1. Introduction

Bitcoin mining can be an energy intensive process, leading to environmental concerns about its associated carbon footprint. Some reports have estimated annualized emissions to be in excess of 85 million metric tons of carbon dioxide equivalent (MtCO2e)[1] as of April 2, 2024. The reason behind this significant impact is the proof-of-work (PoW) consensus mechanism that secures the Bitcoin network. In PoW, miners engage in a competitive race to find solutions (*i.e.*, cryptographic hashes) for Bitcoin blocks, requiring powerful computational hardware like ASIC machines. As more miners join the race, the solution for a block tends to become more difficult. The continuous demand for robust computational power in PoW necessitates significant electricity usage. The use of carbon-based energy generation sources by miners results in the underlying greenhouse gas emissions footprint of the Bitcoin network.

In this paper, we present a solution to this issue by incentivizing miners that use low carbon energy sources. The proposal rewards miners with bitcoins in a trust-independent manner (*i.e.*, without having to trust a third party to earn the reward) when they verifiably use a significant portion of low carbon energy sources in their mining operations. Additionally, it aims to increase the likelihood of routing on-chain transactions to such miners. This not only acknowledges support for more environmentally responsible mining but also encourages other miners to shift towards cleaner energy sources. By promoting this transition, this solution aims to support the Bitcoin network's decarbonization in the long term by financially rewarding miners that use clean energy, while also striving for a good degree of network decentralization and maintaining robust security.

2. Solution

At a high level, the solution involves **identifying** miners that use low-emissions energy sources, **preferentially routing** on-chain transactions to these miners, and **rewarding** them using a 1-of-n multisig script[2] (i.e. any one of the n number of miners can spend the coins) which is attached to the on-chain transactions. The detailed steps are as follows:

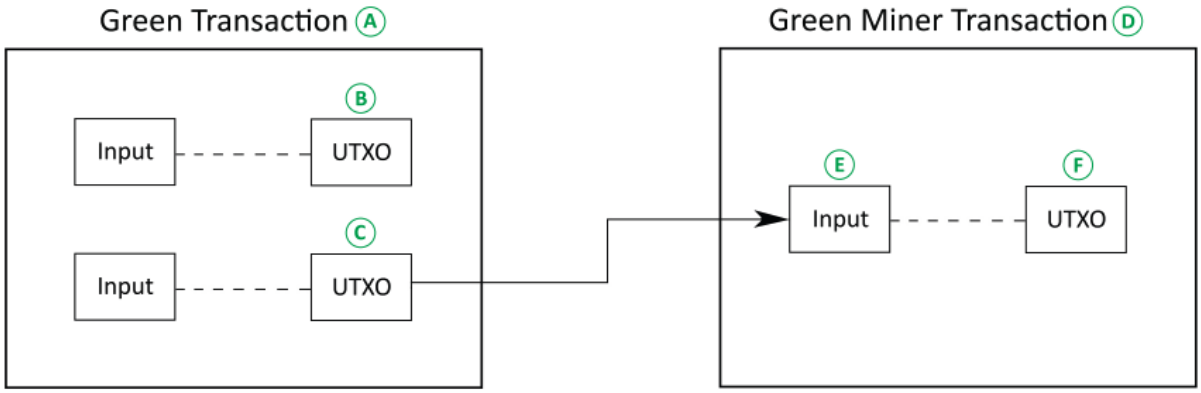
1. The first step is to identify miners that use sufficient proportion of low carbon energy in their mining operations. In this paper, we will refer to these miners as

[1] Cambridge Bitcoin Electricity Consumption Index, https://ccaf.io/cbnsi/cbeci/ghg, originally retrieved Apr. 2, 2024
[2] https://en.bitcoin.it/wiki/Multi-signature

green miners, and we explain how to identify them and determine the sufficiency of their energy usage in Section 3 below.

