



# Bitshala

## Bitcoin Protocol Development

Group Discussion Session #3 - [Mining and Network Block Propagation](#)



**Group Discussion Session**  on Friday, May 17, 2023, at 8:00 PM IST

**Exercise Submission**  Recommend to submit by next Sunday, May 19, 2023

### Meeting Notes & Reminders

- Please try to keep your cameras on as these sessions wouldn't be recorded
- In case you have an updated Discord name during group discussion, please let BitShala Discord admins know and they would update your name in the upcoming instruction sheet

### Your action items

1. Read study material for Session 3: [Mining and Network Block Propagation](#)
2. Review the assigned group, chapter(s), and question(s) provided below. Prepare your answers for the group discussion.
3. If assigned as a deputy , familiarize yourself with the expectations outlined in the [link](#). Your assistance will be valuable in guiding and facilitating the discussion.
4. Join the assigned Group Discussion room on time.
5. Introduce yourself and answer the assigned questions with the help of the deputy  during the group discussion.
6. After the group discussion, return to the BitShala #Lounge where we conclude the discussion with all Cohort participants.

### This week's Chapters:

Week 3: – [Mining and Network Block Propagation](#)

### This week's Questions:

Round 1:

- Why would some miners use parts of the version field as a nonce? What effect did this have on nodes?
- How do P2Pools work? Advantages and disadvantages? Why aren't there any mainstream P2Pools today in the market?



# Bitshala

- How far back into the past can the timestamp in blocks be? Is this validated? How can this be attacked?
- Have we seen the difficulty retarget algorithm be manipulated in other projects? Is this a threat to Bitcoin?
- In your opinion, is it a good or bad thing that specialized hardware is now needed to mine bitcoin rather than letting individual users participate in that part of the ecosystem?
- Consider the following scenario: Segwit2x didn't happen (or miners didn't throw in support for it) and UASF (BIP148) ended up causing a chain split on August 1st, 2017, with minority mining support (e.g. ~10-20%). What would likely happen as a result?
- Can you ensure the transaction will be processed even if you send it with low fees? Which mechanisms do you have to ensure a stuck transaction (due to low fees) gets processed?
- Some mempool divergence is natural in a decentralized system. What negative side effects might we incur if the level of mempool divergence between nodes becomes "too high"? Consider other stack layers (P2P, wallet, validation etc.). What level of divergence do you think the system can safely tolerate?

## Round 2:

- How can changes to Bitcoin's P2P protocol affect mining?
- How is a high stale block rate the best indicator that block propagation times are too high?
- While a low stale block rate can be an indicator that block propagation times are good, it could also be an indicator of something more problematic. What could be a bad reason for there to be very few stale blocks?
- Greg Maxwell mentioned that miners are hesitant to connect with one another directly, even though it would speed up block propagation. Why?
- A low block-orphaning rate can be an indicator that block propagation times are good. It could also be an indicator of something more problematic. What could be a bad reason for there to be very few orphans?



# Bitshala

- How could we speed up block propagation in the network and why is that important for decentralization?
- Compact block relay is a good way to reduce the amount of bandwidth to propagate new blocks to full nodes, but is it the fastest method for a synced node given peers may need to request missing transactions?
- What is a BGP Hijack attack? What prevents it?

## Exercise:

For exercise please create an account on Github Classroom. The link of the weekly exercises gets updated on BitShala Github Classroom.

Here's the link to the exercise - <https://classroom.github.com/a/oVRn6YKx>

For any help related to the exercise feel free to ask questions in the BPD #dev-help of discord.

