#Whitepaper

bitcoinClean

bitcoinClean: A Bitcoin hard fork with 8MB blocksize and replay protection that ensures renewable energy use for mining.

Abstract

bitcoinClean (or BCL) is a Bitcoin hard fork that addresses the rampant pollution from energy production for Bitcoin mining today. Bitcoin's success comes at huge economic and environmental cost, as multiple terawatts of energy are used to mine blocks. Most of this energy is from non-renewable sources.
A recent motherboard article calculated the energy used to confirm a single Bitcoin transaction at 215 kWh, the same amount of energy used by a US household in a week. 87% of this energy comes from fossil fuel use, on average.

bitcoinClean introduces a protocol for peer to peer verification of renewable energy use. bitcoinClean stays true to the original and tested Bitcoin protocol, and will merge future improvements one to one. We believe Bitcoin is the original cryptocoin, and the only one that has proven its viability and durability so far.

The peer to peer verification protocol is called proof-of-greenness and allows for a maximum of confidence in a scenario that is not controlled by central third parties. (which might themselves be corruptible) It aims to ensure that a maximum of miners use renewable or green energy, like water, wind, solar or biogas, geothermal and tidal energy.

bitcoinClean software forks the Bitcoin core software and introduces only minimal changes. This ensures that future improvements to the Bitcoin protocol can and will be merged to bitcoinClean effortlessly. bitcoinClean is also a full blown hard fork. Our first block will be block number 518,800. This means every holder of Bitcoin up until block 517,799 will have the same amount of bitcoinClean available for them when they choose to claim them. Block number 518,800 will arrive on the 17th of April, 2018 at about 4:30 am UTC.

The bitcoinClean team is very well aware of the security issues involved in hard forking a 170 billion dollor blockchain and will guide users by publishing how-to videos, best practice guides and participating in community discussions.

[1] https://motherboard.vice.com/en_us/article/ywbbpm/bitcoin-mining-electricity-consumption-ethereum-energy-climate-change

Introduction

Bitcoin's success came as a surprise. The brilliant simplicity of the concept in managing incentives and the non-reversible nature of its transaction managed to make Bitcoins the first true internet currency. Even though making transactions meant using command line tools at first and transactions cost single dollar fees and took up to a week until confirmed by a few.

The strength of Bitcoin lies in its elegance. It simply isn't reasonable to double spend, mining attacks are prohibitively expensive and the reward system incentivises thousands to participate in mining. Bitcoin's core development team worked extremely hard for the past years to ensure that Bitcoin remained intact. Its development seems steady, calm, well engineered and ultimately helped Bitcoin to achieve the widespread adoption it deserves. By not jumping for quick fixes, through hard forks, for instance, and waiting for great solutions to appear, Bitcoin instilled trust and confidence in merchants, buyers and investors. bitcoinClean wants to stay true to this line while adding a long needed solution to the pollution problem associated with Bitcoin mining.