2. Once green miners are identified, the next step is to obtain their public keys, which will be used to distribute incentives. In this paper, these public keys are referred to as *green keys*, and these can be different from the ones that miners use to collect block rewards.
3. Green keys are then aggregated from different green miners into a single 1-of-n multisig address (designated as the *payout address*) which is used for distributing incentives denominated in bitcoins to miners. Hence, if there are n number of green miners, there will be n number of green keys but a single 1-of-n multisig payout address. This payout address will allow any one of the n green miners to claim the reward. In section 3, we will talk about the management of green keys and payout addresses.
4. To preferentially route transactions to green miners, on-chain transactions are broadcast with low transaction fees (described further below). An additional UTXO is attached to the on-chain transactions with some bitcoins locked in a 1-of-n multisig payout address as an incentive for green miners. Most miners will be disincentivized to process these transactions because of their low transaction fees, but green miners, who will be eligible for the additional incentive, can seek out these transactions (we'll refer to them as *green transactions*, labeled as "A" in the diagram below).
5. When a green miner receives the transaction in the mempool, they identify it as being a green transaction based on the multisig payout address. The miner will need to include the transaction while assembling a block and include an additional redeem transaction (labeled as "D" in the diagram below) within the same block to consume UTXO that locked bitcoins in the payout address. This additional transaction will have a recipient address belonging to the green miner. As a result, only the green miner who includes the green transaction, redeem transaction and successfully mines the next block is assured of earning the bitcoin reward.

   Even though, as described above, the low transaction fees will dissuade non-green miners from prioritizing these on-chain transactions in their block, green miners would want to prioritize these transactions because winning the block would earn them the bitcoin rewards locked in the multisig payout address. This will increase the likelihood of routing on-chain transactions to green miners and incentivize them when they win the block.



A: On-chain green transaction
(i.e. a transaction used to incentivize green miners) with low fees
B: Standard UTXO for other transactions
C: UTXO with green incentive locked in 1-of-n multisig script
D: Redeem transaction by green miner to claim the incentive
E: Input with corresponding unlocking script
F: UTXO to lock incentive to green miner's address

3. Identifying Green Miners

To help identify green miners and onboard them to the solution, we can leverage solutions by providers such as Energy Web, a global non-profit organization with a mission to accelerate the energy transition. Their "Green Proofs for Bitcoin" initiative promotes transparency and supports alignment between Bitcoin mining and global decarbonization efforts. Using the Green Proofs for Bitcoin validation platform, miners can apply for and share their sustainable mining certifications. Miners can then selectively disclose these certifications and the underlying sustainability data with crypto market participants and business counterparties.

Miners can obtain Green Proofs for Bitcoin certification by achieving either a Clean Energy Score or a Grid Impact Score higher than 50. The details of how these scores are calculated can be found here.

Energy Web will also develop a new platform for the miners interested in participating in this solution. Using this new platform, green miners can register themselves and share their green (public) keys. Green incentive program participants can then access this information to streamline the collection of green keys that can be used to generate and manage 1-of-n multisig payout addresses.

While the use of Energy Web's Green Proofs for Bitcoin validation platform is a pragmatic solution to identify green miners, there can be other solutions that would allow for the identification and onboarding of these miners in an even more decentralized manner. For example, other certification bodies could be encouraged to issue interoperable credentials to Bitcoin miners that can be taken as proof of sustainability by the green incentive program.

4. Testing with Miners

We have successfully tested the ideas behind the proposed solution with a Bitcoin miner, DMG Blockchain Solutions Inc.("DMG"), a publicly traded and vertically integrated blockchain and cryptocurrency company that manages, operates, and develops end-to-end digital solutions to monetize the blockchain ecosystem.

In the test, we broadcast multiple low fee transactions to observe how effective the solution would operate under different levels of on-chain transaction volume. Our expectation was that, depending on transaction volume, these transactions would either take a long time to confirm or eventually be dropped by the network. This would increase the chances for green miners to pick up these transactions. We also wanted to test the miner's ability to identify green transactions, include them in their block, and add a separate transaction within the same block to claim the incentive. In the following sections, we'll discuss a sample test.

