LYNX

Technical White Paper 1.0[1]

https://getlynx.io info@getlynx.io @getlynxio

Lynx is an eco-friendly cryptocurrency that discourages mining for profit.

[1] Written by Ben Wilson. This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

Please note: Lynx is an easy-to-use platform that anyone (from the Boy Scouts of America[2] to experienced application developers) can use. Our goal is to attract a broad range of collaborators who will directly benefit from our equitable and sustainable approach. *To reach the widest possible audience, Part 1 of this white paper was written for a non-technical, broad audience.*[3]

[2] Lynx can be used to meet the 'Projects' criteria for the Boy Scouts' "Programming Merit Badge." See: http://usscouts.org/mb/worksheets/Programming.pdf

[3] Throughout the paper, we've done our best to simplify advanced concepts. However, some of the ideas presented require a basic understanding of cryptocurrency and blockchain technology. For more information, please see the "References" section for additional resources.

Abstract

For cryptocurrency to be considered a secure platform for exchange in today's global marketplace, it must be created with global sustainability in mind. As an eco-friendly cryptocurrency, LYNX strives to solve this problem. LYNX is a decentralized cryptocurrency that prioritizes environmental sustainability and ease-of-use for the everyday, non-technical user. Unlike Bitcoin's business rules which promote a consolidated, competitive, inefficient, and profit-driven mining strategy that create an over-reliance on fossil fuels, LYNX business rules promote the opposite. The Lynx code discourages high-volume mining rigs because the code purposefully lacks incentives to mine it for profit. In addition, the entire LYNX network is designed to operate on a collaboration of low power devices that anyone can run, resulting in a collective global mining cost of only dollars a day.[4] This includes mining the coin and confirming transactions. As a result, LYNX is more user-friendly to mine and more eco-friendly than other cryptocurrencies that have unsustainable energy requirements. And, with the majority of coins yet to be mined, the LYNX network can be sustained for thousands of years.[5]

PART 1: NON-TECHNICAL OVERVIEW

History

Lynx is cryptocurrency from the past designed for the future because it evolved from an existing coin: Kittehcoin (MEOW).[6] Released in 2013[7] in response to the Dogecoin project[8] Kittehcoin was initially met with enthusiasm in the crypto community. However, because of a lack of continual development and deliverable solutions, the project remained dormant

[4] This calculation is based on running a 3.2 watt Raspberry PI 3 at USD $0.11/kWh (3.2w X 24h x 0.11)/1000 = $0.008448/day per single Raspberry Pi 3.

[5] This is based on the idea that ~15 billion Lynx blocks remain with a 30 second average block time which equals 7.5 billion minutes or the equivalent of ~14,259 years.

[6] "Kittehcoin." *Github*. https://github.com/kittehcoin/kittehcoin

[7] "Kittehcoin launched! Come get some MEOW now. U haz it! DOGE sad." *Bitcointalk*. December 24, 2013.

[8] Palmer, Jackson. "My Joke Cryptocurrency Hit $2 Billion and Something Is Very Wrong." Motherboard. Jan 11, 2018. https://motherboard.vice.com/en_us/article/9kng57/dogecoin-my-joke-cryptocurrency-hit-2-billion-jackson-palmer-opinion

for years. During this time, hackers identified a design flaw in the code that allowed them to increase the amount of coins released with each block they mined. (In non-technical terms, this is similar to hacking into an ATM machine to receive $20,000 on a $2,000 withdrawal.) This hack upset the fixed scarcity of the coin, immediately devalued it, and users lost confidence in the project. As a result, ongoing interest in the coin waned and it was considered dead.

In 2017, Ben Wilson, a technical application designer with over 25 years of software development experience, decided to fix the coin and revive the dormant community.[9] In fact, Kittehcoin's existing community and user-base is one of the reasons he decided to develop an existing project instead of launch a new one; why try and build a new audience from scratch when one already exists - especially when the existing audience already has an economic incentive to support the project? And, an additional criteria also factored into his decision to develop an existing coin instead of create a new one. New crypto projects and ICO's are often correctly met with skepticism because many of them are scams that don't solve any real problems. So, he decided to demonstrate his ability to solve real problems using cryptocurrency by solving a real cryptocurrency problem. With this in mind, he set out to fix the design flaw in Kittehcoin and re-brand the updated project as Lynx. To accomplish this, he successfully cloned Litecoin and ported the Kittehcoin blockchain to it. Now, LYNX has all the benefits of Litecoin with the full transaction history of Kittehcoin. This fixes the original design flaw, benefits the existing Kittehcoin holders, and implements all of the security features of Litecoin.

The Problem

Summary

Cryptocurrencies who rely solely on Proof of Work (PoW) have four primary, and related, design flaws. First, PoW encourages competitive, profit-driven mining. Second, competitive, profit-driven mining demands the use of expensive, high-powered computer processing to secure the network. Third, expensive, high-powered processing power is a barrier to entry for individuals who want to participate by mining the coin. This create a hierarchical and inequitable system based on who can afford high-powered mining rigs and the electrical costs associated with them, and as a result, few miners control the entire network. Fourth, mining farms are filled with mining rigs that consume an ever-growing and arguably unsustainable amount of electricity. Often, fossil fuels supply power used by these mining

[9] The name Lynx is an homage to Kittehcoin's loyal, cat-loving fan base and to the early text-only web browser (Lynx) Wilson used in college.

farms and the associated environmental impact is measurable in the form of climate change.

Proof of Work

Bitcoin, the first and most popular cryptocurrency, relies on Proof of Work for mining. Proof of Work is "a piece of data which is difficult, costly, and time-consuming to produce but easy for others to verify [and also a] random process with low probability so that a lot of trial and error is required."[10]

According to Investopedia:

> Bitcoin mining is the process by which transactions are verified and added to the public ledger, known as the blockchain, and also the means through which new bitcoin are released. Anyone with access to the internet and suitable hardware can participate in mining. The mining process involves compiling recent transactions into blocks and trying to solve a computationally difficult puzzle. The participant who first solves the puzzle gets to place the next block on the block chain and claim the rewards. The rewards, which incentivize mining, are both the transaction fees associated with the transactions compiled in the block as well as newly released bitcoin.[11]

Because it can be a random process with low probability that requires lots of trial and error, PoW drives global competition through hashing[12] power to win blocks.

Historically, miners (individuals) compete to win a block. This is done by acquiring a 'mining rig' (a computer with specific processing capabilities)[13] that can compete with other similar devices on the network to win a block. By selling the block reward and its associated fees, the miner can pay the cost of the hardware, software license, power and (potentially) make a profit. When Bitcoin (and other cryptocurrencies using PoW) was originally created, mining for blocks could be done on a laptop or PC, but greed fueled global competition. Now, mining rigs require the use of specialized hardware (capable of

[10] "Proof of Work." *Bitcoin Wiki.* https://en.bitcoin.it/wiki/Proof_of_work

[11] "Bitcoin Mining." *Investopedia*. https://www.investopedia.com/terms/b/bitcoin-mining.asp

[12] "Hashing power" refers to computer processing capacity and has a direct relationship to electricity consumption.

[13] For the non-technical audience, please note that "miner" can be used to explain the person who is mining and the computer that is mining. (You know, because understanding crypto isn't hard enough.) Where applicable throughout the paper, we use "miner" to explain the person and "mining rig" to explain the machine.

much higher hashing power and, along with it, increased energy consumption) to win a block. In addition, the number of mining rigs on the network increase the competition between miners to win the block and win the reward ($), but generally[14] the reward stays the same. When a new miner enters a coin eco-system to mine it for profit, the cost to generate a new block increases yet the function of the block does not change; it is still only one block. In short, Proof of Work incentivizes global competition and energy consumption. This is expensive and environmentally unsustainable for coins that use PoW as their mining algorithm. It's scalable - but not environmentally sustainable.

Sustainability

To increase the likelihood of winning a block, miners have scaled their mining rigs and operations. Today, Bitcoin mining is consolidated to a handful of large global mining farms which then send their work to mining pools. A mining farm is a computer data center focused on mining cryptocurrency, and a mining pool is a group of miners who work together to reduce unpredictability of their mining reward. Miners 'point' their hashing power to a particular pool and when the pool wins a block, each miner gets their share measured by the hashes completed by their mining rig. So, miners with more hashing power or more powerful mining rigs, earn a greater percentage of the return. This model helps miners better predict their return on investment. In order for participants in the pool to stay competitive and earn rewards, their hashing power constantly needs to increase.[15] To accomplish this, the pool members invest more money in faster and more efficient chips.[16] Over time this, unfortunately, consolidates the collective mining power of the whole network within a handful of mining pools and farms. This is risky because it can give more power to the miners than to the developers of the project.[17] It consolidates the amount of

[14] Various cryptocurrency projects have unique schedules where the mining reward changes (usually decreases) over time. For the sake of simplicity, we are glossing over that discussion in the Non-Technical Overview section.

[15] This relates to Moore's Law. As defined by Merriam Webster, it refers to "an axiom of microprocessor development usually holding that processing power doubles about every 18 months especially relative to cost or size."

[16] As we see in older larger PoW coin projects, a few mining pools end up competing with each other, ruling out the opportunity for a solo miner to possibly win a block. This isn't necessarily an issue for the miner (because they miss out on the mining reward); it is more of a security risk for the network because of the consolidated power of the pools.

[17] Several articles discuss how miners have throttled innovation in project development by not accepting and/or implementing updates published by the developers of the coin. See: Chester, Jonathan. "The Battle For Bitcoin: What You Need To Know About Bitcoin And Bitcoin Cash." November 17, 2017. *Forbes*. See also: Bustillos, Maria. "Inside the Fight Over Bitcoin's Future." *The New Yorker.* August 25, 2015. https://www.newyorker.com/business/currency/inside-the-fight-over-bitcoins-future

power to only a few individuals who control the mining pools and farms within the network and creates an imbalance within the coin's ecosystem. For cryptocurrencies driven by Proof of Work algorithms, the desire for profit drives users' participation in the network. Therefore, miners' participation isn't necessarily to support the project's long term progress, but to earn money. In a perverse application of Gresham's Law[18], this pushes out individuals who want to participate and support the project but can't afford it. For example, according to a May 2018 *Market Watch* report, the average cost to mine a single Bitcoin in the United States is approximately $4700.[19]

Scalability

This section highlights some of the recent research that addresses the scalability issue:

According to an article in the *MIT Technology Review*, "Bitcoin is Eating Quebec":

- These computers, often called "rigs," are purpose-built. Able to withstand dramatic shifts in temperature and humidity, they are singularly programmed not only to perform just one computation trillions of times each second, but to repeat those computations around the clock and without pause. They are also energy hogs: the 7,000 in Saint-Hyacinthe alone consistently draw more energy than the Montreal Canadiens' nearby hockey arena, even on a sold-out game night…. Factor in additional energy consumption required to cool the computers (they can't function in temperatures over 40°C), and Malone estimates that Bitcoin alone is consuming as much electricity as the entire nation of Ireland at any given moment. And while Bitcoin is the largest proof-of-work cryptocurrency, it's far from the only game in town: at last count, there were nearly 1,500 in operation, each with its own energy demands.[20]

[18] "Gresham's Law." *Merriam Webster.* https://www.merriam-webster.com/dictionary/Gresham's%20law

[19] Hankin, Aaron. "Here's How Much it Costs to Mine a Single Bitcoin in Your Country." Marketwatch. May 11, 2018. https://www.marketwatch.com/story/heres-how-much-it-costs-to-mine-a-single-bitcoin-in-your-country-2018-03-06

[20] Miles, Kathryn. "Bitcoin is eating Quebec." MIT Technology Review. April 11, 2018. https://www.technologyreview.com/s/610786/bitcoin-is-eating-quebec/

According to the 2017 *Wired* article, “The Hard Math Behind Bitcoin’s Global Warming Problem,” “Bitcoin emits the equivalent of 17.7 million tons of carbon dioxide every year.”[21] But that number is increasing.[22]

According to a 2018 article from *Politico* about miners taking over a small town in Washington state[23]:

- By the end of 2018, according to some estimates, miners here could account for anywhere from 15 to 30 percent of all bitcoin mining in the world, an impressive shares of other cryptocurrencies, such as Ethereum and Litecoin. And as with any boomtown, that success has created tensions. There have been disputes between miners and locals, bankruptcies and bribery attempts, lawsuits, even a kind of intensifying guerrilla warfare between local utility crews and a shadowy army of bootleg miners who set up their servers in basements and garages and max out the local electrical grids. More broadly, the region is watching uneasily as one of its biggest natural resources—a gigantic surplus of hydroelectric power—is inhaled.

