant sends a SGX attestation proof to the blockchain network as a join request

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

How PoET works?

Generating blocks

1. The trusted code randomly creates a timer in the SGX
2. Participants Wait for a period of time as specified by the timer
3. The trusted code generates a signed statement on the completion of the timer
4. Participants send their signed statement to the network with a new block.
5. The selection of the block is application specific
   e.g. it can be choosing the longest chain, or run BFT protocols.

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

How PoET works?

Summary

1. SGX randomly generates a timer
2. The lucky one with smallest timer generates a block
3. Since SGX is a trusted execution environment, the code cannot be altered to always generate a small time

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

MONASH University

Quiz (multiple choice):

Assuming the crypto algorithms and SGX are secure, which of the following properties statement is true:

Assignment Project Exam Help

A. Users controlling more SGX-enable machines will have a better chance to generate a block

https://powcoder.com

B. Users can fake a signed certificate on the completion of timer to propose a block

Add WeChat powcoder

C. It is possible for Intel to control the blockchain

D. No fork would occur

Answer:

Assuming the crypto algorithms and SGX are secure, which of the following properties statement is true:

Assignment Project Exam Help

A. Users controlling more SGX-enable machines will have a better chance to generate a block

https://powcoder.com

B. Users can fake a signed certificate on the completion of timer to propose a block

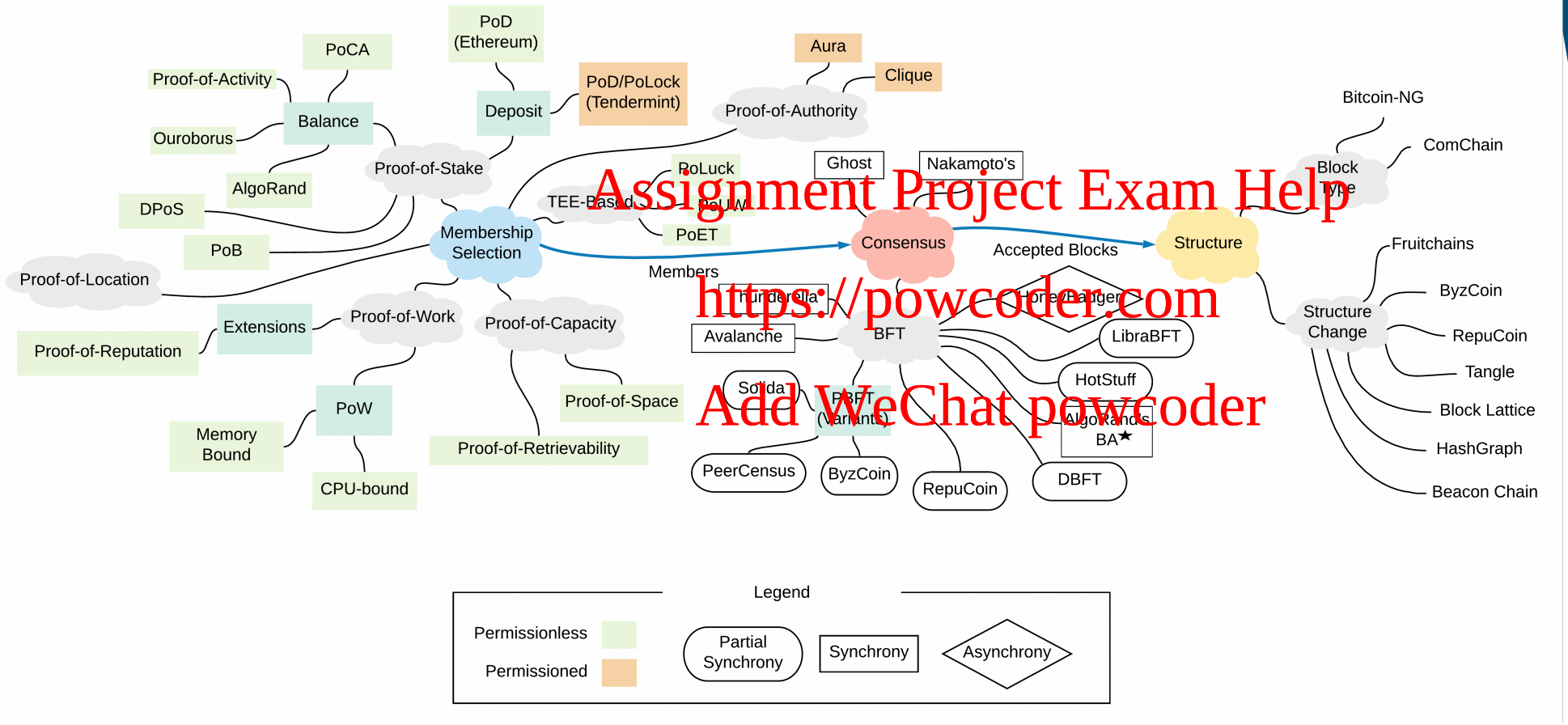
Add WeChat powcoder

C. It is possible for Intel to control the blockchain

D. No fork would occur

MONASH University

Landscape



Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

https://arxiv.org/pdf/1908.08316.pdf

MONASH University

Proof-of-Capacity

Proof-of-Space is a type of consensus algorithm achieved by demonstrating one's legitimate interest by allocating a non-trivial amount of memory or disk space to solve a challenge.

Assignment Project Exam Help

Similar to PoW, but instead of computation, storage is used to earn cryptocurrency by solving a puzzle.

https://powcoder.com

Seen as a fairer and greener alternative by its enthusiasts.

Add WeChat powcoder

For further information on how such solutions can work, see for instance, “SpaceMint: A Cryptocurrency Based on Proofs of Space”.

Proof-of-Capacity

Proof-of-Storage, Proof-of-Retrievability: related to Proof-of-Space, but instead of showing that space is available for solving a puzzle, the prover shows that space is actually used to store a piece of data correctly at the time of proof.

Assignment Project Exam Help

Proof-of-Space-Time: shows the prover has spent an amount of time keeping the reserved space unchanged.

https://powcoder.com

Add WeChat powcoder

Proof-of-Personhood

"Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies"

Core idea: verify *real people*, thereby linking physical and virtual identities and providing a basis to prevent adversaries from mounting Sybil attacks.

Example: each attendee of an event get a cryptographic identity token. Attendees can be disguised to hide their real identity.

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

Next Week

Proof-of-Stake (PoS)

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder