Decentralised Mining Pool for Bitcoin (Draft 0.1)

Kulpreet Singh

Abstract

Bitcoin p2pool's usage has steadily declined over the years, negatively impacting bitcoin's decentralisation. The primary problems with p2pool are twofold. First, the variance in earnings for miners increases with total hashrate participating in the pool. Second, payouts to miners require a linearly increasing blockspace with the number of miners participating in the pool. There are two different proposals under discussion that address these problems, (i) building a directed acyclic graph (DAG) of miner's shares such that miners are rewarded for all their proof of work, and (ii) using payment channels to distribute payouts to miners. In this paper, we present a solution that builds on these two proposals. A DAG of shares is used to compute rewards, and mining rewards are paid out by an anonymous hub communicating with the miners using I2P. Using the payment channels construction, neither the hub nor the miners can cheat. We show that our approach is incentives compatible and describe how the hub maintains its anonymity to resist DDoS attacks.

1 Motivation

P2Pool [4] helps bitcoin's decentralisation by allowing miners to select which transactions they mine. This avoids any potential transaction censorship by pool operators. However, the construction used by P2Pool faces a number of problems that has resulted in miners abandoning the pool. The most often cited problems are:

1. Large variance in earnings for miners.
2. Large number of stale blocks.
3. Large block space requirement for payouts.

The first two problems are a direct consequence of the shares block rate limited to 30 seconds for the bitcoin p2pool. Intuitively, as the hash rate participating in the pool goes up, the difficulty for 30 seconds block rate goes up and smaller miners find it harder to find shares within a 30 second period. This results in an increase in the variance for shares found by miners and thus for the rewards earned by the miners. Ethereum's inclusive protocols [10] address the problem where smaller pools can continue to get rewarded for their PoW, without an increase in variance with increase in global hash rate.

Payouts in P2Pool are included in the coinbase of the block being mined. As the number of participants in P2Pool increase the size of the coinbase transaction increases taking up valuable blockspace that the miners could have earned fees from instead. This puts a cap of sorts on the number of participants in P2Pool.

Knowing the challenges faced by P2Pool, we list the goals of a new decentralised mining pool as:

1. Reduce variance for miners with increasing pool hash rate.

2. Make payouts to miners with constant size block space requirement.

3. Allow miners to select transactions they want to mine, with no potential for a censor to deny them payouts.

4. Provide building blocks for a hash rate futures market. [1]

2 Current Proposals

TerraHash Coin [11], Jute [18] and [17] use a DAG for faster block times and focus on changing the consensus layer of bitcoin. These proposals allow for miners to produce shares that have conflicting transactions and then apply rules to find a set of transactions acceptable at various cuts of the DAG.

Braiding the blockchain proposal [11] shows how smaller more frequent blocks can form a DAG of blocks, with each block pointing to one or more one previous blocks. Blocks in the braid, called beads, can have transactions repeated in different blocks. The proposal describes how duplicate and double spend transactions can be resolved to reach a decision on the state of the ledger at any cut of the DAG.

In the proposal, miners earn a coin native to the braid blockchain, called TerraHash Coin. This coin can then be swapped for BTC. The proposal doesn't yet define how this native coin will be swapped for bitcoin. Some of the suggestions under discussion include using atomic swaps, burning the TerraHash Coin, or using financial instruments like futures of the bitcoin's hash rate to swap TerraHash Coins for BTC. The problems with the atomic swap approach is the need for $O(n)$ block space in number of miners, as we need two transactions to execute a swap with each miner payout. Burning THCoins for BTC requires a trusted third party to execute the burn. Finally, trading THCoins for BTC futures has the problem of introducing centralisation on the futures market operator. There is some discussion around using DEXes for executing futures contracts, but and these are initial ideas and we will evaluted them in the future for incorporating them into our proposal once they have been developed further.

[1] We don't elaborate on this goal in this paper, but readers can look up the gist on TerraHash coins https://gist.github.com/kulpreet/19927c7188a4224ce2de43efb3c69370

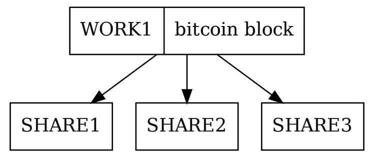

Figure 1: Each WORK generated and shared by a miner is then followed by the SHAREs the miner finds.

