Bitcoin Low-Carbon: A Peer-to-Peer Electronic Cash System

which is Ethical and Ecologically Sustainable

satoshin@bitcoinlc.org

www.bitcoinlc.org

Abstract.

On October 31, 2008 a landmark white paper was published under the pseudonym "Satoshi Nakamoto" entitled "Bitcoin: A Peer-to-Peer Electronic Cash System" and introduced the world to Bitcoin. This paper addresses some of the unforeseeable and unintended negative consequences of the massive growth in Bitcoin since its inception. This includes the inexorably high consumption carbon-based electricity to fuel mining activities as well as the high level of concentration and control of Bitcoin mining including within regimes of questionable human rights records. In this white paper we introduce the concept of 'Bitcoin Low-Carbon' or Bitcoin LC, which provides an ecologically friendlier and more ethical version of Bitcoin Core while retaining all of its security, privacy and an immutable distributed ledger. Ultimately this is the same bitcoin with only a few additional consensus rules in order to allow users to identify bitcoin mined only from renewable energy sources.

In order to accomplish this, Bitcoin LC mandates that Bitcoin's Proof-of-Work (PoW) includes simple information certifying the use of renewable energy-sourced mining where new blocks submitted can only be accepted from miners holding a low carbon emission digital certificate issued by an independent Bitcoin Low-Carbon Foundation.

Such an organization would be open, transparent and its sole function would be to provide simple, compliance verification and issuance of the digital certificate.

Bitcoin LC requires three additional consensus rules related to the insertion of the digital certificate and which are described in this paper. Bitcoin LC operates on the same network parameters as the current version of *Bitcoin Core* and remains a dedicated peer-to-peer electronic cash system permitting online payments transacted directly between individuals without going through any third party. Bitcoin LC also continues to provide the same digital signature and security through a consensus-based distributed ledger with a timestamp as part of the process, while significantly decreasing the risk of a coordinated attack from the ever-increasing concentration of hashing power even as the Bitcoin Low-Carbon network expands.

The solution to the double-spending problem as described by Satoshi in the original version of the white paper, used a peer-to-peer network with consensus-based PoW as the mechanism to avoid the double-spend. However in the case of Bitcoin LC, this process is significantly enhanced by leveraging one network with another as will be described in more detail.

While new chains historically have suffered from a lack of hashing power and would require hundreds of confirmations to ensure the integrity of the chain, Bitcoin LC avoids this problem by

creating a significantly improved network which uses the block header of the current *Bitcoin Core* as an integral part of Bitcoin LC blocks.

The network timestamps combined with the *Bitcoin Core* block header form a double record resulting in a massive proof-of-work. Together they will provide evidence of the greatest amount of hashing power of the genuine chain. Therefore, the possibility that a group of miners holding a majority of the hash power could attack Bitcoin LC is practically impossible to do so.

Bitcoin LC will also have a much greater resistance from any future attacker using quantum computers and make it impossible for it to be outpaced as each new block on the Bitcoin LC chain will contain the hash of the *Bitcoin Core* blockchain as well as the digital certificate held by network nodes for mining. This also guarantees the digital certificate for low carbon emission electricity remains intact.

The entire network topology will remain the same and would continue to broadcast messages to the other network nodes using the same TCP/IP ports on a best-efforts basis while permitting nodes to come and go, and while continuing to accept the longest PoW from the Bitcoin LC chain. At the time of implementation, the *Bitcoin Core* chain will fork, and Bitcoin LC will live on the exact same network and with few additional consensuses rule set.

We believe that over time, as market forces demand greener and more sustainable blockchain operations, bitcoin users will have a powerful incentive to move away from non-renewable energy sources and furthermore that hashing power will progressively migrate from the *Bitcoin Core* to Bitcoin LC.

Introduction

The original Bitcoin white paper was released on October 31, 2008. While most people who were aware of the paper considered it an intellectual curiosity for the most part, few could predict that just a few years later, the underlying technology would become one of the greatest digital innovations of recent financial times.

The concept of "proof-of-work" to verify transactions as used by the Bitcoin network was the underlying method which gave birth to a new generation monetary systems and decentralized finances. No doubt this likely became bigger and more important than its creator had ever anticipated.