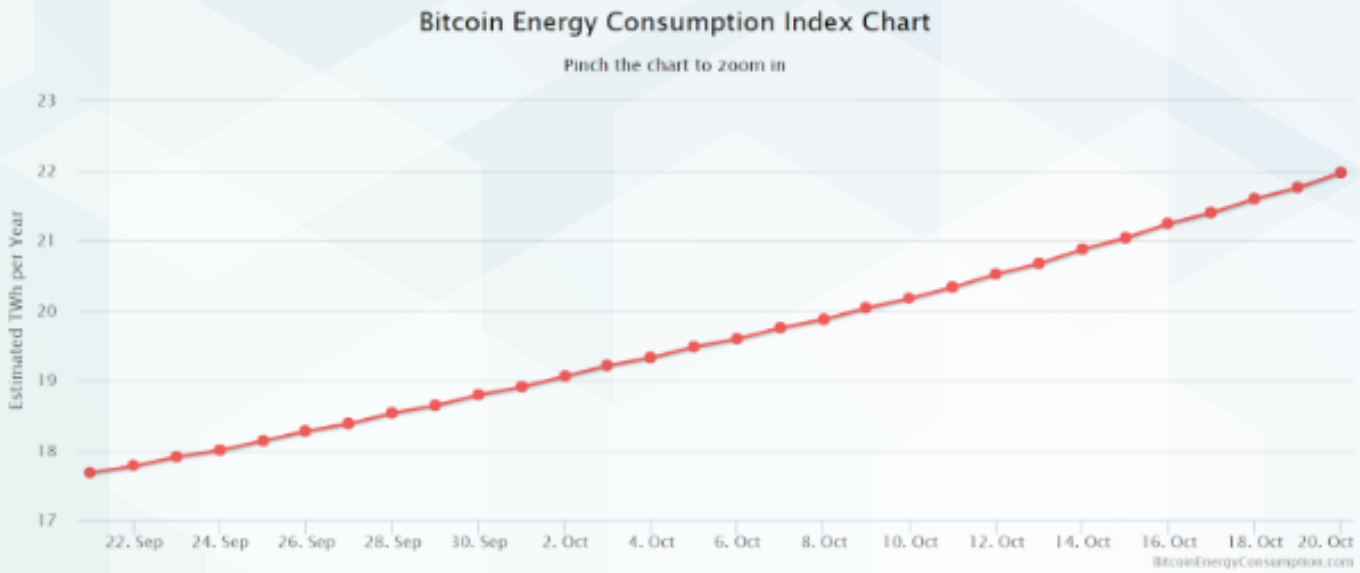
Transaction bandwidth problems

Bitcoin Cash addressed the network bandwidth problem that caused Bitcoin payments to take up to 10 days in summer 2017. Bitcoin wanted to increase its block size to 2MB with the 2X addition to the SegWit update, but failed to generate the necessary miner support in the end.
With the upcoming addition of Lightning Network transactions a very elegant solution that would also help to drastically reduce the electricity needed for one transaction. bitcoinClean will increase the blocksize to 8MB allowing up to 32 transactions per second. bitcoinClean is also Lightning Network ready! When this technology is released, bitcoinClean will adopt it immediately.

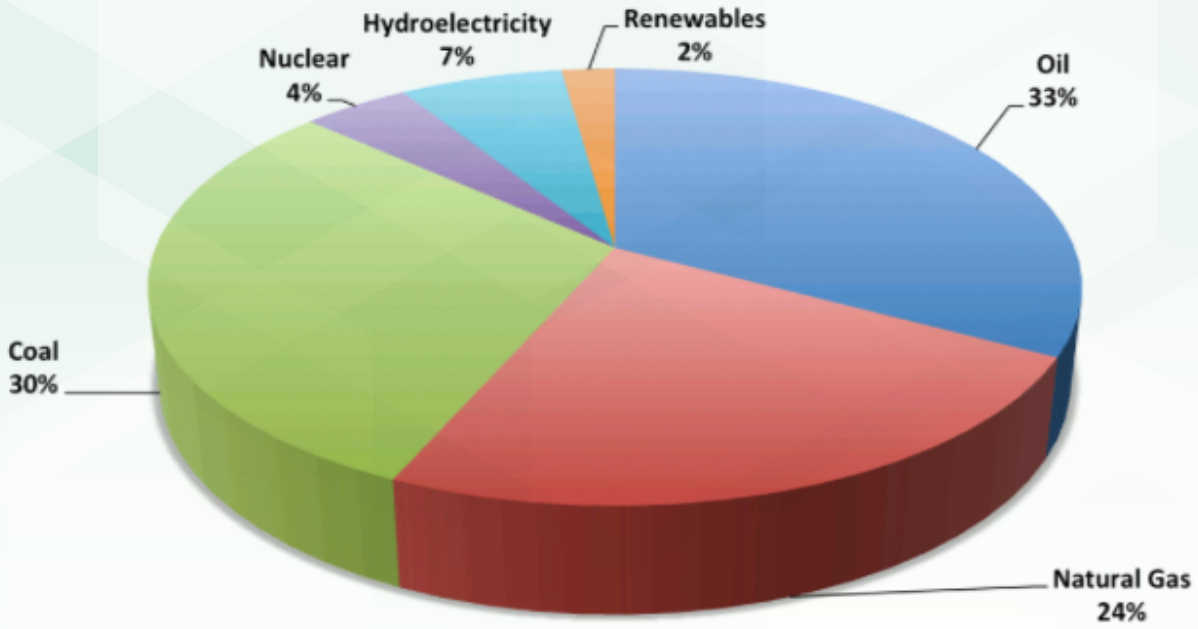
Energy for mining

Currently 12 TWh/year and rising will be consumed through Bitcoin Mining, and another 6 TWh/year by Ethereum Mining. This is the equivalent of 8 million average German households.