Belcher [6] proposes using payment channels to avoid using block space for making payouts to miners. The construction uses payment channels between federated hubs to pay miners after a block has been successfully mined. The payouts are made after a long enough period, similar to the 100 blocks requirements for spending from coinbase transactions. The hub locks in BTC for each miner by opening payment channels for each of the miners. The construction shows how both miners and hubs can not cheat and how the funders of the hub earns rewards for funding the payment channels.

The two ideas of using a DAG and payment channels for rewards payouts together present a potential path for rebooting P2Pool. In the rest of the paper we present a modified version of TerraHash Coin and show how the various components work together.

3 Decentralised Bitcoin Mining

In this section we present a modified version of TerraHash Coin. We propose building a DAG of miner's shares and use that to determine the payout distribution between miners. We then show that miners are rewarded for shares that they broadcast to the p2p network in a timely manner.

3.1 A DAG of Shares

Each miner builds their own block, selecting transactions according to their own criteria. We call this block the WORK. The description of WORK is then disseminated to the p2p network of miners using the compact block specifications [7]. The miner then starts mining on WORK and generates SHAREs. Figure 1 shows the relationship between WORK and its SHAREs. Each WORK created by a miner can result in multiple SHAREs and both the WORK and SHAREs are broadcast to the p2p network. When a miner receives a WORK from other miners it validates this WORK using a local bitcoin node. When a SHARE is received by a miner they are validated against the most received WORK from the miner.

Share	
Blockhash	bitcoin block hash for WORK
list < SHARE >	List of shares referenced by the SHARE
Difficulty	claimed difficulty miner is using
PubKeys	The pubkeys used by the hub to for channel management
I2P destination	The I2P destination for the hub to contact the miner

Table 1: The structure of SHAREs broadcast by miners.

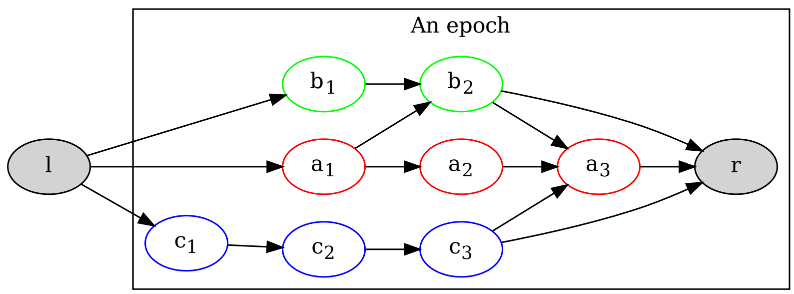

Figure 2: A epoch is defined as all the SHAREs mined between two bitcoin blocks. Here all the SHAREs between l and r are in the same *epoch*.

Table 1 shows the structure of shares broadcast by the miner. Each share includes the blockhash of the WORK the miner is working on, along with the current target difficulty used by the miner, the pubkey that the hub will use to create channels for the miner, and finally an I2P destination address for the hub to reach the miner.

Miners broadcast their SHAREs to the network using a gossip protocol and all the miners maintain the DAG as a replicated database. Each node on the DAG is a SHARE generated by a miner and all miners track the most recently received SHARE from all other miners. Miners include a hash pointer to the most recent known SHAREs from all miners in its own SHARE. This leads to all edges in the DAG pointing from a SHARE to all the SHAREs known by the miner when starting to mine a WORK. This construction of the DAG ensures that the DAG is eventually consistent on all p2p participants. The DAG also includes valid bitcoin blocks, since one of the shares eventually satisfies the then bitcoin difficulty requirement.

Each SHARE that matches or exceeds the current bitcoin difficulty starts a new *epoch* for the p2p mining pool. Figure 2 shows a DAG with three miners particpating in the pool, a, b and c. The nodes in the DAG are the shares generated by the three miners. Nodes l and r are two valid bitcoin blocks that have been mined such that they meet bitcoin's difficulty at the time, and all the blocks between l and r are in the same *epoch*.