As with many remarkable inventions or innovations, there are often unintended negative consequences. In the case of Bitcoin, this is primarily related to the network's growth in energy consumption and related contribution to greenhouse gasses since PoW is, by its very design, highly energy consuming.

Back in 2008, the Bitcoin energy concept was likely quite simple; to utilize idle CPU power from personal computers to run the network with minimal incremental energy draw. However, as "miners" began to appreciate the potential profitability of the process, so too began the process of developing more powerful mining systems, and with the adoption of Application Specific Integrated Circuit (ASIC) technology for mining, the network truly began to grow – and so did power consumption.

As of April 2021, it is estimated that the Bitcoin network had an annualized consumption of some 98 terawatt-hours of electricity per year – or the equivalent of countries like the Netherlands[1]. The network also had an annualized carbon footprint of 46.5 metric tonnes of CO^2 (equivalent to that of Finland). Granted, mining processors are becoming more efficient, but much of that efficiency is offset by the increase in network difficulty and growth in number of miners overall (a large proportion being powered by coal-sourced electricity). However, the overall energy consumption is not as critical to the environment as the source of energy is. As of 2021, most of the mining facilities are still located in China (estimates as high as 70-75%), which rely heavily on coal-based power either directly, or through load balancing[2].

Sustainability and the establishment of a basic ethical framework for the Bitcoin network is truly becoming an issue of concern and while Bitcoin has become exceedingly popular and more mainstream, the majority of financial institutions are still reluctant to invest due to concerns over environmental, sustainability and governance (ESG) concerns[3].Yet the power and value of blockchain technology is undeniable, and there is little chance that blockchain's energy consumption will decrease in the short or medium term.

Over the years, there has been a fair amount written on how blockchain technology can be used as a catalyst for climate action rather than as a contributor to climate change. This includes promoting blockchain as an incentive point for green technology – the belief is that miners are easily interruptible energy consumers and as such can take up non-peak demand from green energy sources like wind and solar, thereby creating the economies of scale needed to make these green energy sources economically viable. Other justifications focus on blockchain's ability to support "green finance" and other green transactions.

However, while these are interesting and valid arguments, they are essentially based on an approach of carbon offsets rather than carbon substitution as they do not address the underlying issue of electricity from carbon-fueled sources which powers a large proportion of Bitcoin mining. There is no incentive to move away from carbon-based mining nor is there any way to identify bitcoin mined with carbon-based power versus renewable energy. As such, under these initiatives alone, there would not likely be a decrease in Bitcoin's overall carbon footprint.

So the problem remains of how to deal with these ESG concerns in an inherently conservative ideology (the concept of a safe, secure, private, decentralized and distributed system) when dealing with what is essentially a non-differentiated commodity, as well as provide users of bitcoin the ability to truly choose a greener option.

For solutions we can look at what has been accomplished in other industries under similar circumstances and equally difficult conditions and use these lessons learned for the Bitcoin network.

As an example, in the 1980's the world markets were made aware of what came to be known as "blood diamonds" or "conflict diamonds" – diamonds originating from conflict regions of the world, proceeds of which were used to finance conflict situations. As diamonds (particularly rough diamonds) are a generally undifferentiated commodity, it was difficult to separate such diamonds from diamonds of legitimate origin.

[1] Source: Digiconomist

[2] *ibid*

[3] https://www.coindesk.com/the-myths-and-realities-of-green-bitcoin

The eventual decline of conflict diamonds occurred primarily because;

1) Awareness of conflict diamonds made them undesirable (i.e., market forces)
2) Laws made them illegal to purchase/sell which was internationally monitored
3) A basic certification process put into place intended on reducing circulation of blood diamonds (the Kimberley Process) coupled with technology to trace origin of diamonds (e.g., X-ray diffraction "fingerprinting" of the product)

Although the approach was flawed on many levels (e.g., hard to enforce), the approach of combining moral principles and establishment of legal foundations for the industry along with methods of compliance of monitoring through technology was sound, and can be applied to some extent to a greener and more ethical Bitcoin network.