4.1 Testing Setup

We publicly broadcast two transactions identified by the hashes `7c60f98157c6d9d958cc90cdf2ae30d67c237e0bb8aab03688f621004ea1a768` and `0a929ba61c72a4f3311102e7c127bb9bddabc0c652ee713a9fc791fd6fab73e1`, each of which included 0.0001 BTC as a green incentive to the payout address `32orJvB4V7sxH8m6AwwLVBKKGm142UgiYg`. The fee rates of the transactions were set to 64.8 sat/vB and 67.1 sat/vB, respectively, when the no priority fee of Bitcoin network was about 72 sat/vB.

4.2 Testing Results

The transaction landed in DMG's mempool soon after it was broadcast. They were able to detect our low fee transaction and included it in their block template. They mined the next block after two days. As we expected, no other miner picked up the low fee transaction during this period. When DMG mined the block, they had included the low fee transactions and claimed the green incentive by including transaction `8e59cf7d258e08716bfc6d4f54389495d7d62545c5950accc16ae371ab4333c3` in the same block.

This validated our belief that transactions could be preferentially routed to green miners and that those miners could receive the specified incentive using the proposed mechanism.

5. Considerations

5.1 Low fees vs. zero fees

The on-chain transactions can be broadcast with either low transaction fees or zero transaction fees to dissuade non-green miners from picking them up. Here we will discuss the tradeoffs of each option.

If the on-chain transaction is broadcast with zero fees, it can greatly discourage non-green miners from picking up our transactions. However, sometimes these transactions may not be routed to any miners. This is because some Bitcoin nodes use fee filters to decide which transactions to relay. They may configure their nodes to ignore or prioritize transactions based on the fees. Transactions with low or no fees may be filtered out and not relayed to the broader network. Also, when the nodes are accepting zero fee transactions, malicious actors can flood them with many zero-fee transactions.

The chances of a transaction flood DoS attack can be mitigated by instead using "sufficiently" low fees. However, in some instances, especially when on-chain transaction volume is low, a non-green miner can still choose to pick up the low fee transaction. Note that, in this case, the non-green miner won't be able to earn the incentive from the 1-of-n multisig payout address, while any one of the green miners can. This reward can be seen as providing an additional incentive for green miners to adopt sustainable mining practices, albeit more in the form of an indirect grant. As more green miners are onboarded to the solution, the chances of non-green miners mining the transactions should further reduce. Also, although a green miner may earn the incentive by broadcasting the redeem transaction even if a non-green miner mines the low-fee transaction, the green miner is still incentivized to mine the transaction itself as this guarantees that it will earn the reward, rather than another green miner from the multisig set.

So, the transactions should usually be broadcast with a transaction fee that is low enough to discourage a non-green miner from picking up the green transaction but sufficient to be relayed to the broader Bitcoin network and be capable of mitigating the possibility of a transaction flood DoS attack.

5.2 Storage Space

The size of transactions to redeem bitcoins locked in 1-of-n multisig can increase as more green miners are onboarded. This is because (depending on the multisig implementation) the size of the redeem script can be directly proportional to the size of n. The solution also needs extra blockchain space due to the additional transactions that miners need to add in the block to claim their incentive. In the Bitcoin ecosystem, blockchain space is a valuable resource. To efficiently utilize blockchain space, we can implement the following steps to ensure that the redemption script is space efficient:

a) Miners are first organized into m groups. If there are N miners, each group will ideally contain N/m miners. To achieve this, select an appropriate value for m, making sure that the remainder of N/m is minimized (ideally zero).
b) For every new transaction to be broadcast, cyclically iterate through m groups to select the next group of miners, take their public keys, and use them in 1-of-n multisig script where n is the number of miners in that group. For example, if there are 7 (i.e., $N=7$) green miners, one option is to create 3 (i.e., m) groups and adjust one remaining miner in the first group. Hence the first group will have $n=3$ miners while the remaining two groups will each have $n=2$ miners.

This will ensure that the size of the transaction to redeem bitcoins is bounded by the number of miners in a group. The trade-off we need to make with this option is that it reduces the number of miners that can collect the incentive from N to $\text{ceil}(N/m)$. If the specific number of miners i.e. n in a group have limited hash power or n is sufficiently small, this could lead to delays in transaction confirmations as discussed in the following section.