## Study Group, Meeting Link, and Questions:

Main Hall Link: <https://discord.gg/MBvB3ngyDv?event=1224717900892606465>

Respective Group's Discord Link:

Group 1: <https://discord.gg/MqeQRNcm5k>

Group 2: <https://discord.gg/RNa8bJZF8e>

Group 3: <https://discord.gg/gm8DQSU6G>

Group 4: <https://discord.gg/9uXzCDvc4e>

Group 5: <https://discord.gg/D8qU7NXxAR>

Group 6: <https://discord.gg/cwahh2xtw9>

Group 7: <https://discord.gg/96Qu4NbSgn>

## Group Member Question

Group	Name / DiscordName	Round 1	Round 2
<a href="#">Group 1</a>	ahasunos / thevirtualbuddy	Why would some miners use parts of the version field as a nonce? What effect did this have on nodes?	How can changes to Bitcoin's P2P protocol affect mining?
	yami	How do P2Pools work? Advantages and disadvantages? Why aren't there any	How is a high stale block rate the best indicator that block propagation times are



# Bitshala

		mainstream P2Pools today in the market?	too high?
	Divyansh	How far back into the past can the timestamp in blocks be? Is this validated? How can this be attacked?	Alternatively, while a low stale block rate can be an indicator that block propagation times are good, it could also be an indicator of something more problematic. What could be a bad reason for there to be very few stale blocks?
	Sahil tgs	Have we seen the difficulty retarget algorithm be manipulated in other projects? Is this a threat to Bitcoin?	Greg Maxwell mentioned that miners are hesitant to connect with one another directly, even though it would speed up block propagation. Why?
	Olanma 🤖	In your opinion, is it a good or bad thing that specialized hardware is now needed to mine bitcoin rather than letting individual users participate in that part of the ecosystem?	A low block-orphaning rate can be an indicator that block propagation times are good. It could also be an indicator of something more problematic. What could be a bad reason for there to be very few orphans?
	Akshay Shukla	Consider the following scenario: Segwit2x didn't happen (or miners didn't throw in support for it) and UASF (BIP148) ended up causing a chain split on August 1st, 2017, with minority mining support (e.g. ~10-20%). What would likely happen as a result?	How could we speed up block propagation in the network and why is that important for decentralization?
	codingp110	Can you ensure the transaction will be processed even if you send it with low fees? Which mechanisms do you have to ensure a stuck transaction (due to low fees) gets processed?	Compact block relay is a good way to reduce the amount of bandwidth to propagate new blocks to full nodes, but is it the fastest method for a synced node given peers may need to request missing transactions?
	Faisal Qureshi	Some mempool divergence is natural in a decentralized system. What negative side effects might we incur if the level of mempool divergence between nodes becomes "too high"? Consider other stack layers (P2P, wallet, validation etc.). What level of divergence do you think the system can safely tolerate?	What is a BGP Hijack attack? What prevents it?
<a href="#">Group 2</a>	Yash Gupta	Why would some miners use parts of the version field as a nonce? What effect did this have on nodes?	How can changes to Bitcoin's P2P protocol affect mining?
	claddy	How do P2Pools work? Advantages and disadvantages? Why aren't there any mainstream P2Pools today in the market?	How is a high stale block rate the best indicator that block propagation times are too high?