[2] https://en.wikipedia.org/wiki/Bitcoin_scalability_problem
[3] https://digiconomist.net/bitcoin-energy-consumption



The energy mix worldwide consist of 87% percent fossil fuels, according to BP statistical review of world energy, 2014.

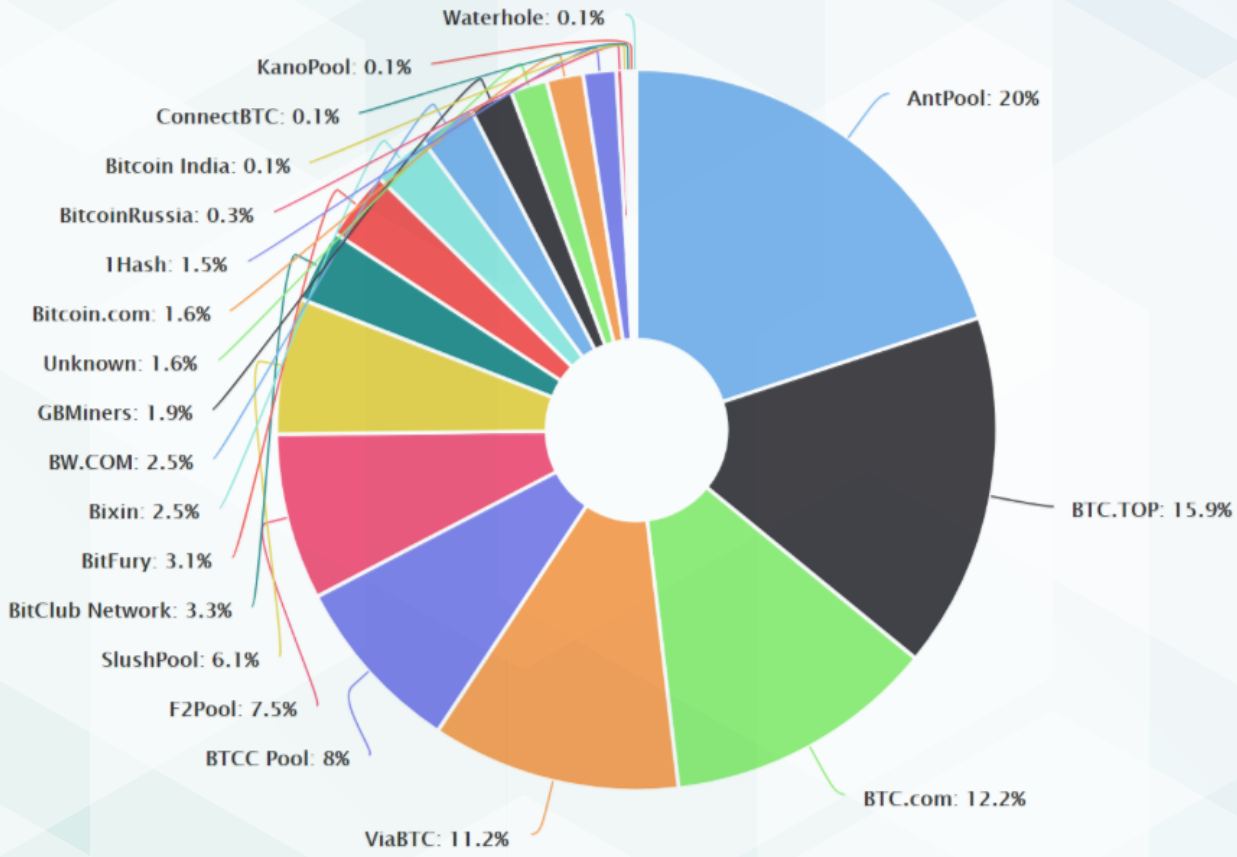


Producing 1 TWh of electrical energy emits 592.500 metric tons of CO2. So the total CO2 Emissions from BTC and ETH mining are to the tune of 17 million metric tons of CO2. This is the equivalent of the yearly carbon emission from 3.530.000 cars, or all of the cars of Austria and Switzerland combined. This clearly calls for action. bitcoinClean ensures that miners use renewable energy. A proof-of-greenness protocol uses peer to peer review of renewable energy use in a decentralised fashion, that has no need for certification authorities.

