
NPTEL ONLINE CERTIFICATION COURSES

# Blockchain and its applications

Prof. Sandip Chakraborty

Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

## Lecture 21: Beyond PoW

# CONCEPTS COVERED

- **Open Consensus beyond PoW**

# KEYWORDS

- Proof of Stake (PoS)
- Proof of Burn (PoB)
- Proof of Elapsed Time (PoET)

# The Limit of PoW

- **The Good**: A fully decentralized consensus for permissionless models
  - works good for cryptocurrencies – serves its purposes

# The Limit of PoW

- **The Bad:** Do not trust the individuals, but trust the society as a whole
  - You need a real large network to prevent the 51% attack – **not at all suitable for enterprise applications**

# The Limit of PoW

- **The Ugly**: Low transaction throughput, Overuse of computing power !!
  - (Bitcoin) 3.3 to 7 transactions per second, (Ethereum) ~15 transactions per second
  - Millions of miners – thousands tries, but only one gets the success

# Bitcoin Energy Consumption

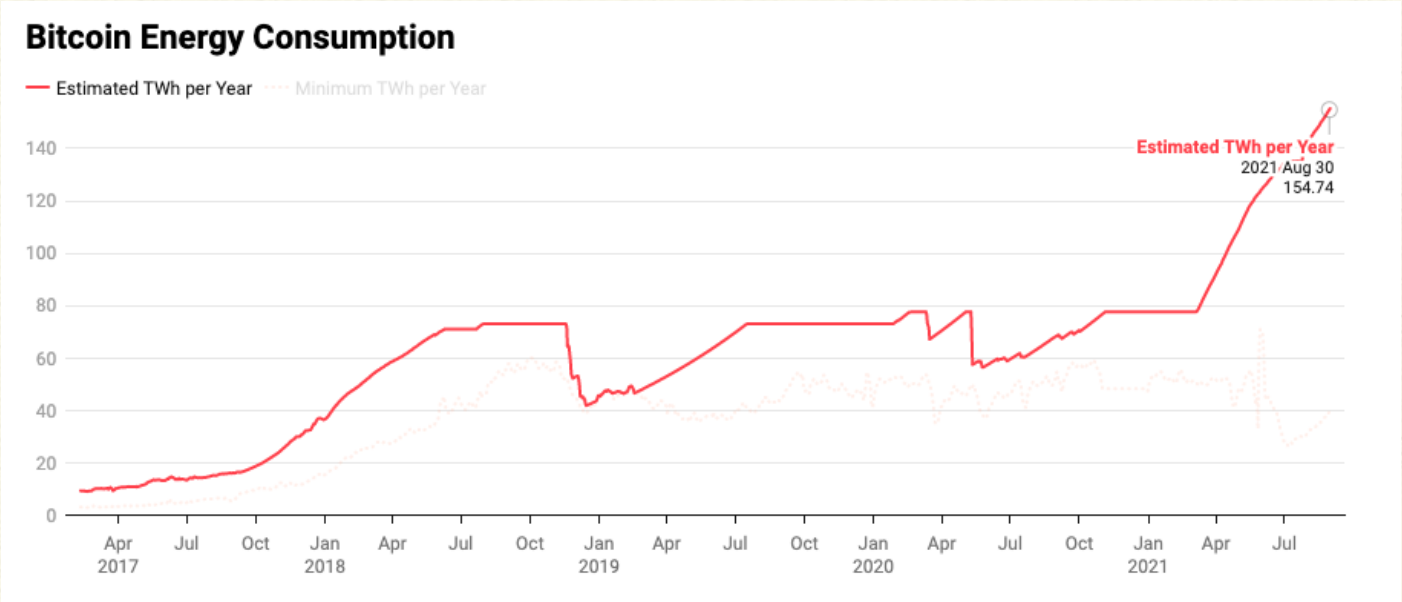
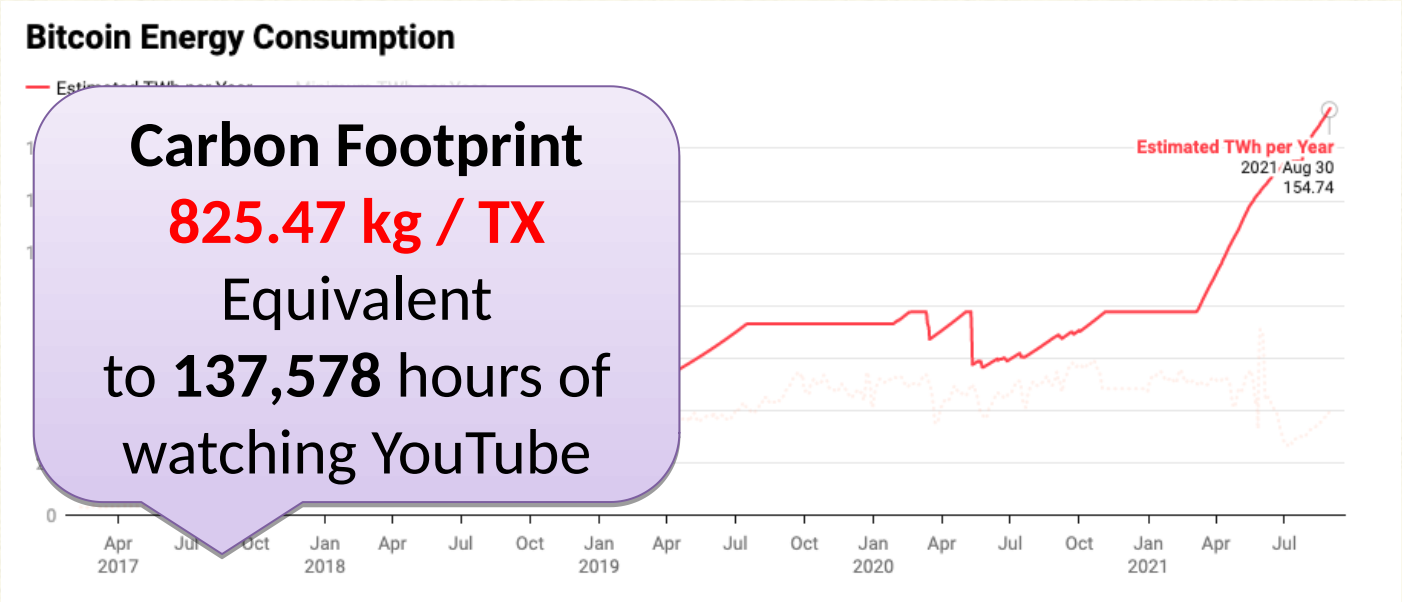



