FINE 434: FinTech

Lecture 18

Professor Fahad Saleh

McGill University - Desautels

Speeding up the Blockchain

Bitcoin has $\sim$ 9.5 minute block times and a block size limit

Ethereum has 10 - 20 second block times and a block gas limit

Why not have higher throughput?

Speeding up the Blockchain

Bitcoin has $\sim$ 9.5 minute block times and a block size limit

Ethereum has 10 - 20 second block times and a block gas limit

Why not have higher throughput?

Learning by doing...

Implementation

Within a Proof-of-Work (PoW) system, how would we achieve higher throughput?

Implementation

Within a Proof-of-Work (PoW) system, how would we achieve higher throughput?

Adjust the Difficulty!

An easier puzzle takes less trials to solve and therefore generates a valid block sooner

More valid blocks per unit time means higher throughput

Approximately, the PoW puzzle asks that we find s such that:

$Int(Hex(Hash(Encode(x))))$ falls within $S \subseteq \{0, ..., 2^{256} - 1\}$

How likely is it that a single value of x solves the PoW puzzle?

SHA 256 outputs are supposed be uniformly distributed.

Loosely, for any str x and any v between 0 and $2^{256} - 1$,

$$\mathbb{P}(Int(Hex(Hash(Encode(x)))) = v) = \frac{1}{2^{256}}$$

Question: $\mathbb{P}(Int(Hex(Hash(Encode(x)))) \in S) =$??

$$\begin{aligned}
&\mathbb{P}(Int(Hex(Hash(Encode(x)))) \in S) \\
&= \sum_{s \in S} \mathbb{P}(Int(Hex(Hash(Encode(x)))) = s) \\
&= \sum_{s \in S} \frac{1}{2^{256}} \\
&= \frac{|S|}{2^{256}}
\end{aligned}$$

You don't need to understand the formalism above, but you do need to internalize the result!

If you must, take the following as a fact:

For any x : $\mathbb{P}(Int(Hex(Hash(Encode(x)))) \in S) = \frac{|S|}{2^{256}}$

Examples

Let $S := \{n \in \{0, ...2^{256} - 1\} : n \leqslant 2^{255}\}$

What is $\mathbb{P}(Int(Hex(Hash(Encode(x)))) \in S)$?

Examples

Let $S \coloneqq \{n \in \{0, ...2^{256} - 1\} : n \leqslant 2^{255}\}$

What is $\mathbb{P}(Int(Hex(Hash(Encode(x)))) \in S)$?

$\frac{2^{255}+1}{2^{256}}$

Let $S \coloneqq \{n \in \{0, ...2^{256} - 1\} : n \,\%\, 16 = 0\}$

What is $\mathbb{P}(Int(Hex(Hash(Encode(x)))) \in S)$?

Suppose the network computes N hashes within 1 second. Suppose further each hash produces a valid block with probability $p \in [0, 1]$. How many valid blocks do we expect within 1 second?

$$
\begin{aligned}
&\mathbb{E}[\text{Valid Blocks in 1 second}] \\
&= \mathbb{E}[\sum_{n=1}^{N} \mathcal{I}\{nth \text{ hash produces a valid block}\}] \\
&= \sum_{n=1}^{N} \mathbb{P}\{nth \text{ hash produces a valid block}\} \\
&= N \times p
\end{aligned}
$$

Suppose the network computes N hashes within 1 second. Suppose further each hash produces a valid block with probability $p \in [0, 1]$. How many valid blocks do we expect within 1 second?

$$\begin{aligned}
&\mathbb{E}[\text{Valid Blocks in 1 second}] \\
&= \mathbb{E}[\sum_{n=1}^{N} \mathcal{I}\{nth \text{ hash produces a valid block}\}] \\
&= \sum_{n=1}^{N} \mathbb{P}\{nth \text{ hash produces a valid block}\} \\
&= N \times p
\end{aligned}$$

If the network hash-rate is fixed then we can only speed up the blockchain by increasing p

Are there any downsides to increasing p?