[4] http://large.stanford.edu/courses/2014/ph240/aljama2/docs/bpreview.pdf
[5] https://carbonfund.org/how-we-calculate/
[6] https://www.epa.gov/greenvehicles/greenhouse-gas-emissions-typical-passenger-vehicle-0

Mining power distribution

Bitcoin mining distribution is very centralised at the time of this writing.



While some of those pools allow their users to vote on decisions as they wish, not all do. This creates tremendous power in the hands of very few. We hope that the push to use green energy will at least redistribute some of that power to the hands of new entrepreneurs that use smaller, greener power sources like small hydroelectric power plants.

Bitcoin hard fork, block number #518,800

bitcoinClean wants to have the same widespread distribution and acceptance as Bitcoin. This is why we choose to hard fork the Bitcoin blockchain. Our block of reference will be number 517,799, which will arrive sometime on the 17th of April, 2018.

Hard forking Bitcoin means that every owner of Bitcoin at block #517,799 will have the same amount of bitcoinClean at our "first" block #518,800. These are controlled by the same private keys. To help users mitigate the risk of phishing attacks and compromising their Bitcoin holdings we will develop detailed guidelines and videos. bitcoinClean will offer replay protection by modifying the transaction structure. This means that Bitcoin(and Bitcoin Cash, Gold, Diamond) transactions will be rejected on the bitcoinClean network and vice versa.

bitcoinClean will use the hard fork to introduce 8MB blocksize. Bitcoin faces disastrous transaction bottlenecks, with transactions costing double digit USD amounts and taking multiple days.

[7] https://blockchain.info/de/pools

Mining with renewable energy sources

As we have seen, vast quantities of CO2 are produced as the electricity needed for mining is produced. 87% of fuels used here are fossil fuels. This leaves much to be desired but opens up vast space for improval. bitcoinClean wants to be the first cryptocoin that is mined with renewable energy only.
The challenge: How can the network verify that its miners run on renewable energy? To this end we devised a peer to peer verification system that will ensure a maximum of accuracy for control and a big social incentive for miners to come clean. We called this protocol Proof-of-Greenness or PoG.

How PoG works in detail

Each bitcoinClean address has two score associated, **Rank** and **Impact.** A block submitted is only valid if the submitting miner has a **Rank above 100.** Each miner starts with a Rank of 0.

To increase their Rank, miners publish documents and pictures that prove they use clean energy sources for mining. To this end they can publish utility bills from a green energy supplier, or documentation of owning a hydroelectric power generator or power station, or operate a biogas plant, in short any means of renewable energy production or consumption.
They can publish this proof on a service of their choosing. This could be a mega.nz link or a Google Drive folder, or a private FTP server or a dedicated web service like GrennMiners.com.

The important point here is that the documents are accessible by at least every other certified green miner. Only miners with Rank above 100 can upvote or downvote these claims to greenness, after reviewing the documentation submitted. Every miner can vote only once on each miner he wishes to vote on with the same decision.If he upvoted he can only vote again to downvote, and vice versa.
Each confirmation increases the Rank. Each denial decreases the Rank.

So how much does an upvote increase the Rank?

At first we opted for a very straightforward solution with fixed amounts. It soon became apparent that this could lead to widespread abuse of the system as friends would just confirm each other regardless of true greenness, or upvotes would be sold.
Instead we devised a ranking system that allows prolific users to gain impact on the network and probably even charge for scrutinizing other miners.

The Rank of each miner is calculated this way

$$Rank = \sum_{1}^{n} \frac{Upvote \times Impact}{1.000088^{ageInBlocks}} - \sum_{1}^{m} \frac{Downvote \times Impact}{1.000088^{ageInBlocks}}$$

Where n is the number of upvotes received and m is the number of downvotes received.
The votes age by 0,0088% per block. A one year old vote is only counted as 20% of a newer vote. This way miners are incentivised to keep their profiles up to date and remain transparent about what they do.