3.1.1 Miner Defined Difficulty

The nodes in the DAG are SHAREs mined at difficulty level selected by the miner. This difficulty can be dynamically changed by the miner after each SHARE, depending on the miner's observation of the p2p network's hashrate. This dynamic difficulty adjustment allows miners to adjust the rate at which they produce SHAREs. This is important as smaller miners can produce low difficulty shares to match the share rate of the larger miners in the pool. Even if smaller miners earn a smaller reward, they will earn these rewards for all their work.

In the next section we then describe how all peers compute their fair share of profits using the DAG of shares. We then show how our reward computation algorithm is incentives compatible [16].

3.2 Incentives Compatible Rewards

Each participating node, which includes the miners and the hub, maintains a local replica of the the SHAREs DAG. Each SHARE includes a reference to the shares the miner was aware of when the SHARE was found. If a miner a doesn't include the SHAREs of miner b, it signals a failure of communication between the two miners. We introduce a rule that miner a in such a situation stops including references to b's SHAREs.

The incentive in lay terms is that all miners should include the SHAREs discovered by other miners, as otherwise they will be excluded by other miners and they will lose the opportunity to be rewarded for their work. We identify this degenerative case as "isolated miners" and argue that miners have no incentives to act in this manner. Figure 3 shows a DAG where all three miners a, b and c are working independently. In such a situation when the miner a discovers a share a_3 that is a valid bitcoin block the reward is not shared with any other miner as a_3 does not include any references to shares from other miners.

With the above understanding of why miners will co-operate, we now state the rules to calculate how the block reward should be divided between miners.

1. Traverse the DAG in reverse order from the SHARE that found a bitcoin block to the previous bitcoin block found and collect this set of shares.

2. From the above set of shares remove all shares that don't have a reverse path to the previous bitcoin block.

3. Distribute the reward between miners weighted by the sum of the difficultly of all SHAREs found by miners.

As an example, consider the p2p network of miners a, b and c with the DAG of shares as shown in Figure 4. In the DAG, the set of shares that receive reward

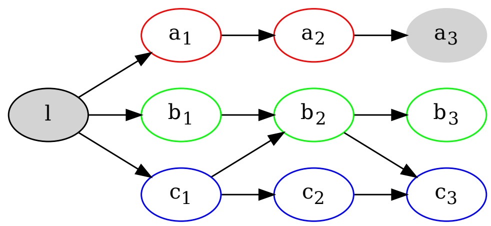

Figure 3: a discovers a share and the reward is not shared with any other miner.

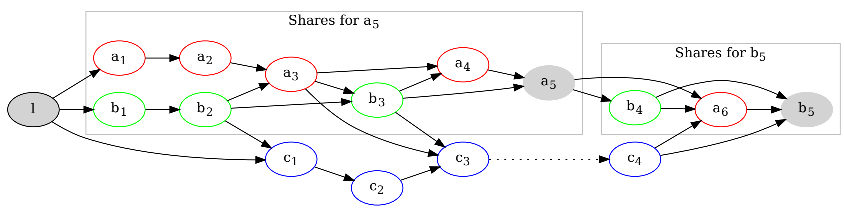

Figure 4: Two epochs in a DAG of shares mined by three mines — a, b and c. The shares in grey meet the bitcoin difficulty at the time they were mined.

proportional to their difficulty are $\{a_1..a_5, b_1..b_3\}$. The shares $\{c_1..c_3\}$ do not receive any reward as they are not reachable from the bitcoin block, a_5, even if they are reachable from l.

For the second bitcoin block b_5 only the miners a and b receive rewards in proportion to the difficulties of their shares $\{b_4, b_5, a_6\}$. c doesn't receive any reward for c_4 as it is doesn't include a reference to the last found bitcoin block a_5.

Given the above rules, we show how they together provide an incentives compatible reward function [16]. We present an outline of proofs that will be be formalised in future work.

3.2.1 Incentive Compatibility

A reward function is defined to as incentive compatible if every miner's best response strategy reports full solutions immediately [16]. Where a "full solution" is a share that meets the bitcoin network's difficulty requirement.