# Bitshala

	Bala	How far back into the past can the timestamp in blocks be? Is this validated? How can this be attacked?	Alternatively, while a low stale block rate can be an indicator that block propagation times are good, it could also be an indicator of something more problematic. What could be a bad reason for there to be very few stale blocks?
	plebji	Have we seen the difficulty retarget algorithm be manipulated in other projects? Is this a threat to Bitcoin?	Greg Maxwell mentioned that miners are hesitant to connect with one another directly, even though it would speed up block propagation. Why?
	Beulah Evanjalin 🤖	In your opinion, is it a good or bad thing that specialized hardware is now needed to mine bitcoin rather than letting individual users participate in that part of the ecosystem?	A low block-orphaning rate can be an indicator that block propagation times are good. It could also be an indicator of something more problematic. What could be a bad reason for there to be very few orphans?
	Agnivo	Consider the following scenario: Segwit2x didn't happen (or miners didn't throw in support for it) and UASF (BIP148) ended up causing a chain split on August 1st, 2017, with minority mining support (e.g. ~10-20%). What would likely happen as a result?	How could we speed up block propagation in the network and why is that important for decentralization?
	47h4rv4	Can you ensure the transaction will be processed even if you send it with low fees? Which mechanisms do you have to ensure a stuck transaction (due to low fees) gets processed?	Compact block relay is a good way to reduce the amount of bandwidth to propagate new blocks to full nodes, but is it the fastest method for a synced node given peers may need to request missing transactions?
	Basanta Goswami	Some mempool divergence is natural in a decentralized system. What negative side effects might we incur if the level of mempool divergence between nodes becomes "too high"? Consider other stack layers (P2P, wallet, validation etc.). What level of divergence do you think the system can safely tolerate?	What is a BGP Hijack attack? What prevents it?
<a href="#">Group 3</a>	BlueHill	Why would some miners use parts of the version field as a nonce? What effect did this have on nodes?	How can changes to Bitcoin's P2P protocol affect mining?
	delcin	How do P2Pools work? Advantages and disadvantages? Why aren't there any mainstream P2Pools today in the market?	How is a high stale block rate the best indicator that block propagation times are too high?
	Tavis Mariageorge James	How far back into the past can the timestamp in blocks be? Is this validated? How can this be attacked?	Alternatively, while a low stale block rate can be an indicator that block propagation times are good, it could also be an indicator



# Bitshala

			of something more problematic. What could be a bad reason for there to be very few stale blocks?
	Mango Elephant	Have we seen the difficulty retarget algorithm be manipulated in other projects? Is this a threat to Bitcoin?	Greg Maxwell mentioned that miners are hesitant to connect with one another directly, even though it would speed up block propagation. Why?
	Bhupattii 🧐	In your opinion, is it a good or bad thing that specialized hardware is now needed to mine bitcoin rather than letting individual users participate in that part of the ecosystem?	A low block-orphaning rate can be an indicator that block propagation times are good. It could also be an indicator of something more problematic. What could be a bad reason for there to be very few orphans?
	Aditya Gupta	Consider the following scenario: Segwit2x didn't happen (or miners didn't throw in support for it) and UASF (BIP148) ended up causing a chain split on August 1st, 2017, with minority mining support (e.g. ~10-20%). What would likely happen as a result?	How could we speed up block propagation in the network and why is that important for decentralization?
	Deepto	Can you ensure the transaction will be processed even if you send it with low fees? Which mechanisms do you have to ensure a stuck transaction (due to low fees) gets processed?	Compact block relay is a good way to reduce the amount of bandwidth to propagate new blocks to full nodes, but is it the fastest method for a synced node given peers may need to request missing transactions?
	Savil	Some mempool divergence is natural in a decentralized system. What negative side effects might we incur if the level of mempool divergence between nodes becomes "too high"? Consider other stack layers (P2P, wallet, validation etc.). What level of divergence do you think the system can safely tolerate?	What is a BGP Hijack attack? What prevents it?
<a href="#">Group 4</a>	Harsh Jain	Why would some miners use parts of the version field as a nonce? What effect did this have on nodes?	How can changes to Bitcoin's P2P protocol affect mining?
	Sambhav	How do P2Pools work? Advantages and disadvantages? Why aren't there any mainstream P2Pools today in the market?	How is a high stale block rate the best indicator that block propagation times are too high?
	mrinmoy 🧐	How far back into the past can the timestamp in blocks be? Is this validated? How can this be attacked?	Alternatively, while a low stale block rate can be an indicator that block propagation times are good, it could also be an indicator of something more problematic. What could be a bad reason for there to be very few stale blocks?