Each address has an associated **Impact** score.

$$5 * tanh\left(\left(\sum_{1}^{p} voteconfirmation \times confirmationlevel \right) - \sum_{1}^{q} voterefutal \times rebuttallevel \right) \div 128)$$

Where p is the total number of times a miner's vote -on another miner's greenness - has been confirmed and q the total number of times a miner's vote has been rebutted by other miners.

Impact is the factor that determines the weight of a vote in the Rank calculation above. It starts out with 0. This means the first vote a miner casts has no effect. Only after other miners confirm his decisions his weight increases gradually towards a limit of 5. That means a very experienced voter with a great track record can vote with a lot more impact than a relatively new voter.

The confirmation-or refutallevel signifies the amount of confirmations the initial vote received.
This level is also fed into a hyperbolic tangens function.

$$\text{So } confirmationlevel \text{ or } rebuttallevel = 1 + 2 * tanh \sum_{1}^{r} votes\,.$$

Where r is the total number of same minded votes and each vote counts as 1. The first confirmation counts as 1, the second a bit more and so on until each additional confirmation has a **confirmationlevel** (or rebuttallevel) of nearly 3.

When a vote get's rebutted by other miners, a miners Impact decreases, and decreases more with each succinct rebuttal. If a miner gets rebutted often enough, by voting randomly or trolling, his impact trends towards zero, making his votes ineffective.

Only confirmations or rebuttals in the last 50,000 blocks or counted towards the confirmationlevel.

Who can vote Only addresses whose Rank is above 100 can vote. This means that once a miner's address is confirmed clean, he or she can then start to vote on other miner's claim to greenness, as long as her Rank stays above 100. Impact is just used to calculate how much one vote counts. It does not consitute any proof of greenness and does not qualify an address for voting.

A word about proofs submitted Users are free to submit anything they think proves beyond doubt their actual use of renewable energy. It is the responsibility of the potential miner to convince his peers that he is genuine.
We'll give some starting points here. Renewable energy is either bought by a specific provider like Verbund AG in Austria or Grünwelt Energie in Germany. Or it's produced by miners who own or operate a power plant. These power plants can operate on a variety of technologies like hydroelectric power, biogas burners, wind power, solar panels, tidal power generators, and many more options.

The potential miner should then collect pictures of documents that prove his purchase of renewable energy or pictures of the power plant and data of it's power production.
It can then add other information to link that document to her. An IP address, a geo-tag, a picture, a scan of an ID. Anything that paints a credible picture.
The information should only be made visible to other miners, to ensure a maximum of privacy for this sensitive information. Miners can see other miners on the bitcoinClean network and chat with them.

Verifiers and Auditors Since confirming or denying pay we expect that some users will operate a small miner and concentrate on auditing other miners.

This could lead to the formation of specialized companies with very high Impact that can certify miners in return for a fee.

Pool mining Since most miners do not solo mine, but are part of larger mining pools, the actual entity that will submit a block is a pool, not a single miner. Since pools create their own, and competing, protocols for work share submission, they have to ensure that their miners are green. This is not regulated by the bitcoinClean protocol. But mining pools are subject to the same peer to peer confirmation rules like any other miner, so could be disallowed to submit blocks by sufficient denials of plausibility.

We can imagine two scenarios that are not mutually exclusive:
1. Every single miner verifies himself, and the uses his confirmation privileges to confirm the pools greenness.
2. The pool demands proof from it's users and then publishes this proof in order to pass confirmation.

The actual dynamics of this peer to peer review will be very interesting to see unfold. We can think of many scenarios where users intimidate, haras, band together, fake or otherwise game the system. The real world seems to be like that, and proof of clean energy in household power suppliers is often slippery and hardly transparent. We believe the protocol outlined here offers an improvement by empowering more people to ve-

rify, deny or audit others. It is more democratic and more inclusive, and more in line with the spirit of openness and transparency that Nakamoto must have had in mind when designing Bitcoin.

Technical implementation of proof-of-greenness

Proof of Greenness is implemented as a set of patches against bitcoin v0.15.
Miners with non-whitelisted (i.e. not enough Rank) addresses are not prevented from mining blocks but cannot submit valid blocks, as Rank above 60 is a criterion for valid block submission.

The intention is to ensure that all miners exclusively use renewable energy. It is up to the participants to govern what exactly that means, and how it is proven. The software strictly provides a means of enforcement.