Given the rules in Section 3.2, if a miner finds a bitcoin block the miner wants to get maximum reward possible based on all the shares it has found and therefore is incentivized to announce their SHARE as soon as it finds the block. The longer a miner waits to announce the bitcoin block to the bitcoin network, the higher the probability that some other miner on the pool will find a different bitcoin block that doesn't reward their latest shares that haven't reached the other miner. Further still, the rewards calculation can be adjusted to give an extra reward to the miner that finds the block. This is similar to what p2pool does and Belcher also mentions in his proposal.

3.2.2 Proportional Payments

As per [16], we require that miners are paid in proportion to the amount of work they have performed.

Since rewards are calculated at the end of an epoch and a miner is incentivized to include hash pointers to the most recent shares seen from all miners, it directly follows that all miners are guaranteed payments for their shares that have reached the miner who found the block. It is also clear here that miners are incentivized to propagate their shares to the network as fast as they can.

3.2.3 Budget Balanced

Again, as per [16] we would like the pool operator to never incur a deficit. From the rules, since rewards are paid at the end of the epoch, a hub pays out rewards without losing or retaining any amount.

3.3 Payment Channels

We propose using Payment Channels for paying miners based on the proposal by Belcher [6]. The construction of the payments channels we present is similar to Belcher's construction, but there are a few changes and we highlight them before describing the details.

- In the Belcher proposal, the pool had to predict how much work miners will be able to contribute for the next block. Instead our DAG based scheme results in an incentives compatible distribution of rewards among miners.
- Belcher proposes uses multiple hubs to prevent DDoS attacks on hubs, we instead use a single hub, and prevent DDoS attacks by keeping the hub hidden using I2P [5, 9] for communication between the hub and miners.

The rest of the construction is similar to the early versions presented by Belcher — There is a one-way channel between the hub and each of the miners. The hub updates the state of each channel with appropriate reward after each block is found.

Coinbase	
`2 H M 2 CHECKMULTISIG`	(cb_1)
`OR`	
`hash(X) + Hub P2WPKH`	(cb_2)
`OR`	
`M and CHECKSEQUENCEVERIFY 6 months`	(cb_3)

Table 2: Coinbase transaction with hub and miner public keys.

3.3.1 Coinbase

We use Belcher [6] construction where each miner builds a coinbase transaction that can be spent in one of the following three ways:

1. Co-operatively by Hub and Miner, or
2. By the Hub with a hash lock for pre-image `X`, or
3. By the Miner that found the bitcoin block, but after waiting for six months.

The scriptPubKey for the above conditions in the coinbase is shown in Table 2. These conditions mean that the hub can not spend the coinbase without revealing the pre-image X. This pre-image is included in the construction of payment channels, as we will see in the next section. This use of pre-image in both the coinbase and the payment channel definition guarantees that miners get paid for their accumulated payouts if the Hub defects and spends through the cb_2 branch. We discuss how the miner and the hub don't gain by defecting in Section 3.5.

3.3.2 One-way Channels

One-Way payment channels between hub and all miners allow miners to receive payouts while consuming a constant size blockspace in the bitcoin block they mine. The use of payment channels is what makes the pool scale up without losing blockspace. The miners therefore avoid losing the fees that can be earned from the blockspace.

Just like in the early versions of proposal by Belcher we use one-way payment channels. One-Way payment channels solve the problem of aggregating a miner's payouts requiring a single blockchain transaction for spending multiple payouts earned from their PoW shares.

We use one-way instead of bidirectional payment channels as an initial implementation. If required we can switch to bidirectional channels [15] allowing miners to spend their mining payouts over the lightning network. However, for now, we deliberately stay away from the complexity of making the hub a lightning node. If there is interest from miners to use the lightning network, we can build it in the future.

Fund Transaction

Input	Output	

Hub's UTXO
(Signed by the hub)
	`2 H  M  2 CHECKMULTISIG`
	`OR`
	`2 H' M' 2 CHECKMULTISIG + Hash(X)`
	(R coins)
		(f_1)
		
		(f_2)

Table 3: Fund transaction for payment channel between hub and miner.