Bitcoin is developing a negative reputation in the eyes of the public for being environmentally non-sustainable. The market is demanding greener blockchain operations. Bitcoin Low-Carbon will provide digital proof that the coin was produced within a consensus-based sustainable framework.

Bitcoin Low-Carbon will be the same bitcoin, but minted on an environmentally sustainable chain.

We believe that only small changes need to be implemented to the current Bitcoin chain to achieve this goal. Under the proposed system, the current *Bitcoin Core* chain would remain an integral part of the Bitcoin low-carbon chain. We would expect this would result in fewer miners using carbon-based energy, along with a move to greener, certificate-based miners migrating to Bitcoin Low-Carbon over time.

The Value of Bitcoin

Bitcoin has proven over the past decade that it is both a mechanism of commerce on the Internet, allowing users to rely less on traditional financial institutions, as well as a store of value for bitcoin holders. Both of these functions are only expected to grow over time.

Bitcoin is the peer-to-peer cash system its inventor envisioned in the original white paper; a financial transaction system used by millions of users everyday eliminating the need of a third party by effectively permitting non-reversible transactions. With traditional transactions, even if a third party can be trusted, too often one or more of the transactional parties may not have complete control over it, as in the case where a transactional-intermediary block or freezes a transaction.

Dealing with the Unforeseeable Problem

This paper deals with a problem that Satoshi could never have reasonably foreseen; the current and staggering increase in the use of carbon-sourced electricity for mining, particularly in certain regions of the world, often coupled with the high concentration of hashing power in these same regions resulting in an environmentally unsustainable situation, potentially threatening the independence of the network through centralization.

Furthermore, as concentration within the network continues to rise and with the inevitable use of quantum computers in a near future, additional safeguards need to be implemented to prevent double spending attacks on the Bitcoin network or perhaps some disruption of the network. *Bitcoin Core* could face such a problem if honest nodes no longer collectively control the majority of hashing power.

In order to address these problems Bitcoin LC includes these simple three OP_RETURN values in each miner's new proposed blocks coinbase transaction:

x the corresponding *Bitcoin Core* legacy block hash
y a renewable mining certificate with extended signature of miner's Bitcoin LC coinbase address with the expiration timestamps
z root certificate signature of the bitcoinlc.org foundation with expiration timestamps

Miners are required to signed their coinbase address using the certificate obtained by an independent organization, the Bitcoin Low-Carbon Foundation.

Certificates would only be issued to nodes/miners which meet a verifiable sustainable standard that is based solely on confirmation that the mining operation is powered solely with renewable energy. Regarding the potential issues of concentration and double-spend attacks, this is dealt with by having the distributed timestamp of the improved decentralized network node use the proof-of-work contained in the *Bitcoin Core* block headers within the Bitcoin LC coinbase OP_RETURN.

Standards would no doubt evolve over time, reflecting the demands of the market.

Bitcoin Low-Carbon Improved Chain

Bitcoin LC will continue using the identical transactional system as in the *Bitcoin Core*; both as a chain of digital signatures and as it has evolved to the Segregated Witness upgrade activated at block 477,120 on July 21, 2017, in the software upgrade referred to as Bitcoin Improvement Proposal (BIP) 91.

As with the *Bitcoin Core*, an existing Bitcoin address holder can transfer coins to another address by signing a transaction using its private key in favor of the recipient public key hash based on the Elliptic Curve Digital Signature Algorithm (Secp256k1).

The payee will continue to verify the signatures to evidence chain of custody.