# Bitshala

	Ranjithkumar Annadurai	Have we seen the difficulty retarget algorithm be manipulated in other projects? Is this a threat to Bitcoin?	Greg Maxwell mentioned that miners are hesitant to connect with one another directly, even though it would speed up block propagation. Why?
	P.M.Jesu Melwin	In your opinion, is it a good or bad thing that specialized hardware is now needed to mine bitcoin rather than letting individual users participate in that part of the ecosystem?	A low block-orphaning rate can be an indicator that block propagation times are good. It could also be an indicator of something more problematic. What could be a bad reason for there to be very few orphans?
	PAVAN KALYAN S	Consider the following scenario: Segwit2x didn't happen (or miners didn't throw in support for it) and UASF (BIP148) ended up causing a chain split on August 1st, 2017, with minority mining support (e.g. ~10-20%). What would likely happen as a result?	How could we speed up block propagation in the network and why is that important for decentralization?
	Makam Aravind	Can you ensure the transaction will be processed even if you send it with low fees? Which mechanisms do you have to ensure a stuck transaction (due to low fees) gets processed?	Compact block relay is a good way to reduce the amount of bandwidth to propagate new blocks to full nodes, but is it the fastest method for a synced node given peers may need to request missing transactions?
	Panuganti Neha	Some mempool divergence is natural in a decentralized system. What negative side effects might we incur if the level of mempool divergence between nodes becomes "too high"? Consider other stack layers (P2P, wallet, validation etc.). What level of divergence do you think the system can safely tolerate?	What is a BGP Hijack attack? What prevents it?
<a href="#">Group 5</a>	Vasu Khanna	Why would some miners use parts of the version field as a nonce? What effect did this have on nodes?	How can changes to Bitcoin's P2P protocol affect mining?
	Jhelam Rout	How do P2Pools work? Advantages and disadvantages? Why aren't there any mainstream P2Pools today in the market?	How is a high stale block rate the best indicator that block propagation times are too high?
	Aadarsh	How far back into the past can the timestamp in blocks be? Is this validated? How can this be attacked?	Alternatively, while a low stale block rate can be an indicator that block propagation times are good, it could also be an indicator of something more problematic. What could be a bad reason for there to be very few stale blocks?
	Kinshuk 🤖	Have we seen the difficulty retarget algorithm be manipulated in other projects? Is this a threat to Bitcoin?	Greg Maxwell mentioned that miners are hesitant to connect with one another directly, even though it would speed up



# Bitshala

			block propagation. Why?
	bit-aloo	In your opinion, is it a good or bad thing that specialized hardware is now needed to mine bitcoin rather than letting individual users participate in that part of the ecosystem?	A low block-orphaning rate can be an indicator that block propagation times are good. It could also be an indicator of something more problematic. What could be a bad reason for there to be very few orphans?
	Vinay	Consider the following scenario: Segwit2x didn't happen (or miners didn't throw in support for it) and UASF (BIP148) ended up causing a chain split on August 1st, 2017, with minority mining support (e.g. ~10-20%). What would likely happen as a result?	How could we speed up block propagation in the network and why is that important for decentralization?
	Shivansh Gupta	Can you ensure the transaction will be processed even if you send it with low fees? Which mechanisms do you have to ensure a stuck transaction (due to low fees) gets processed?	Compact block relay is a good way to reduce the amount of bandwidth to propagate new blocks to full nodes, but is it the fastest method for a synced node given peers may need to request missing transactions?
	Prakash	Some mempool divergence is natural in a decentralized system. What negative side effects might we incur if the level of mempool divergence between nodes becomes "too high"? Consider other stack layers (P2P, wallet, validation etc.). What level of divergence do you think the system can safely tolerate?	What is a BGP Hijack attack? What prevents it?
<a href="#">Group 6</a>	Luciana/hazel	Why would some miners use parts of the version field as a nonce? What effect did this have on nodes?	How can changes to Bitcoin's P2P protocol affect mining?
	Suparnojit Sarkar	How do P2Pools work? Advantages and disadvantages? Why aren't there any mainstream P2Pools today in the market?	How is a high stale block rate the best indicator that block propagation times are too high?
	Ayush Bachan	How far back into the past can the timestamp in blocks be? Is this validated? How can this be attacked?	Alternatively, while a low stale block rate can be an indicator that block propagation times are good, it could also be an indicator of something more problematic. What could be a bad reason for there to be very few stale blocks?
	Praveen	Have we seen the difficulty retarget algorithm be manipulated in other projects? Is this a threat to Bitcoin?	Greg Maxwell mentioned that miners are hesitant to connect with one another directly, even though it would speed up block propagation. Why?