Refund Transaction. Locktime 6 months

Input	Output
Fund Tx (Signed by miner)	`P2WPKH Hub's address` (R coins)

Table 4: Refund transaction signed by miner and held by hub.

Each miner has a one-way payment channel with the hub using a two of two multisig with a time lock of six months. For each payout a miner receives over the payment channel, the hub will charge an agreed upon fees between the miner and the hub. Belcher's proposal recommends a 0.1% fees for the hub.

3.3.3 Payment Channel Transactions

The hub creates a funding channel locking an amount R of bitcoin. The miner then creates a refund transaction, spending the funding transaction and sending the R bitcoin back to the hub. The refund transaction has a locktime of six months allowing the miner to accumulate their payout over the six month period. The protocol can be extended to allow each miner to agree upon a locktime with the hub. In this case, the trade-off will be between the fees charged by the hub and the length of the locktime.

The funding transaction includes an input from the hub and an output that can be spent in one of the two conditions shown in Table 3. `H` and `M` are the public keys for hub and miner, they are called the co-operative keys by Belcher. While `H'` and `M'` are alternative public keys for hub and miner, and are called the uncooperative keys in the Belcher proposal.

The hub doesn't broadcast the funding transaction, instead it waits for the miner to create refund transaction. This is the same as any other timelocked one-way channel construction, i.e. the miner creates a refund transaction with a timelock, signs it and sends it to the hub. The refund transaction is shown in Table 4.

With the refund transaction, if the miner stops responding, the hub can get a refund in six months time. However, the hub can be attacked by sending requests to open new channels and locking up the hub's liquidity. We resolve this

Payment Transaction

Input	Output	
Fund Tx	`2 H  M  2 CHECKMULTISIG`	(p_1)
(Signed by the hub using H')	`OR`	
	`2 H' M' 2 CHECKMULTISIG + Hash(X)`	
	(Hub: $R - earnings$; Miner: $earnings$)	(p_2)

Table 5: Payment channel update transaction sent from hub to the miner.

by requiring the hub to open a channel to a miner only after it has contributed enough shares. This could be a parameter of the pool instantiation, anywhere between one to 100 bitcoin blocks. The threshold number of shares required before opening the channel is a configuration parameter for the hub. The miner will still receive the payouts for the shares generated, it is only that the channel opening is delayed.

On receiving the refund transaction, the hub broadcasts the funding transaction. Once the funding transaction is confirmed, the hub can start sending payouts to the miner. These payouts are determined in proportion to the shares found by the miner and included in the DAG as described in Section 3.2.

The payment transactions are updates to the channel where each update increases the earnings of the miner. The payment transactions are signed by the hub using the non-cooperating key, `H'`. Table 5 shows the structure of the payment transactions.

The hub updates the payment channel for each miner with payouts as determined by the incentives compatible rewards algorithm shown in Section 3.2. In the next section we present how the payouts are distributed, we then show how the hub and the miners are dis-incentivized to cheat.

3.4 Anonymous Payouts

Once a miner mines a share that also meets the currently bitcoin difficulty, the miner immediately broadcasts the block to the bitcoin network. The coinbase of this block as shown in Table 2 can now be spent by one of the following branches:

Co-operative Branch: (cb_1) The miner and the hub by both signing the first branch co-operatively.

Hub Branch: (cb_2) The hub alone, by publishing the pre-image `X`.

Miner Branch: (cb_3) the miner alone, after waiting for six months.

The proposal by Belcher specifies a payout algorithm that requires the hub updates the state of all channels, i.e. make payment to all miners. Once it has done so, the miner signs the first branch of the coinbase transaction and hands the coinbase to the hub. The hub can now redeem the entire payout. We use the same approach, requiring the miner to receive all channel updates from the hub before signing the co-operative branch. The miner first verifies that that the channel updates are properly signed by the hub, and there is one update for all miners in proportion to the rewards distribution algorithm.

3.5 Defecting Does Not Pay

Using the above construction of the payment channel and the distributed payout algorithm, we now show that defecting by the hub or the miner doesn't pay.