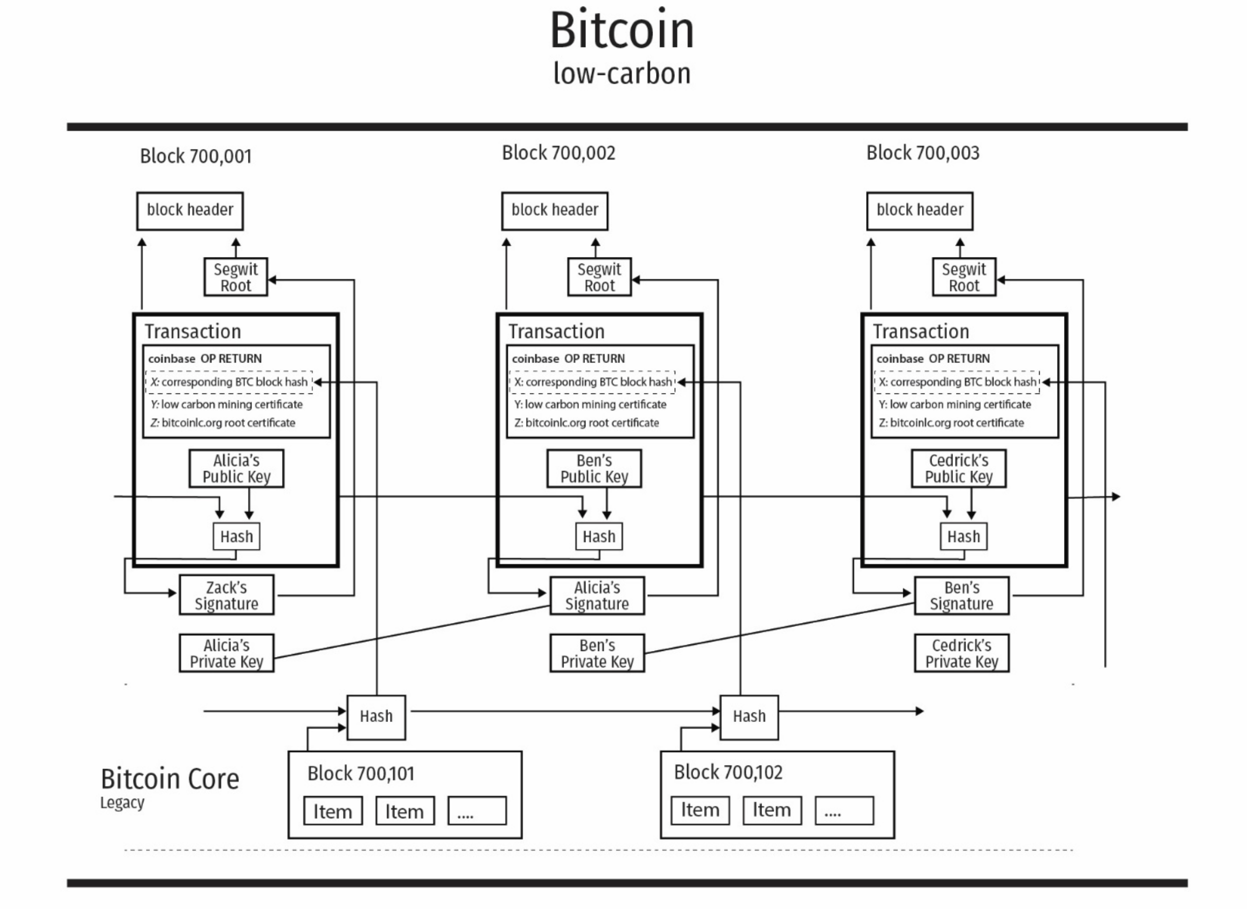
Also, as with the *Bitcoin Core*, the payee must be able to verify that one of the previous coin owners did not double-spend the coin, and so the payee will continue to need to rely on the distributed PoW and in this respect, Bitcoin LC has a significant advantage over the existing *Bitcoin Core* chain.

Bitcoin LC will use *Bitcoin Core* blocks headers in each block minted into the Bitcoin LC chain. As such, the probability of allowing a double-spend attack is reduced to virtually zero. Furthermore, the integrity of the Bitcoin LC timestamp is doubly locked down by using the *Bitcoin Core* block headers in Bitcoin LC blocks.

Therefore, Bitcoin LC is highly distributed upon inception (at the moment of the fork) as it immediately forces *Bitcoin Core* block headers into the protocol.

Agreement on which transaction comes first occurs at every few blocks or so which makes it unlikely to impossible for the majority of the nodes to disagree on the order of transactions. Currently the existing *Bitcoin Core* chain is vulnerable under circumstances whereby a concentration of dishonest hash power tries to take significant advantage in proposing a longest chain and proof-of-work. Bitcoin LC protects against this in that the next mining block can only be undertaken by using the corresponding *Bitcoin Core* block header and where timing is subject to normal statistical fluctuations of blocks time creation of both chains. This permits every node on the network to evaluate the valid transactions and reach consensus with the longest chain almost in real-time, without slowing overall transactions.