**Image Source: Digiconomist Bitcoin Energy Consumption Index**

# Bitcoin Energy Consumption



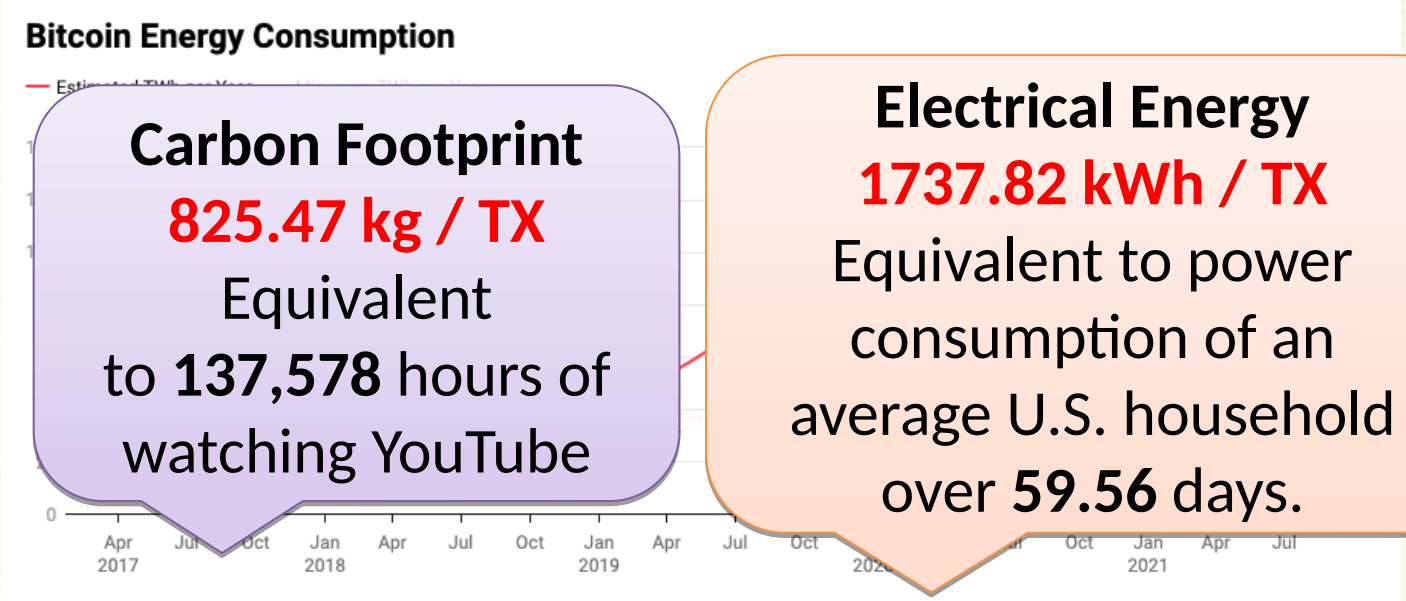

**Carbon Footprint**

**825.47 kg / TX**

Equivalent to **137,578** hours of watching YouTube

**Image Source: Digiconomist Bitcoin Energy Consumption Index**

# Bitcoin Energy Consumption




**Carbon Footprint**
**825.47 kg / TX**
Equivalent to **137,578** hours of watching YouTube

**Electrical Energy**
**1737.82 kWh / TX**
Equivalent to power consumption of an average U.S. household over **59.56** days.