The implementation contains a specialized client and several patches. Bitcoin is considered upstream, which means that new features and fixes to Bitcoin, like SegWit2X, are to be regularly applied unless there is a really good reason not to.

Functionality

A Impact and a Rank is associated with addresses, and a white-listed address possesses a Rank above 60.

Null-data transactions are an informal standard for an unspendable data-only transactions in the Bitcoin blockchain.

A trusted address A1 may issue null-data transaction containing an ASCII char array representing a verb followed by another address A2, which is called a vote.

If the verb is TRUST, it the vote is taken as an indication that A2 has proven compliance to the mutual set of agreements to the satisfaction of A1, and A2's Impact increases.

If the verb is BAN, the vote is taken as an indication that A2 has been proven not to be compliant, and A2's Impact decreases. If A1 does not know either way, A1 does not vote at all.

Mechanism

Vote client A vote client is a separate program that allows the convenient submission of a vote transaction to a running bitcoin core daemon, the main software, using raw bitcoin transaction API calls.

Wallet patch The wallet patch is a modification to the bitcoin daemon wallet's block verification code, adding a scan for vote transactions with six or more confirmations, and caching those votes to a binary file in the bitcoin data directory.

Trust calculation patch The trust calculation patch scans the vote file on daemon startup and after block verification in order to maintain the Impact for each address that was voted on.

Trust enforcement patch Every time a mining reward is entered into the system, the receiving addresses Impact is check for sufficiency. If the Impact is insufficient, the reward is set to zero.

Vote enforcement patch Every time a vote is issued, the sending addresses Impact is checked for sufficiency. If the Impact is insufficient, the vote is not permitted to enter the memory pool.

Security If a vote transaction or a mining reward is entered into the memory pool by a rogue client, it is rejected as invalid and never confirmed by the other clients. This is the same security mechanism that bitcoin

uses to achieve consensus for its transactions- the modifications only make the rules slightly more dynamic, but nothing inherently new is introduced. This guarantees the same standard of security for trust that is used for Bitcoin's transactions.

Why not Proof-of-Stake?

Proof-of-Stake is said to address the issue of mining energy usage while at the same time increasing security for the network.

Ethereum is planning to switch to Proof-of-Stake mining in the future. This was repeatedly announced by the Ethereum consortium and repeatedly delayed. It will then join currencies like Peercoin, Decred and Nxt that already implement either a pure Proof-of-Stake protocol or use a hybrid approach.

The main difference between Proof-of-Work (PoW) and Proof-of-Stake (PoS) mining is: in PoS, only nodes that already hold coins are eligible to be selected to mine a new block. The difficulty necessary for PoW mining is drastically reduced, so that energy usage is radically lowered, compared to PoW.
The rewards are decreased accordingly as well.

PoS uses a hashing function to link some previous blocks with the currently mined, or forged as it is then called, block, which is then signed with a miner's private key. The new block has no special requirements on its hash, so is very easy to compute. This is meant to save energy. At the same time fever coins need to paid out for this task, because it's cheap to do, so the monetary supply doesn't need to increase by fixed amounts every few minutes.

We believe that PoS mining is risky for the following reasons:
PoS creates a powerful incentive for Nodes to vote on both ends of a fork. This is called the zero-stake-problem. In mining this would mean double the effort, hence half the profit. The miner is sure to lose 50% on the blockchain that didn't make the cut.

In PoS this becomes a highly complex problem. The main logical conundrum inherent in PoS is related to Gödels incompleteness theorem. Gödel elegantly showed at the beginning of the 20th century that no system is able to prove completeness from within itself.

In PoS this means that Nodes can fork to achieve double-spending, then vote on the "correct" and "forged" chain at the same time.

Ethereum's Casper protocol addresses that by penalizing the forged chain, basically taking away the coins there. But, what if the Node then just forks away the penalty - and so on. This can only be relieved by a third party, meaning a social consensus must then decide which chain is right. But this would mean a central authority exists, even it would be more or less democratic at that point. Bitcoin votes showed that only about 6% of users participated. That's hardly a representative majority.