5.3 Transaction Confirmation Time

Prioritizing green miners may lead to longer transaction confirmation times because the solution aims to prevent non-green miners from processing our transactions. The grouping method, as explained above in section 0, can further contribute to longer confirmation times. If a transaction isn't confirmed within an acceptable timeframe, fee bumping mechanisms like RBF (Replace-By-Fee)[3] and CPFP (Child-Pays-For-Parent)[4] can be used to expedite confirmation, albeit with an increased risk of non-green miners processing the transaction. This issue will be mitigated as more green miners are onboarded to the solution.

Note that even a malicious green miner can potentially use CPFP to increase the fee of a transaction, thereby raising the chances of a non-green miner picking up the green

[3] https://en.bitcoin.it/wiki/Replace_by_fee
[4] https://en.bitcoin.it/wiki/Miner_fees#Feerates_for_dependent_transactions_.28child-pays-for-parent.29

transaction. However, this behavior can be detected on-chain, and one can take appropriate action, such as removing the miner from the solution.

5.4 Privacy

Observers can identify which transactions are incentivizing miners due to the inclusion of 1-of-n multisig script. If there are not many participants who are incentivizing green miners this way, it may be possible to establish a link between the transaction and a specific VASP that broadcast the transaction. On the flip-side however, this trade-off will allow for transparent proof that the incentives were indeed paid to the green miners.

5.5 Pooled-miners vs Solo-miners

Miners either mine in groups, referred here as *pooled miners*, by combining their computing power and resources to increase their chances of successfully mining a block, or they can mine on their own, referred here as *solo miners*, without joining a pool. For miners working in pools, there is an entity called a pool operator that manages and operates them. The pool operator is also usually responsible for distributing rewards to the miners contributing to the pool.

For our 1-of-n multisig script, the green keys of pooled miners contributing to the pool can't be used because they do not have the authority to decide which transaction will be included in the next block. So, they may not have the ability to claim the bitcoins locked in the multisig script. To address this, the script needs to reference the key of the pool operator, and the operator will then distribute rewards to the pooled miners. As a result, the 1-of-n multisig payout address will only be created using the green keys of pool operators, solo miners, or a combination of both, but not those of pooled miners.

This may change when a new feature in stratum V2 protocol, which is an improvement and upgrade to pooled mining, is adopted by pooled miners. It will enable them to include transactions they want in the block. Hence, they won't have to depend on pool operators to claim the bitcoins locked in the 1-of-n multisig script, making the solution more decentralized. The solution will then be able to use pooled miners' keys in the 1-of-n multisig script instead of the pool operator's key.

6. Alternate Approaches

The solution outlined here aims to achieve a good degree of decentralization, ease of implementation and trust independence while distributing incentives. There isn't a centralized entity that distributes incentives; instead, they are guaranteed a reward when they mine the indicated on-chain transactions and include the redeem

transaction. However, as mentioned previously in the “Considerations” section, the solution requires miners to add an extra transaction in the block to claim the incentive and there is some possibility that a non-green miner may pick up a green transaction even though they can’t claim the incentive.

While we currently believe these trade-offs are acceptable, it is possible to design alternative solutions where transactions and rewards can be sent to miners via a private mechanism rather than using the public mempool. Technologies such as lightning network and smart contracts could also be alternate ways to address these issues. However, this might come at the expense of trust dependence and a more complex implementation.

7. Conclusion

As interest in Bitcoin and the number of applications using the Bitcoin blockchain continues to grow, we should be mindful of the potential environmental impact of large-scale Bitcoin mining. One way to reduce the carbon footprint of Proof-of-Work consensus protocols like Bitcoin is to increase the use of low-carbon energy sources by Bitcoin mining operations. This paper proposes an approach to incentivize miners to use these “greener” energy sources in a manner compatible with current usage and while maintaining to the greatest extent possible the decentralized model inherent in the Bitcoin protocol. We hope that this solution contributes to further discussion and innovation around Bitcoin and its use cases and welcome industry feedback on potential improvements.

The authors wish to thank the members of PayPal’s Blockchain Research Group and Social and Environmental Impact team who helped flesh out the initial thinking behind the Green Mining Initiative as well as DMG and Energy Web for their contributions to the initial testing.