According to a 2018 article from *Vox*, “electricity consumption from Bitcoin rose to a record high of 47.4 terawatt-hours… That’s roughly the energy used by all of Singapore, a country of 5.6 million people. It brings the rate of carbon dioxide emissions from Bitcoin up to 23.2 million metric tons per year. And it’s not showing any signs of slowing down.”[24]

According to a March 2018 article from *The Atlantic*:

> To keep up, bitcoin miners have had to make tremendous leaps in scale. In 2012, a bitcoin mining outfit might have measured its consumption in the kilowatts.

[21] Rogers, Adam. “The Hard Math Behind Bitcoin’s Global Warming Problem.” Wired. December 15, 2017. https://www.wired.com/story/bitcoin-global-warming/

[22] According to this chart, you can see the exponential growth of the miners consumption of electricity: https://blockchain.info/charts/hash-rate?timespan=all

[23] Roberts, Paul. “This is What Happens When Bitcoin Miners Take Over Your Town.” Politico. March/April 2018. https://www.politico.com/magazine/story/2018/03/09/bitcoin-mining-energy-prices-smalltown-feature-217230?utm_source=digg&utm_medium=email

[24] Irfan, Umair. “Bitcoin’s Price Dropped but It’s Still Devouring an Obscene Amount of Energy. *Vox.* Feb 6, 2018. https://www.vox.com/energy-and-environment/2018/1/18/16901422/bitcoin-price-crash-energy-emissions

> Now, the sites are scaling up so fast that we're talking about gigawatts, which are thousands of megawatts, which themselves are thousands of kilowatts[25]… To realize the technology's backers' visions, the electrical consumption would have to keep growing at this breakneck pace. At a time when climate change requires that energy demand be bent downward, bitcoin miners sucking up city-size supplies of cheap and carbon-free hydroelectricity is a massive problem. And in China, where most mining is done with subsidized electricity produced in coal-fired power plants, it's an even bigger problem. This externality alone could wipe out a range of the benefits that bitcoin advocates imagine could result from the use of cryptocurrencies. Let's stipulate that blockchains are useful and interesting. But will they be worth the energy it takes to do all that computation?"[26]

Unchecked, exponential scaling is unsustainable. This is the problem; Lynx has a solution.[27]

The Solution

Summary

Lynx created the Hybrid Proof of Work solution. Lynx business rules encourage the use of low-cost computing (like a Raspberry Pi which only consumes around 3 watts of electricity) to mine the coin. As a result, the electrical cost to maintain the Lynx network is a fraction of Bitcoin's, yielding a low environmental impact. The emphasis on low-cost computing also creates a more decentralized, broad miner base which strengthens the stability and security of the currency. And, the easy-to-use tools and broad miner base creates a more equitable cryptocurrency that anyone can use for generations to come. Lynx was designed to have minimal environmental impact because it's committed to creating global solutions and maintaining a small carbon footprint.

[25] Remember (as stated earlier): *the cost to generate a new block increases yet the function of the block does not change;* it is still only one block minted at a regular interval. This contributes to the global competition required to mine Proof of Work coins.

[26] Madrigal, Alexis. "Bitcoin Mining Turns Mining into Profit." *The Atlantic.* May 12, 2018. Within this quote, Madrigal also references the 2017 *Vox* article by Umair Irfan, "Bitcoin's Price Spikes is Driving an Extraordinary Surge in Energy Use."
https://www.vox.com/energy-and-environment/2017/12/2/16724786/bitcoin-mining-energy-electricity

[27] Other projects are also trying to solve this problem (like Proof of Capacity, BurstCoin, and Spacemesh), but not like Lynx. What differentiates Lynx are the three rules in the Hybrid Proof of Work.

Hybrid Proof of Work[28]

For a cryptocurrency to be considered eco-friendly[29], the electricity requirements to run the global network (including the hardware and software) must have a minimal impact on the environment.[30] To ensure environmental sustainability, Lynx developed Hybrid Proof of Work (HPoW). Lynx HPoW still uses PoW *but modifies it so it isn't profitable* and, as a result, creates an entire cryptocurrency network that can run on energy efficient, easy to set-up, low-cost computers or cloud services. This removes any barriers to entry for non-technical individuals or organizations who want to get involved with, support, and build applications on a stable and secure cryptocurrency project.

HPoW removes the profit incentive for miners because the mining reward is so low. In fact, mining farms would actually lose money if they tried to mine Lynx, meaning they will leave Lynx to the individuals who want to solve the sustainability problem. This takes control away from mining farms and pools and puts it squarely into the hands of individuals (solo miners) who want to build upon and use Lynx. HPoW supports network maintenance by incentivizing and empowering those who want to use Lynx. With every new solo miner that connects, the network becomes more secure by reducing the risks associated with a centralized and hierarchical cryptocurrency network. This security is achieved through redundancy: the more individual nodes on the network, the stronger the network becomes. If an individual node or miner fails, or if an entire region of nodes fail due to widespread power outages or war, the network is still secure because mining rigs are plentiful.

The following criteria bring stability to Lynx and maintain network integrity.

1) The low cost to maintain each mining rig in the global Lynx network.
2) The low work output of each mining rig in the global Lynx network.
3) The lilliputian impact to the global Lynx network should an individual mining rig fail.

[28] The "technological specifications" section explains the parameters and business rules for Hybrid Proof of Work.

[29] Brown, Mike. "Bitcoin's Energy Consumption is Killing the Planet but There is a Solution." *Inverse.* https://www.inverse.com/article/39138-bitcoin-energy-consumptionDecember 12, 2017.