3.5.1 Hub Defects

If the hub defects and pays itself from the coinbase it uses the cb_2 branch of the coinbase. In doing so, the hub has to reveal the pre-image `X`. With the pre-image available, all miners will use the p_2 branch of their payment channel transactions and close their channels and receive all payouts earned up to that block.

It is possible that the hub defects on the very first block mined and the miners lose their earnings for that single block. But that will end the pool before it could be useful.

The hub could defect after a few blocks have been mined. In such a case the miners will receive their fair share of earnings for all previous blocks, but it will again be the end of life for the pool.

Remember the hub charges fees to fund the payment channels between the itself and the miners. When the pool ends, the hub loses a profit making opportunity. We argue that the incentive to defect reduces as the size of the pool grows.

It is worth noting that if the hub is co-opted, all it can do is deny miners a payouts for the number of blocks the pool delays the payments by. We introduced the idea of this ranging from one to 100 blocks. Further, if the hub is co-opted, all miners will immediately close their channels, collect their payouts and re-organise with a different hub.

3.5.2 Miner Defects

A miner that found the block could chose to not sign the co-operative branch (cb_1) of the coinbase. In such a case, the hub will wait for a timeout period much shorter than the locktime on the miner branch (cb_3) and receive the payout using the (cb_2) branch of the coinbase. In response to this, all other miners will close their channels by signing the p_2 branch of the payment transaction by using the pre-image `X` included in (cb_2) broadcast by the hub. This will close all channels and require that all these channels are opened again. Such an attack by the miner will hurt miners on the network who have not yet earned enough payouts to amortise the cost of closing the channel.

Say a miner starts participating in the pool, and after N blocks successfully mines a bitcoin block, but refuses to sign the co-operative branch of the coinbase allowing the hub to claim the coinbase reward. In such a case all miners have to close their channels and claim the rewards they have earned. Miners who recently joined the pool stand to lose the most because of the forced closure of channels.

However, the miner also loses any payouts for all the shares it mined since the last block was found by the pool. A malicious miner could contribute a large portion of the pool's hash rate and then refuse to sign the co-operative branch. This will disrupt the functioning of the pool and a well funded censor could be willing to execute such an attack. The only defence here is that the miners re-organise and start a different instance of the pool hiding their activity behind I2P tunnels. We elaborate on our use of I2P in Section 3.6.

3.5.3 Hub and Miner Collude

The hub and the miner could collude where they co-operate to spend the coinbase to themselves without requiring that the hub pays all other miners as per the reward schedule. The motivation for the miner is a big payout it can receive. However, such an action by the hub will end the pool and the stream of future profits for the hub.

3.5.4 DDoS on the Hub

The hub can be attacked using a distributed denial of service attack rendering it unable to process requests to open new channels and to distributed payouts to miners. Belcher in his proposal suggested the use of multiple hubs as a defence against such an attack. The proposal also points out that multiple hubs will reduce the liquidity required to open channels with miners.

According to Belcher's proposal, with multiple hubs available on the p2p network miners will open channels to all hubs and receive payouts from all of the hubs. The coinbase is split between hubs in such a way that if any hub defects, the other hubs can still spend the coinbase and split the block reward between them. In this way all miners receive payouts in proportion to the shares contributed by them.

Creating a larger coinbase for multiple hubs scales if we can use Taproot [14, 12, 13] once it is activated. The solution uses staggered timeouts for hubs to spend the coinbase in case of hubs defecting or coming under DDoS attacks. This option is worth exploring once Taproot is enabled and the pool will benefit from multiple hubs. This will be even more useful as with the multiple hubs construction reduces the liquidity requirements for all hubs. The only problem is that in case of hubs defecting, the staggered timeouts can result in a large wait for the payouts to be distributed.