The following diagram details the parallel *Bitcoin Core* and Bitcoin Low Carbon chains



Bitcoin Core Timestamp Server Concept

The original Bitcoin white paper suggested perhaps "tongue in cheek" that a widely published newspaper could serve as a timestamp mechanism, but that it would at the same time be very impractical.

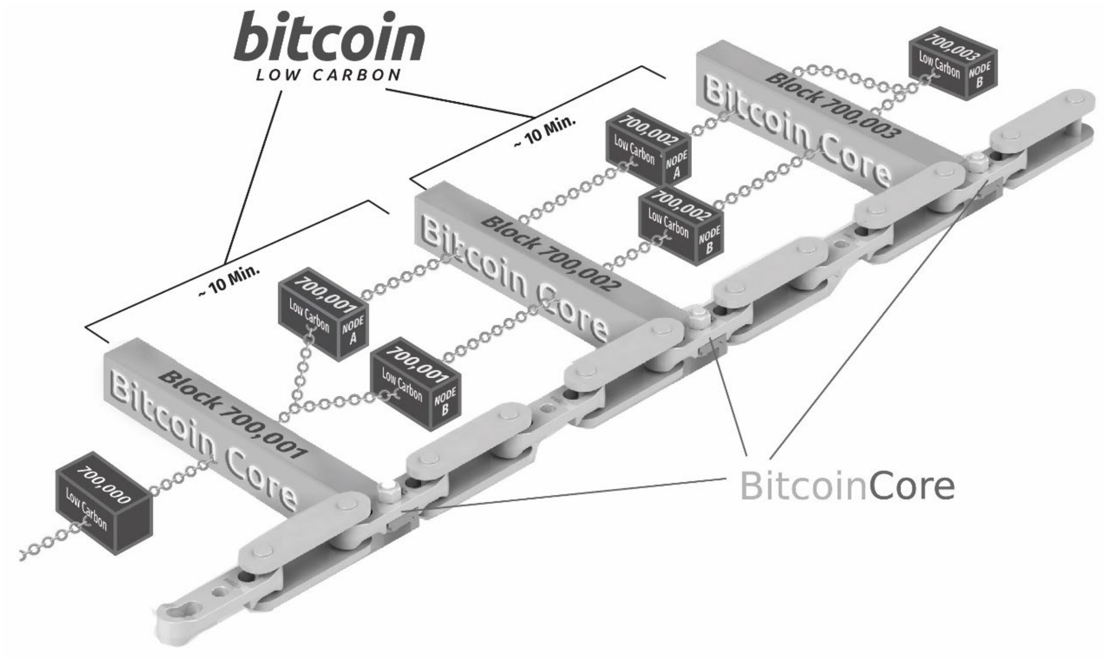
Through the implementation of Bitcoin LC, along with the integration of the *Bitcoin Core* block headers hash to each new block, this will have the double effect of integrating a widely published Bitcoin "newspaper" timestamp every 10 minutes or so, i.e., the *Bitcoin Core* block headers in addition to the Unix time into the Bitcoin LC blocks.

Under a scenario where if, for any reason, an extreme concentration of hash power is assembled and mobilized, including a possible digital cryptocurrency world war, even a sequential timestamp blockchain hash can be redone several blocks back if necessary.

Contrary to various *Bitcoin Core*-type side chains such as *RSK*[4], smartcontract-based solutions or even merged mining projects like *Namecoin*[5] which rely on aleatory OP_RETURNS insertions into the main chain, Bitcoin Low-Carbon works the other way around. It inserts *Bitcoin Core* block hashes into each coinbase transaction OP_RETURN.