[30] Verma, Sid. "Bitcoin's Exorbitant Energy Costs May Prove to Be Biggest Risk." *Bloomberg*. November 9, 2017.

Each mining rig only requires a low power computer (such as a Raspberry Pi) and the free Lynx Cryptocurrency Installer (LynxCI). The cost is minimal and the set-up can be accomplished by non-technical users.[31]

Non-Technical Summary

In short, Lynx business rules discourage mining for profit and this differentiates Lynx from most other cryptocurrencies currently in production. By rendering mining unprofitable, the electricity needed to mine and run the global Lynx network is minimal. Ultimately, this is an eco-friendly solution because it supports environmental sustainability. And, because of the redundancies in the network design and the enhanced coin parameters, the coin is secure.

[31] The following non-technical video contains everything you need to buy, know, and do to set up the LynxCi on a Raspberry Pi 3. Visit: https://getlynx.io/can-non-techies-mine-lynx-crypto/

PART 2: TECHNICAL SPECIFICATIONS

To ensure environmental sustainability, Lynx developed Hybrid Proof-of-Work (HPoW). Lynx HPoW still uses PoW *but modifies it so it isn't profitable.* Below are the coin parameters and the HPoW business rules.

Basic Coin Parameters

1. 30-second block time
2. Cost of a transaction is .0001 Lynx/kilobyte
3. 1 week block reward maturity[32] for miners
4. 1 Lynx block reward plus fees

The coin parameters are changes from Lynx's upstream, Litecoin. These parameters reduce the likelihood of miner profitability. Removing the profit incentive for miners ensures that Lynx developers can maintain control of the project's innovation and continue to pursue efforts of lowering mining costs.

1. The first parameter makes for fast first confirmation times on transactions. Additionally, with a ~1MB block size, as transaction volume grows, we will be able to handle higher transactions per second.
2. The cost of a transaction is not zero, to reduce dust[33] attacks, but is still so inexpensive, that transaction fees will not be a barrier to using Lynx regularly.
3. The Miner must wait one full week to gain access to their block reward. This modification makes it very difficult for a miner to immediately sell their mining reward on an exchange.
4. The fourth parameter is that Lynx's block reward is so low, it is intentionally unprofitable to mine. By removing as many incentives as possible for ASIC miners, only individuals who actually use Lynx are incentivized to run a LynxCI node either on a low power device or in the cloud.

The coin parameters plus the Hybrid Proof of Work create Lynx primary business rules and, as a result, these business rules create barriers for high-powered ASIC mining.

[32] This is the amount of time a miner must wait to claim the block reward and fees from winning a block. This slows down the velocity of money on the network and restricts miners from quickly selling their mining rewards on exchanges.

[33] The smallest amount of Lynx is 0.00000001 Lynx. This amount is also called a 'liv', inspired by the idea that "all cats have nine lives" and the author's housecat, Olivia, who is possibly the best cat ever.

Hybrid Proof of Work Rules

1. A single miner can’t win a block more than once every 30 minutes.
2. The miner’s reward address balance must be greater than or equal to a required fluctuating minimum amount of Lynx to win a block.
3. By using random selection, the fastest miners are not always guaranteed to win the block reward.

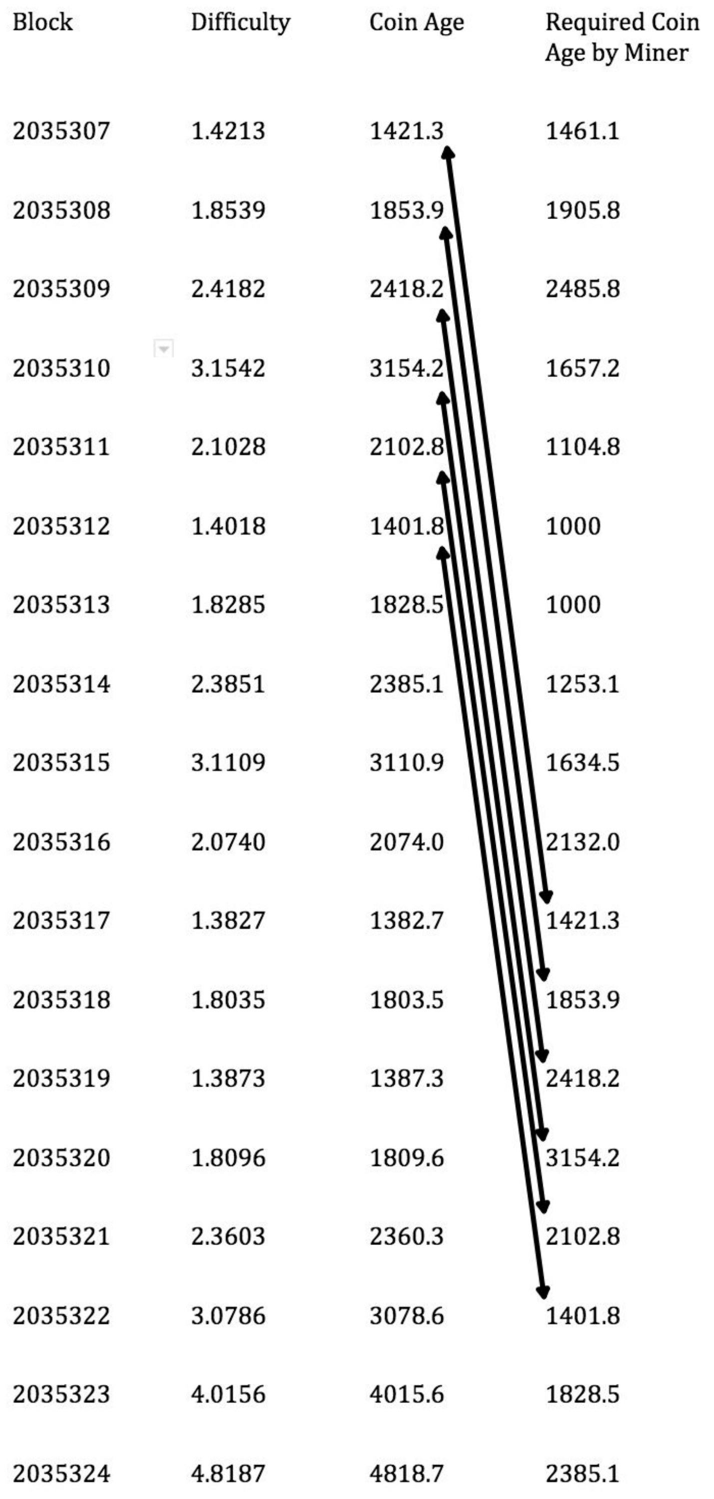
Lynx implements a series of business rules that must be met by the miner to successfully get a candidate block accepted by the network. Taken together, the three business rules result in “Hybrid Proof of Work” (HPoW).[34]