# Bitshala

	Tanveer 🧑	In your opinion, is it a good or bad thing that specialized hardware is now needed to mine bitcoin rather than letting individual users participate in that part of the ecosystem?	A low block-orphaning rate can be an indicator that block propagation times are good. It could also be an indicator of something more problematic. What could be a bad reason for there to be very few orphans?
	Saurav	Consider the following scenario: Segwit2x didn't happen (or miners didn't throw in support for it) and UASF (BIP148) ended up causing a chain split on August 1st, 2017, with minority mining support (e.g. ~10-20%). What would likely happen as a result?	How could we speed up block propagation in the network and why is that important for decentralization?
	ajeet	Can you ensure the transaction will be processed even if you send it with low fees? Which mechanisms do you have to ensure a stuck transaction (due to low fees) gets processed?	Compact block relay is a good way to reduce the amount of bandwidth to propagate new blocks to full nodes, but is it the fastest method for a synced node given peers may need to request missing transactions?
	Aman Kumar Pandey	Some mempool divergence is natural in a decentralized system. What negative side effects might we incur if the level of mempool divergence between nodes becomes "too high"? Consider other stack layers (P2P, wallet, validation etc.). What level of divergence do you think the system can safely tolerate?	What is a BGP Hijack attack? What prevents it?
<a href="#">Group 7</a>	S S Pratap Tanari	Why would some miners use parts of the version field as a nonce? What effect did this have on nodes?	How can changes to Bitcoin's P2P protocol affect mining?
	Ankush Sharesth	How do P2Pools work? Advantages and disadvantages? Why aren't there any mainstream P2Pools today in the market?	How is a high stale block rate the best indicator that block propagation times are too high?
	Mccalabrese	How far back into the past can the timestamp in blocks be? Is this validated? How can this be attacked?	Alternatively, while a low stale block rate can be an indicator that block propagation times are good, it could also be an indicator of something more problematic. What could be a bad reason for there to be very few stale blocks?
	Md amir	Have we seen the difficulty retarget algorithm be manipulated in other projects? Is this a threat to Bitcoin?	Greg Maxwell mentioned that miners are hesitant to connect with one another directly, even though it would speed up block propagation. Why?
	sudonims 🧑	In your opinion, is it a good or bad thing that specialized hardware is now needed to mine bitcoin rather than letting	A low block-orphaning rate can be an indicator that block propagation times are good. It could also be an indicator of



# Bitshala

		individual users participate in that part of the ecosystem?	something more problematic. What could be a bad reason for there to be very few orphans?
	Pallab J D Goswami	Consider the following scenario: Segwit2x didn't happen (or miners didn't throw in support for it) and UASF (BIP148) ended up causing a chain split on August 1st, 2017, with minority mining support (e.g. ~10-20%). What would likely happen as a result?	How could we speed up block propagation in the network and why is that important for decentralization?
	Sameer	Can you ensure the transaction will be processed even if you send it with low fees? Which mechanisms do you have to ensure a stuck transaction (due to low fees) gets processed?	Compact block relay is a good way to reduce the amount of bandwidth to propagate new blocks to full nodes, but is it the fastest method for a synced node given peers may need to request missing transactions?
	gite	Some mempool divergence is natural in a decentralized system. What negative side effects might we incur if the level of mempool divergence between nodes becomes "too high"? Consider other stack layers (P2P, wallet, validation etc.). What level of divergence do you think the system can safely tolerate?	What is a BGP Hijack attack? What prevents it?