The second criticism focuses on the incentives of PoS. PoS incentivizes Nodes to hold coins. It would also incentivize a whole industry that would lend coins to Nodes to be used in specific votes, in return for an interest payment. PoW generates coins for miners. These coins were already incentivized to be held, since the underlying currencies were often highly volatile and a price increase likely. But currencies become vital through commerce and spending. This problem becomes greatly aggravated through PoS, where Nodes are essentially paid to simply sit on their coins.

But the main argument is complexity. PoW is a very simple, democratic and elegant solution to block verification and blockchain maintenance. PoS is incredibly hard to get right. The ongoing delay in Ethereum's switch to PoS, plus the inability of its founding board to reach unanimous support of a single technology can and should be viewed as precursors to larger problems that are bound to surface once a PoS protocol is rolled out. We therefore conclude that PoS is a good idea, but very hard to implement, with large, often unaddressed inherent risks. This means that it will take a very long time to get right, and until then will find no widespread acceptance.

[8] https://www.coindesk.com/ethereums-big-switch-the-new-roadmap-to-proof-of-stake/
[9] https://docs.decred.org//

Conclusion

bitcoinClean is a Bitcoin clone in every aspect of the protocol, like the ingenious way Nakamoto designed to thwart double spending, or the incredible addition of UTXO transactions for smaller clients, remain the same. We encourage readers of this Whitepaper to become active in the community by reading the original Bitcoin Whitepaper, by participating in forums or simply by mining bitcoinClean.

Bitcoin users can participate after the hard fork by using their bitcoinClean, by mining and by promoting clean energy usage for mining among their peers.

Premining and use of premined coins

The initiators of bitcoinClean will premine 500.000 coins. In order not to introduce additional scarcity we will raise the limit of mineable bitcoinClean to 21,500,000.

We understand that this is a controversial issue and we do not want or try to hide the fact.
We believe there is no moral conflict in creating a useful new currency that creates value for all bitcoin holders (and hodlers) as well as for the team and the future promotion of bitcoinClean.
Bitcoin's famed originator Satoshi Nakamoto mined more than a million Bitcoins initially. He has so far not touched a single one of those that are clearly attributed to him. But he could, and in our view this would be justfied.

In order to provide transparency we will disclose the according wallets used and provide insight into the expenses.
Currently we plan to distribute the coins as follows:
250.000 coins will be kept used to promote and develop bitcoinClean in the future. While these funds are controlled by the bitcoinClean development team, we will publish the address so expenses can be verified.
100.000 coins will be used in the launch of bitcoinClean for endorsements, advertising and marketing.
50.000 coins will be used to promote bitcoinclean for listings on exchanges and including it in wallets.
30.000 coins will be used to pay the developers.
70.000 coins will be distributed to the founders and initiators

The coins will be transfered from the CoinBase to addresses controlled by the founders within the first block after the hard fork. This can be later be verified with any Blockchain Explorer. We plan to use a significant portion of these funds to promote the currency and make sure the clean energy revolution acquires enough steam to make a lasting change to the way that cryptocurrencies are mined.

bitcoinClean starts the clean energy revolution in cryptocurrencies.

[10] https://en.wikipedia.org/wiki/G%C3%B6del%27s_incompleteness_theorems/
[11] https://www.coindesk.com/ethereum-casper-proof-stake-rewrite-rules-blockchain/
[12] https://bitcoin.org/bitcoin.pdf

References

1. https://motherboard.vice.com/en_us/article/ywbbpm/bitcoin-mining-electricity-consumption-ethereum-energy-climate-change
2. https://en.wikipedia.org/wiki/Bitcoin_scalability_problem
3. https://digiconomist.net/bitcoin-energy-consumption
4. http://large.stanford.edu/courses/2014/ph240/aljama2/docs/bpreview.pdf
5. https://carbonfund.org/how-we-calculate/
6. https://www.epa.gov/greenvehicles/greenhouse-gas-emissions-typical-passenger-vehicle-0
7. https://blockchain.info/de/pools
8. https://www.coindesk.com/ethereums-big-switch-the-new-roadmap-to-proof-of-stake/
9. https://docs.decred.org/
10. https://en.wikipedia.org/wiki/G%C3%B6del%27s_incompleteness_theorems
11. https://www.coindesk.com/ethereum-casper-proof-stake-rewrite-rules-blockchain/
12. https://bitcoin.org/bitcoin.pdf

bitcoinClean