1. The first rule requires the miner's address cannot have been the recipient of a mining reward in the previous 60 blocks (~30 minutes). The address supplied within the candidate block coinbase header value is checked during verification by other nodes. If a match is found in the previous 60 blocks, the candidate block is refused even if they have the fastest solve time for the hash. The verification fails and the block is considered invalid.

2. The second rule requires the address supplied for the coinbase reward must have a coin age of 1000 or greater. The coin age is the product of the number of coins in the miner reward address (at the time the candidate block is created) and the difficulty value of the previous 10th block[35] from the current one being solved. This number can never be less than 1000. The following chart shows a series of blocks and the coin age requirement for the miner, for the respective block.

[34] These rules are subject to change.

[35] This is intended to remove issues with network latency. Global network latency will sometimes delay propagation of the previous block’s status. This means a miner might start mining the next block too late and this isn’t fair to the respective miner. However, the likelihood the mining node has the previous 10th block (from the one they are working on) is high. So, the rolling nature of the update allows for all nodes to always know the difficulty value they should be working with and it removes the reliance upon the timestamp value in the block. If the miner is working with the wrong coin age value, it can be assumed they are not fully in sync or experiencing network latency issues. This rule also scales with Nielsen’s Law. See the References section for more information.



Block	Difficulty	Coin Age	Required Coin Age by Miner
2035307	1.4213	1421.3	1461.1
2035308	1.8539	1853.9	1905.8
2035309	2.4182	2418.2	2485.8
2035310	3.1542	3154.2	1657.2
2035311	2.1028	2102.8	1104.8
2035312	1.4018	1401.8	1000
2035313	1.8285	1828.5	1000
2035314	2.3851	2385.1	1253.1
2035315	3.1109	3110.9	1634.5
2035316	2.0740	2074.0	2132.0
2035317	1.3827	1382.7	1421.3
2035318	1.8035	1803.5	1853.9
2035319	1.3873	1387.3	2418.2
2035320	1.8096	1809.6	3154.2
2035321	2.3603	2360.3	2102.8
2035322	3.0786	3078.6	1401.8
2035323	4.0156	4015.6	1828.5
2035324	4.8187	4818.7	2385.1

3. The third (and last rule) concerns the reward address submitted in the candidate block. After executing a single SHA256 hash on the miners reward address, the last

> 2 characters found must match the last 2 characters of the block hash value submitted by the miner in the candidate block. This randomizes who can actually win the block. Even the fastest miner can’t be guaranteed to win the block or a series of blocks in succession.

Additionally, the Hybrid Proof of Work requirements can be independently checked by all other nodes on the network during the confirmation phase. It's easy to see if a submitted block is valid. Due to the low miner reward, the intended network topology would ideally consist of mostly low power mining rigs. As a result of the HPoW rules, the likelihood is good that every miner that complies could win a block, not just the most powerful miner. These business rules won’t work well for mining pools so solo mining will become the primary mining method.

Collaborative mining pools will lose interest due to the low mining reward and the long block maturity. Without the profit incentive, the collective effort of a mining pool poses no benefit. As a result, high-capacity miners with expensive mining hardware will reject Lynx as a profitable coin project to mine.

If a high capacity miner still decides to mine Lynx, they will realize solo mining only brings them a reward of 1 Lynx per block. A creative miner might try to manipulate the system by rotating new addresses after each block is won.[36]

Lynx has implemented an aggressive difficulty adjustment algorithm[37] that prevents inordinately long block times after an ASIC leaves the network. While a small disruption in average blocktime may occur, the protocol will tolerate the change.

Taking power away from ASICS allows the network difficulty to drop further along with the network hash rate.[38] This lowers the electrical and hardware cost of the network and further secures the network by flattening the miner base and increasing the likelihood that truly anyone could mine blocks and confirm transactions.

In short, Lynx remains a Proof of Work project despite borrowing ideas from Proof of Stake. The HPoW rules ensure that blocks continue to get mined by a broad network of miners which makes the network more resilient, as the network cannot be controlled by a few powerful miners or pools.

[36] For more information, please see the “51% Brute Force Attack” section of the paper.

[37] Digishield was implemented in early 2018.

[38] “Bitcoin Difficulty.” *Bitcoin Wisdom*. https://bitcoinwisdom.com/bitcoin/difficulty

Block Validation Process

The Lynx code includes the DigiShield[39] difficulty adjustment algorithm. This enhancement better ensures the 30-second block-time average and provides support for low-hash, eco-friendly mining rigs to mine blocks after a high-powered mining rig leaves.

The Hybrid Proof of Work business rules have priority over the difficulty adjustment algorithm. So, when the network is comprised of thousands of mining rigs, the competition between nodes should be balanced. After an occasional ASIC disrupts the network hashing speed, the difficulty adjustment algorithm will quickly retarget the difficulty value. Since each Lynx node is running the same code, each is responsible for confirming transactions received by their peers.[40] The peers review the pre-existing requirements and HPoW business rules by answering the following questions:

1. Is the coinbase address in the block used in the last 60 blocks? If yes, this block is not confirmed and not propagated to peers.
2. Is the coin age of the submitted coinbase address lower than the required value? If yes, the block is not confirmed and not propagated to peers.
3. Is the last 2 digit value found in the coinbase address (as a string) different from the last 2 digit value found in the candidate block hash (as a string)? If yes, the block is not confirmed and not propagated to peers.