Forks

What if two miners find a block at the same time?

Forks

What if two miners find a block at the same time?

... that will probably never happen

Forks

What if two miners find a block at the same time?

... that will probably never happen

... but it's a distributed system! Miners need to communicate and communication takes time. What if Miner 1 solves then puzzle and afterwards Miner 2 solves the puzzle before she hears from Miner 1?

That will create a "fork" because Miners will disagree about who solved the PoW puzzle.

Forks

What if two miners find a block at the same time?

... that will probably never happen

... but it's a distributed system! Miners need to communicate and communication takes time. What if Miner 1 solves then puzzle and afterwards Miner 2 solves the puzzle before she hears from Miner 1?

That will create a "fork" because Miners will disagree about who solved the PoW puzzle.

Why can't the mining network agree that both solutions are valid?

Forks

What if two miners find a block at the same time?

... that will probably never happen

... but it's a distributed system! Miners need to communicate and communication takes time. What if Miner 1 solves then puzzle and afterwards Miner 2 solves the puzzle before she hears from Miner 1?

That will create a "fork" because Miners will disagree about who solved the PoW puzzle.

Why can't the mining network agree that both solutions are valid? (Check Lecture 17 if unclear)

Fork Probability

Let's suppose each miner hashes once at the start of each second and it takes one second to communicate. Then,

$$\begin{aligned}
&\mathbb{P}\{\text{Fork}\} \\
&= \mathbb{P}\{\geqslant 2 \text{ Valid Blocks}\} \\
&= 1 - \mathbb{P}\{0 \text{ Valid Blocks}\} - \mathbb{P}\{1 \text{ Valid Block}\} \\
&= 1 - (1-p)^N - N \times p(1-p)^{N-1}
\end{aligned}$$

What happens as p increases?

What can we conclude about throughput and fork probabilities?

Do It Yourself

Let's Hash...

Bitcoin is a payments blockchain

People use payment systems for speed

How can Bitcoin achieve widespread adoption if it's slow?

Maybe we should just speed up the blockchain and put up with forks?

Proof-of-Work's Limited Adoption Problem*

Franz J. Hinzen† Kose John‡ Fahad Saleh§

"A question remains regarding whether Bitcoin's limited usage arises due to its infancy or because of its underlying economic structure. This paper answers that question... the economics of PoW payments blockchains make limited adoption an inescapable outcome."

PoW Payments Blockchain

- Electronic Payment Ledger
  - Transactions are recorded in discrete chunks called blocks
  - Blocks are chained together in a near-chronological order
  - Speed is Service
- Permissionless Distributed System
  - Nodes Must Agree on Ledger Contents
  - Free Entry among Miners

Typical PoW blockchains impose a supply constraint

Positive demand shocks induces a price increase (fees)

Fee increases induces Miner entry

Miner entry protracts consensus process

Prohibitive wait times result

Payment system viability relies on speed, so limited adoption arises

Fixed Supply + Free Entry + Consensus = Limited Adoption

One putative solution: Relax the artificial supply constraint
i.e., Let block times vary with demand

One putative solution: Relax the artificial supply constraint
i.e., Let block times vary with demand

Result: Arbitrarily fast block times cause delays to diverge purely due to the consensus process

Thus, even with dynamic block times, limited adoption obtains

One putative solution: Relax the artificial supply constraint i.e., Let block times vary with demand

Result: Arbitrarily fast block times cause delays to diverge purely due to the consensus process

Thus, even with dynamic block times, limited adoption obtains

Speeding up the blockchain... does not speed up the blockchain!

Then... what are the prospects for blockchain?

Then... what are the prospects for blockchain?

> Now this is not the end. It is not even the beginning of the end. But it is, perhaps, the end of the beginning.
>
> **Winston Churchill**

"Our critique does not apply to other blockchains... [and therefore] highlights the need for research on alternatives..."
- Hinzen, John and Saleh (2019)

Looking Ahead

Subsequent Topics (Time Permitting)

- Proof-of-Stake
- Ethereum
- Private Blockchain