**Image Source: Digiconomist Bitcoin Energy Consumption Index**

# Proof of Stake (PoS)

- Possibly proposed in 2011 by a Member in Bitcoin Forum - https://bitcointalk.org/index.php?topic=27787.0
  - Make a transition from PoW to PoS when bitcoins are widely distributed

# Proof of Stake (PoS)

- PoW vs PoS
  - **PoW**: Probability of mining a block depends on the work done by the miner
  - **PoS**: Amount of bitcoin that the miner holds – Miner holding 1% of the Bitcoin can mine 1% of the PoS blocks.

# Proof of Stake (PoS)

- Provides increased protection
  - Executing an attack is expensive, you need more Bitcoins
  - **Reduced incentive for attack** – the attacker needs to own a majority of bitcoins – an attack will have more affect on the attacker

# Proof of Stake (PoS)

- Variants of “stake”
  - Randomization in combination of the stake (*used in Nxt and BlackCoin*)
  - **Coin-age**: Number of coins multiplied by the number of days the coins have been held (*used in Peercoin*)

# Proof of Burn (PoB)

- Miners should show proof that they have *burned* some coins
  - Sent them to a verifiably un-spendable address
  - Expensive just like PoW, but no external resources are used other than the burned coins
- PoW vs PoB
  - Real resource vs virtual/digital resource
- PoB works by burning PoW mined cryptocurrencies

# Proof of Burn (PoB)

- Mine … some coin
  - S…
  - B… used c…
- PoW…
  - P…
- PoB w… …cies

## PoS and PoB

**Ultimately depends on PoW mined cryptocurrencies**

**You cannot use them to bootstrap a new blockchain**

# Proof of Elapsed Time (PoET)

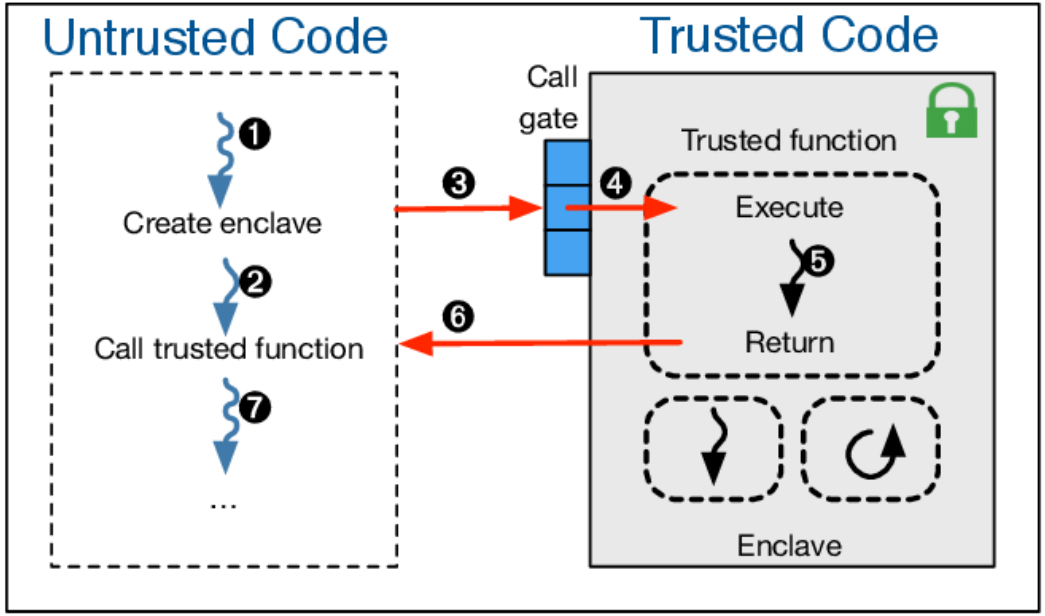
- Proposed by Intel, as a part of **Hyperledger Sawtooth** – a blockchain platform for building distributed ledger applications

- **Basic idea:**
  - Each participant in the blockchain network waits a random amount of time
  - The first participant to finish becomes the leader for the new block

# Proof of Elapsed Time (PoET)

- How will one verify that the proposer has **really waited** ?
  - Utilize special CPU instruction set – *Intel Software Guard Extension* (SGX) – a trusted execution platform
  - The trusted code is private to the rest of the application
  - The specialized hardware provides an attestation that the trusted code has been set up correctly

# Intel SGX


Untrusted Code
Trusted Code
Call gate
Trusted function
Create enclave
Call trusted function
...
Execute
Return
Enclave
1
2
3
4
5
6
7

# Conclusion

- PoW is significantly costly
  - Reduce the cost by moving towards PoS/PoB
- Los-cost consensus from the bootstrap: PoET
  - Needs specialized hardware
- What about enterprise application?


Thank
you