LynxCI - Lynx Cryptocurrency Installer

The Lynx Cryptocurrency Installer (LynxCI)[41] is a program that runs on a Linux operating system - specifically Ubuntu and Raspian.[42] LynxCI installs the latest stable release of Lynx along with the full historical blockchain history of the project which includes over four

[39] "What is DigiShield & How it Works to Retarget Difficulty." Bitcoin Forum. March 22, 2014. https://bitcointalk.org/index.php?topic=526721.0

[40] Peers are other Lynx nodes that a respective node communicates with. Due to the large size of the Lynx network, a single node can't talk to every other node, so a short list of peers are selected and this forms a mesh of interconnected nodes.

[41] "Lynx Node Builder." *Github*. https://github.com/doh9Xiet7weesh9va9th/LynxNodeBuilder

[42] Several members of the Lynx community on Discord have assisted us with code. Developers who are interested in volunteering are invited to contact us via Discord.

years of transactional data. LynxCI also installs a mining software package[43] that allows the device to mine the Lynx HPoW coin. Through solo mining, the software allows the node to actively participate in the Lynx network by creating and confirming transactions on the network in the mining process. LynxCI is intended to be used on computers with relatively limited RAM and processing power (such as Raspberry Pi 3), but it can also be used in cloud VM environments.

LynxCI ISO

The ISO is a stand alone file that can be flashed to a micro-SD card and then physically inserted into a low power device.[44] When the device is powered on, it automatically configures itself and, after a short amount of time, completely runs all functions of LynxCI without a KVM.[45] This version uses the Raspbian Lite operating system based on Debian.

LynxCI for Linode

A Stackscript extends the functions of LynxCI for use on the the linode.com platform. This allows an individual to create a node for as little as USD $5/month and replicate all the features of the Raspberry Pi 3 implementation. This version uses the Ubuntu operating system.

LynxCI Functions

LynxCI builds a Lynx node that provides the following functions:

Mining

The node participates in both pool mining and solo mining. The current release randomly selects the option to solo mine or pool mine. Future updates will change this random selection to only solo mining once HPoW is released.

Transaction Verification

Each device runs a full node so a full copy of the blockchain is maintained and verified while Lynx runs.

[43] Pruvot, Tanguy. ”CPUMiner-Multi.” *GitHub.* https://github.com/tpruvot/cpuminer-multi

[44] For more information (and to view the URL to the instructional video), see “Can Non-Techies Mine Lynx” in the References section.

[45] KVM refers to keyboard, video and mouse.

Block Explorer

If the device detects enough system resources, a more robust Block Explorer will run, but will fall back to a less processor-intensive version in the event fewer hardware resources are available.

Network Topology

Each node silently sends anonymous usage data to a polling server in the cloud. This will allow the mapping functions to render real time maps for users to see the physical global network.

Local RPC functions

For use with decentralized exchanges and external application development, all RPC functions are fully supported on each node device. By default, the wallet functions are disabled for security reasons.

News Feed & Links

In addition to Twitter feeds and Discord widget, rendering of RSS news information comes from the getlynx.io website and other sources. The local node will provide a single source for information about the network and project.

Seed node capable

If a node owner would like to volunteer, a DNS entry can be assigned to the node so the device is used as a default seed node option for wallets when connecting to the network.

All the above listed functions are configured with default values and allow the user to run them without configuration. This ‘headless’ design allow users ranging from totally non-technical to experienced IT professionals to easily create a Lynx node that supports the network. Each node on the network receives equal treatment.

Mitigated Risks

The coin parameters plus the Hybrid Proof of Work create Lynx primary business rules and, as a result, these business rules address the likelihood of a successful 51% attack.

51% Attack

When a coin project has a relatively low hashing power, it is at higher risk of succumbing to a 51% attack. A 51% attack[46] occurs when a single miner gets to control a majority of the hashing power of the network for a sustained period of time.[47] This miner then has some degree of control of the blocks mined for a short period of time and bad things can happen [48] if they are able to retain control of that majority network hashing power. The risk of financial loss to members is low as the attacker can only modify their own transactions or delay the confirmation of other transactions (in addition to a few other things), but they can't undo past transactions or steal anyone's coins. Overall, a successful 51% attack can just be embarrassing for a coin with a low market cap value. In rare cases, if the attack is timed properly with a large purchase, the attacker might be able to pull off a double spend [49] but it is unlikely anyone is buying houses with Lynx based on the current transaction volume of the network. Additionally, one could mitigate that risk by waiting for a greater number of confirmations from the network.

One industry answer to this problem is to engage with higher and higher network hashing power as this will require an attacker to lay out a considerable amount of investment for a very low likelihood of success. Additionally, the network would see the bad actor attempt and might decide to proactively ban this miner.

It is reasonable to conclude that because Lynx is run on a network of low power devices for mining and transaction confirmation, it could suffer from a 51% attack. Lynx will avoid this attack with HPoW. Rule 3 of HPoW removes the premise that an attacker could succeed with a 51% attack for a sustained period of time by simply having the highest hashing power rig on the network. By creating business rules that delay and distribute the opportunity for a miner to win a block, Lynx thwarts the ability for a single powerful miner to win a block over and over again. No longer will the most powerful miner win the next block with confidence. In addition to making Lynx mining unprofitable, the HPoW business rules used during the creation of a block require the miner to comply. If the miner does not, the network invalidates blocks created by that miner. These business rules don't completely rule out the opportunity for a successful 51% attack, but they diminish its risk.

[46] "51% Attack, Majority Hashrate Attack." *Bitcoin.org.* https://bitcoin.org/en/glossary/51-percent-attack

[47] In this instance, the use of "miner" refers to BOTH a mining rig AND the person who owns/controls that mining rig.