We propose a different solution that requires a single hub. The advantage is a simpler channel construction and allow us to build the mining pool without waiting for Taproot activation. The single hub approach requires that all miners

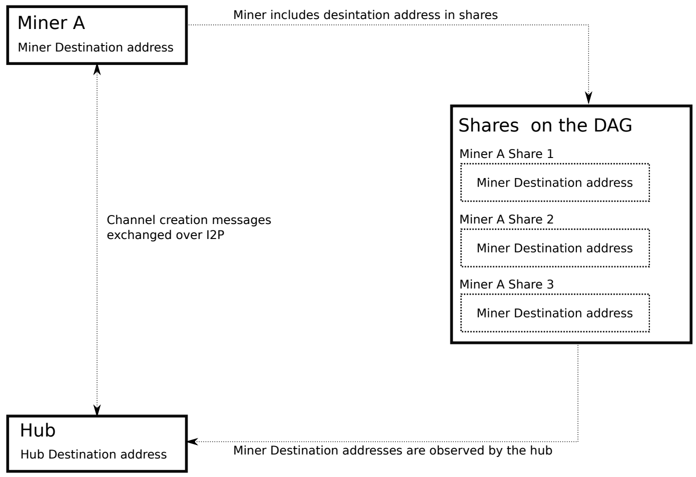

Figure 5: Discovery of miner I2P destination addresses enables communication for creating channels.

open I2P tunnels to gateways and publish the gateway's address in the shares they broadcast on the p2p network. The hub then can communicate with miners by opening new tunnels and remaining anonymous. We present this approach in the next section.

3.6 Anonymous Hub Miner Communication

The hub and the miner need to exchange messages at the time of channel creation as well updating the channel state when the hub makes a payout to the miners. The channel management messages are exchanged infrequently as compared to the SHAREs broadcast messages and don't have the same timeliness requirements as the shares broadcasts. We propose adopting a solution that doesn't compromise on the hub's anonymity and makes a trade-off with increased latency of the channel management messages.

We use I2P's tunnels to avoid compromising the anonymity by setting up separate inbound and outbound tunnels, as required by I2P. According to the I2P documentation [2]:

> A tunnel is a directed path through an explicitly selected list of routers. Layered encryption is used, so each of the routers can only decrypt a single layer. The decrypted information contains the IP of the next router, along with the encrypted information to be forwarded. Each tunnel has a starting point (the first router, also known as "gateway") and an end point. Messages can be sent only in one way. To send messages back, another tunnel is required.

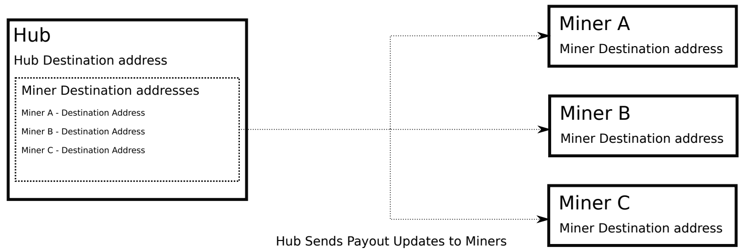

Figure 6: Hub sends one way updates to miners without revealing its destination address.

There are two types of control messages exchanged between the hub and the miner: 1. the channel creation messages when the miner first joins the pool and 2. the payout messages whenever a block is found.

Miners will run an I2P node next to their mining controller and setup an incoming tunnel. Once the tunnel is ready, miners include their I2P destination address in their share headers. The hub can then send messages to the miner through the I2P tunnel. By hiding their real I.P. address miners can increase their anonymity, and in turn help the hub maintain its anonymity too.

The hub participates in the shares broadcast p2p network and identifies a new miner along with the new miner's destination address. Once the miner has mined for a certain time period, the hub contacts the miner and provides its own destination address in the message [3]. Figure 6 shows how the "Miner A" announces its I2P destination address, enabling the hub to contact the miner for exchanging channel creation messages. The hub inturn uses different destination addresses when contacting each hub, further strengthening its anonymity and resistance to DDoS attacks.

To prevent the tunnel endpoint and gateway from seeing the messages being exchanged, the hub and the miner use I2P's layered encryption, called garlic routing [1]. With the destination addresses of both the new miner and the hub known to each other the two can proceed to anonymously setup a payment channel as described in Section 3.3.

To send payouts as channel state updates, the hub again uses the I2P destination address of each miner and sends a one way message, with no reply destination included in the message. This allows the hub to remain anonymous and makes it relatively hard to DDoS the hub. The hub sends all miners updates to all payment channels. This allows the miner who discovered a block to verify that the hub has paid everyone.