Bitcoin Low-Carbon and the Improved Proof-of-Work

The nonces trial-and-error proof-of-work method will remain the same; seeking a value that would produce a certain amount of zero bits after being hashed by still using the SHA-256 cryptographic protocol in front of the next block hash while network difficulty adjustments will obviously be set independently from that of *Bitcoin Core*. The combined effect of dual hash difficulty will make it practically impossible to alter the chain even through the use of quantum computers and/or some extreme concentration of the hash power as it would require simultaneous alteration of both *Bitcoin Core* and Bitcoin LC.



Each *Bitcoin Core* block acts as a bulkhead partition wall, protecting Bitcoin Low Carbon blocks

As originally expressed by Satoshi, a one Internet IP-based address for one vote system could be easily subverted by groups that would be able to allocate many IPs to the network. Satoshi provided the

[4] https://www.rsk.co/

[5] https://en.wikipedia.org/wiki/Namecoin

cryptographic innovation of proof-of-work to be essentially; one ASIC to represent one vote. However, with the very clever introduction of the concept of pooling ASIC-based computers, Satoshi's fears of concentrated power and resources have become apparent, as evidenced by concentration of hash power in certain areas of the world or by certain groups.

As such, transactions contained in the *Bitcoin Core* blocks and their resulting hash will permit nodes and miners of the Bitcoin LC chain to assure that the integrity of each block as it is being backed by a *Bitcoin Core* block with a valid timestamp. Furthermore, each Bitcoin LC block must contain an authentic certificate issued to miners by the not-for-profit Bitcoin Low-Carbon Foundation which maintains standards of ethics and sustainability. The result is one of security and the assurance that the coin minted can be specifically identified as meeting those standards.

As miners and nodes would be expected to progressively migrate some hash power from the *Bitcoin Core* chain to the Bitcoin LC chain over time, network difficultly will be adjusted accordingly while maintaining both chains in the best possible ethical and environmentally sustainable conditions moving forward. Consequentially, the Bitcoin LC will automatically adjust its proof-of-work difficulty as with the *Bitcoin Core* chain to maintain a block generated every 10 minutes or so while naturally maintaining synchronisation with *Bitcoin Core.*

Bitcoin LC Network

Steps on the improved network will be the same as for the existing network except for three additions as identified below:

Step	Description	Existing or New
1)	New transactions are broadcasted to all nodes.	Existing
2)	Each node collects the new Bitcoin LC transactions into a block.	Existing
3)	Each node inserts in its coinbase transaction OP_RETURN:	Existing
	- the corresponding *Bitcoin Core* legacy block hash (*Bitcoin Core* block x + 100);	**New**
	- a renewable energy mining certificate and;	**New**
	- the root certificate of the *Bitcoin Low Carbon Foundation*	**New**
5)	Each node works on finding the proof-of-work for its block.	Existing
6)	When a node finds a proof-of-work, it broadcasts the block to all nodes.	Existing
7)	Nodes accept the block only if all transactions in it are valid, not already spent, and they contain the *Bitcoin Core* sequential block hash with miner coinbase address with its digital signature authenticated by a public key traceable back to the Bitcoin Low Carbon Foundation trusted root.	Existing
8)	Nodes express their acceptance of the block by working on creating the next block using the hash of the accepted block as the previous hash.	Existing

Nodes will continue to consider the longest chain to be the correct one and will keep working on extending Bitcoin LC chain.

Since Bitcoin LC relies on the *Bitcoin Core's* block hash, it would be near impossible to have long distinctive branches as double-spend transactions would be detected by the other nodes while waiting for the *Bitcoin Core* correspondent block header. In the event that two separate branches tie, the tie would be broken in the following blocks or so as the next PoW would include the next *Bitcoin Core* block header, making all nodes switch to the longest chain immediately.

Implementation and Incentive

Implementation of the Bitcoin LC will start at the *Bitcoin Core* chain block height 700,000 and would begin mining at block 700,001 by waiting for a 100-block buffer in the *Bitcoin Core* chain. At the point of implementation, the chain will fork into a *Bitcoin Core* and Bitcoin LC. Holders of coins in *Bitcoin Core* at the time of the fork will also hold the same amount Bitcoin Low-Carbon coins.

A Bitcoin LC wallet, block explorers and mining pools will be made available. Both chains will exist concurrently, and *Bitcoin Core* block headers will be used by Bitcoin LC's PoW.