[48] "What can an attacker with 51% of hash power do?" *Stack Exchange.* https://bitcoin.stackexchange.com/questions/658/what-can-an-attacker-with-51-of-hash-power-do

[49] "Double Spending." *Investopedia.* https://www.investopedia.com/terms/d/doublespending.asp

Because the mining reward is so low, the primary reason someone might try a 51% attack is to attempt a double spend.[50] To accomplish this, an attacker could create a script that dynamically switches out the mining reward address with a new one each time a block is won to subvert Rule 1. This would need to be done quickly between blocks due to the random nature of Rule 3. Additionally, the cost to the attacker would increase, as a result of the increased mining difficulty. Since the coin age is unknown, a considerable amount of Lynx would be required in each address. Throughout this process, the attacker would have to maintain the fastest miners on the Lynx network to complete this task. The cost of having the required number of Lynx addresses with the required coin age amount would be high and unpredictable. Eventually, these business rules will be coded into Lynx so HPoW can dynamically respond based on the network node count, coin market valuation, and algorithm difficulty value. Exchanges are advised to require 200 confirmations on all deposits.

Transaction Malleability[51]

A miner compiles their own version of Lynx without the restrictive business rules for mining. This attack is expected and the answer would be to require all nodes to actually check new blocks during block validation, which they already do. This will add a slight amount of time to the validation step, but the other nodes that receive the new false block will quickly notice the block does not comply with the business rules and the block will be dropped, the chain will fork and miners will continue working to find a new block that complies with the business rules. Since the longest chain wins and the forks naturally occur, this process will gracefully work itself out. For very large transactions, users would be wise to see 200 confirmations (~100 minutes) and for medium transactions, users should wait for 30 confirmations (~15 minutes).

[50] Oberhaus, Daniel “Cryptocurrency Miners Are Sabotaging Blockchains for Their Personal Gain.” *Motherboard*. May 25, 2018. https://motherboard.vice.com/en_us/article/a3a38e/what-is-a-51-percent-attack-silicon-valley-bitcoin-gold-verge-monacoin-cryptocurrency

[51] Klitzke, Evan. “Bitcoin Transaction Malleability.” July 20. 2017. https://eklitzke.org/bitcoin-transaction-malleability

PART 3: ROADMAP

LYNX is currently available on the Cryptopia exchange and on the Coinomi mobile wallet platform.[52] Lynx's listing on Cryptopia's LTC market helps to keep the coin stable, and Coinomi offers another place (in addition to the desktop wallets on the Lynx website) to store it.[53]

The list below briefly describes some of Lynx "to-do" list items and goals for the project.

LynxCI for Amazon AWS

Extend the functions of LynxCI into an AMI image for use on the Amazon.com AWS platform. The AWS customer can easily find the free AMI image and leverage all the features built into the LynxCI code on the AWS platform. Cost can be as low as USD ~$5/month and users can opt to build larger sizes as they like.[54]

Builder project for the Raspberry Pi platform

By leveraging the LynxCI script, popular builder websites are interested in including cryptocurrency projects. Because Lynx is low risk, low cost and fast, kids can play with the LynxCI script to build a node, customize it and then build applications on it. With a working example of solo mining, kids can get excited about the project and get involved. The feeling of participating in a global project, in even the smallest amount, can be very inspiring for young girls and boys. This roadmap item justifies the numerous amount of comments in the LynxCI code. For a person who is new to Bash,[55] the included comments can prevent a great deal of frustration.

[52] When Lynx was listed on Cryptopia, Kittehcoin was de-listed and removed to avoid any confusion. This was done to phase out the defunct coin (MEOW) and prevent scammers from continuing to work on that broken code base. Lynx is currently available at: https://www.cryptopia.co.nz

[53] See: https://coinomi.com

[54] It is important to remember that the mining power of the CPU in this environment is throttled to 10% capacity due to restrictions for mining in the cloud, and this value is subject to change in future releases. This value can be easily changed by the user and it is up to them to assign a temperature safe value for their device. Even at 100% CPU usage, mining Lynx on the device will not be profitable or even cover the hourly cost of electricity.

[55] "GNU Bash." *GNU Operating System*. https://www.gnu.org/software/bash/

Jaxx Mobile Wallet Integration[56]

Lynx is already listed in Coinomi. Getting listed on the Jaxx mobile wallet will provide another option for users.

Blocknet DX trading platform Integration

Centralized exchanges are risky and may eventually become obsolete for a number of reasons. They boast expensive on-ramping cost for emerging projects and are vulnerable to hacking and internal theft. With the advent of Atomic Swaps between compliant coin projects, the idea of centralized exchanges will slowly dissolve. Therefore, decentralized exchanges may be the future of cryptocurrency trading and Lynx is primed for early adoption because Lynx is Atomic Swap compliant.

Real-time global map of LynxCI nodes

The objective is to build a real-time map that displays global distribution of LynxCI devices. This idea is modeled after the Global Bitcoin Node Distribution Map.[57] This map will use real-time publicly accessible data that is globally polled from LynxCI devices. The length of time the data is stored is 1 hour and the exact data extracted from LynxCI nodes is limited to the public IP, the block height, and the MAC address. No personally identifiable data will be collected. This code will be open source and available for public audit.

Real-time energy calculator of LynxCI nodes

In an effort to be transparent about the eco-friendly nature of the coin and the low cost to run the network, this tool allows the visitor to view the real-time electrical consumption of the global Lynx network, specifically the LynxCI nodes. In fact, this calculator will be displayed on the same LynxCI web page as the global map distribution of LynxCI nodes. The calculator will default to the current data set from the global mapping tool, but the user will have the ability to override the default values and enter their own numbers. The calculator will factor in the country of the LynxCI device and query for the average price per kilowatt hour in the respective country. While IP addresses can be spoofed and the exact termination point can't always be verified, this will still provide a useful report of the Lynx network cost by country.

[56] See: https://jaxx.io

[57] "Global Bitcoin Nodes Distribution." *Bitnodes*. https://bitnodes.earn.com

Dynamic HPoW Parameters

Using the real-time data collected from exchanges, the global node map and the algorithm difficulty value, the HPoW parameters will self-adjust. This removes the opportunity for human error and allows the network to scale more smoothly based on price, usage, and mining activity.

Solo mining only by 2019

The long term strategy for the Lynx network is to remove node hierarchy within the global Lynx network. Removing mining pools is a critical step in this project.