4 Future Work

Our proposal presents an approach to enable decentralised mining for bitcoin. Apart from the work of describing the various components in detail, we also want to provide results from simulations, formalised proofs of rewards schemes and possible extensions to using multiple hubs.

Before we work on implementing the system, our next step is to simulate p2p mining network using ns-3 [8] and make informed decisions about how large a network a single hub can support. The observations we want to make are how large a p2p network can be sustained without an increase in work lost by miners. Each instance of the pool uses a single hub and the p2p network of miners can grow as long as miners are communicate WORK and SHAREs with each other within bounded latencies. We want to find the bounds of these limits using a simulation.

We also want to specify the p2p protocols and the message formats for both the SHAREs propagation and channel management networks. By publishing the specifications separate from the source code, we aim to receive more feedback from the community. We want to use the model presented in [16] to provide proofs for how the rewards distribution is incentives compatible. We would like to build further on the multiple hubs construction described by Belcher once Taproot is activated on bitcoin.

5 Acknowledgements

Please to review! Many wow! ;)

References

[1] Garlic routing and "garlic" terminology. `https://geti2p.net/en/docs/how/garlic-routing`.

[2] I2p: A scalable framework for anonymous communication. `https://geti2p.net/en/docs/how/tech-intro`.

[3] I2p: Streaming library. `https://geti2p.net/en/docs/api/streaming`.

[4] P2pool. `https://en.bitcoin.it/wiki/P2Pool`.

[5] ASTOLFI, F., KROESE, J., AND VAN OORSCHOT, J. I2p - the invisible internet project. Web technology report, Media Technology, Leiden University, 2015.

[6] BELCHER. Payment channel payouts: An idea for improving p2pool scalability. `https://bitcointalk.org/index.php?topic=2135429.0`.

[7] CORALLO, M. Compact block relay. `https://github.com/bitcoin/bips/blob/master/bip-0152.mediawiki`.

[8] HENDERSON, T. R., LACAGE, M., RILEY, G. F., DOWELL, C., AND KOPENA, J. Network simulations with the ns-3 simulator. *SIGCOMM demonstration 14*, 14 (2008), 527.

[9] Hoang, N. P., Kintis, P., Antonakakis, M., and Polychronakis, M. An empirical study of the i2p anonymity network and its censorship resistance.

[10] Lewenberg, Y., Sompolinsky, Y., and Zohar, A. Inclusive block chain protocols. In *Financial Cryptography and Data Security* (Berlin, Heidelberg, 2015), R. Böhme and T. Okamoto, Eds., Springer Berlin Heidelberg, pp. 528–547.

[11] McElrath, B. Decentralized mining pools for bitcoin. `https://www.youtube.com/watch?v=91WKy7RYHD4`.

[12] Pieter Wuille, Jonas Nick, A. T. Bip 341: Taproot: Segwit version 1 spending rules. `https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki`.

[13] Pieter Wuille, Jonas Nick, A. T. Bip 342: Validation of taproot scripts. `https://github.com/bitcoin/bips/blob/master/bip-0342.mediawiki`.

[14] Pieter Wuille, Jonas Nick, T. R. Bip 340: Schnorr signatures for secp256k1. `https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki`.

[15] Poon, J., and Dryja, T. The bitcoin lightning network: Scalable off-chain instant payments, 2016.

[16] Schrijvers, O., Bonneau, J., Boneh, D., and Roughgarden, T. Incentive compatibility of bitcoin mining pool reward functions. In *Financial Cryptography and Data Security* (Berlin, Heidelberg, 2017), J. Grossklags and B. Preneel, Eds., Springer Berlin Heidelberg, pp. 477–498.

[17] Sompolinsky, Y., Lewenberg, Y., and Zohar, A. Spectre: A fast and scalable cryptocurrency protocol. Cryptology ePrint Archive, Report 2016/1159, 2016. `https://eprint.iacr.org/2016/1159`.

[18] Vorick, D. Jute: More scalable, more decentralized proof-of-work consensus. `https://github.com/Taek42/jute`.