The protocol will remain exactly the same regarding coinbase rewards to the miners and maintaining the coins in circulation with the same steady addition as per the protocol already in place. Miners will also continue to have the incentive of each transaction fee while the protocol would continue maintaining the inflation balance.

Nodes and miners would not be able to propose a block without a valid digital certificate of renewable energy usage adding the incentive to stay environmentally friendly.

Reclaiming Disk Space and Block Size

The implementation of the hashed Merkle tree and the Segwit in 2017 had the effective block size increased from the original Bitcoin software node. Although, with the widespread adoption of Bitcoin as a store of value and as a peer-to-peer cash system, and since there has been an urgent shift toward greener and sustainable technology, Bitcoin LC will maintain the current block size but can be increased as need in the future.

As Satoshi pointed it out, Moore's Law continues to predict exponential storage capacity in the future, which will be more than capable of supporting and eventually increasing the Bitcoin LC block size.

Simplified Payment Verification

It is possible to verify payments without running a full Bitcoin LC node. A user only needs to keep a copy of the block headers of the longest PoW chain, which they can acquire by querying network nodes until they are convinced that they have the longest chain, by obtaining the Merkle branch linking the transaction to the block that it is timestamped in.

As with *Bitcoin Core*, users cannot check the transaction for themselves, but by linking it to a place in the chain, they can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.

Longest Proof-of-Work Chain

The longest PoW will be easy to confirm by looking for the presence of a corresponding *Bitcoin Core* block header inside Bitcoin LC blocks. Contrary to the existing *Bitcoin Core*, which operates by itself, there is no other way but to wait for a real time competing chain(s) to vanish after a certain period leaving only the one which is globally accepted.

Combining and Splitting Value

Bitcoin LC will use the same method as *Bitcoin Core* by allowing value to be split and combined, and for transactions to contain multiple inputs and outputs.

Privacy

All Bitcoin LC transactions will be announced publicly as is done currently and privacy will still be maintained by keeping public keys anonymous.

Probability of Maintaining a Fraudulent Chain

As Satoshi pointed out at the time, the probability for a coordinated group of attackers to maintain the longest chain for several blocks ahead is exceptionally low. With Bitcoin LC, the probability is even lower, approaching zero.

Conclusion

We are proposing a simple and necessary improvement of the electronic transaction system as originally envisioned by Satoshi.

Moving forward, Bitcoin LC will maintain an ethical and sustainable system of peer-to-peer networks using PoW to record a public history of transactions while improving the prevention of double-spend attacks.

Nodes and miners will be required to use renewable energy and comply with an ethical framework. Public and institutional preference for bitcoin with these verifiable attributes will promote the progressive migration away from high carbon Bitcoin Core mining operations in favor of the more sustainable Bitcoin LC.

Miners proposing a block without a valid ethical and environmental certificate would be rejected.

Some have been proposing to buy and accumulate *Bitcoin Core* coins from miners that only use renewable energy, but this is not realistic as the Merkle tree containing transaction data will continue on the chain and will continue to be minted by miners using non-renewable carbon-based sources.

By bringing *Bitcoin Core* block header hashes into Bitcoin LC blocks, the PoW is increased exponentially and prevents attackers from using increasing hash power concentration or even quantum computing to launch an attack.

Nodes will continue to be able to leave and rejoin the network at will, accepting in a simple and fast way. The proof-of-work chain as “proof of what happened” would be confirmed by highly distributed timestamp PoW.

No concentration of ASIC power could be used to attempt to subvert the network as it has in the past since the PoW would reside in doubly locked down blocks one after another.

The consensus mechanism of Bitcoin LC will be enforced through the widely distributed PoW of the *Bitcoin Core* chain thereby preventing control through the concentration of hash power.

From the point of inception, users and holders of the Bitcoin Low-Carbon digital asset will be assured of the long-term sustainability of the network.

With the safeguards of a *Bitcoin Core* chain combined with the Bitcoin LC chain, all participants in the network can expect full sovereignty of their share of the growing global new digital monetary system, along with a day-to-day cash currency transactional instrument, thereby offering true digital currency independence with no ability for any participant of group to dominate the network.