Application Integration

Our primary long term goal for Lynx is application integration. With its low implementation costs, decentralized network topology, and long-term sustainable energy costs, Lynx provides a viable building platform for technical application designers.

References

"51% Attack, Majority Hashrate Attack." *Bitcoin.org.* https://bitcoin.org/en/glossary/51-percent-attack

"Bitcoin Difficulty." *Bitcoin Wisdom.* https://bitcoinwisdom.com/bitcoin/difficulty

"Bitcoin Mining." *Investopedia*. https://www.investopedia.com/terms/b/bitcoin-mining.asp

Brown, Mike. "Bitcoin's Energy Consumption is Killing the Planet but There is a Solution." *Inverse*. December 12, 2017. https://www.inverse.com/article/39138-bitcoin-energy-consumption

Bustillos, Maria. "Inside the Fight Over Bitcoin's Future." *The New Yorker.* August 25, 2015. https://www.newyorker.com/business/currency/inside-the-fight-over-bitcoins-future

"Can Non-Techies Mine Lynx?" *GetLynxio.* https://getlynx.io/can-non-techies-mine-lynx-crypto/

Chester, Jonathan. "The Battle For Bitcoin: What You Need To Know About Bitcoin And Bitcoin Cash." *Forbes*. November 17, 2017. https://www.forbes.com/sites/jonathanchester/2017/11/27/the-battle-for-bitcoin-what-you-need-to-know-about-bitcoin-and-bitcoin-cash/#115b9dc6331f

"Database." *Wikipedia*. https://en.wikipedia.org/wiki/Database

"Double Spending." *Investopedia*. https://www.investopedia.com/terms/d/doublespending.asp

"Global Bitcoin Nodes Distribution." *Bitnodes*. https://bitnodes.earn.com

"GNU Bash." GNU Operating System. https://www.gnu.org/software/bash/

"Gresham's Law." *Merriam Webster.* https://www.merriam-webster.com/dictionary/Gresham's%20law

Hankin, Aaron. “Here’s How Much it Costs to Mine a Single Bitcoin in Your Country.” *Marketwatch*. May 11, 2018 https://www.marketwatch.com/story/heres-how-much-it-costs-to-mine-a-single-bitcoin-in-your-country-2018-03-06

Irfan, Umair.

- “Bitcoin’s Price Spikes is Driving an Extraordinary Surge in Energy Use.” *Vox*. December 7, 2017. https://www.vox.com/energy-and-environment/2017/12/2/16724786/bitcoin-mining-energy-electricity
- “Bitcoin’s Price Dropped but it’s Still Devouring an Obscene Amount of Energy. *Vox*. Feb 6, 2018. https://www.vox.com/energy-and-environment/2018/1/18/16901422/bitcoin-price-crash-energy-emissions

“Kittehcoin.” *Github*. https://github.com/kittehcoin/kittehcoin

“Kittehcoin launched! Come get some MEOW now. U haz it! DOGE sad.” *Bitcointalk*. December 24, 2013. https://bitcointalk.org/index.php?topic=383068.0

Klitzke, Evan. “Bitcoin Transaction Malleability.” July 20, 2017. https://eklitzke.org/bitcoin-transaction-malleability

“Lynx Node Builder.” *Github*. https://github.com/doh9Xiet7weesh9va9th/LynxNodeBuilder

Madrigal, Alexis. “Bitcoin Mining Turns Money into Profit.” *The Atlantic.* May 12, 2018 https://www.theatlantic.com/technology/archive/2018/03/bitcoin-mining-arbitrages-cheap-electricity-into-money/555416/

Miles, Kathryn. “Bitcoin is eating Quebec.” *MIT Technology Review*. April 11, 2018. https://www.technologyreview.com/s/610786/bitcoin-is-eating-quebec/

“Moore’s Law.” *Merriam Webster Dictionary.* https://www.merriam-webster.com/dictionary/Moore's%20law

Palmer, Jackson. “My Joke Cryptocurrency Hit $2 Billion and Something Is Very Wrong.”

Motherboard. Jan 11, 2018. https://motherboard.vice.com/en_us/article/9kng57/dogecoin-my-joke-cryptocurrency-hit-2-billion-jackson-palmer-opinion

Nielsen, Jakob. “Nielsen’s Law.” *Nielsen Norman Group.* April 5, 1998. https://www.nngroup.com/articles/law-of-bandwidth/

Oberhaus, Daniel “Cryptocurrency Miners Are Sabotaging Blockchains for Their Personal Gain.” *Motherboard*. May 25, 2018. https://motherboard.vice.com/en_us/article/a3a38e/what-is-a-51-percent-attack-silicon-valley-bitcoin-gold-verge-monacoin-cryptocurrency

“Programming Merit Badge.” *Boy Scouts of America.* 2017. http://usscouts.org/mb/worksheets/Programming.pdf

“Proof of Work.” *Bitcoin Wiki.* https://en.bitcoin.it/wiki/Proof_of_work

Pruvot,Tanguy. ”CPUMiner-Multi.” GitHub. https://github.com/tpruvot/cpuminer-multi

Roberts, Paul. “This is What Happens When Bitcoin Miners Take Over Your Town.” *Politico*. March/April 2018. https://www.politico.com/magazine/story/2018/03/09/bitcoin-mining-energy-prices-smalltown-feature-217230?utm_source=digg&utm_medium=email

Rogers, Adam. “The Hard Math Behind Bitcoin’s Global Warming Problem.” *Wired*. December 15, 2017. https://www.wired.com/story/bitcoin-global-warming/

Verma, Sid. “Bitcoin's Exorbitant Energy Costs May Prove to Be Biggest Risk.” *Bloomberg*. November 9, 2017. https://www.bloomberg.com/news/articles/2017-11-09/bitcoin-s-exorbitant-energy-costs-may-prove-to-be-biggest-risk

“What can an attacker with 51% of hash power do?” *Stack Exchange.* https://bitcoin.stackexchange.com/questions/658/what-can-an-attacker-with-51-of-hash-power-do

“What is DigiShield & How it Works to Retarget Difficulty.” *Bitcoin Forum*. March 22, 2014. https://bitcointalk.org/index.php?topic=526721.0