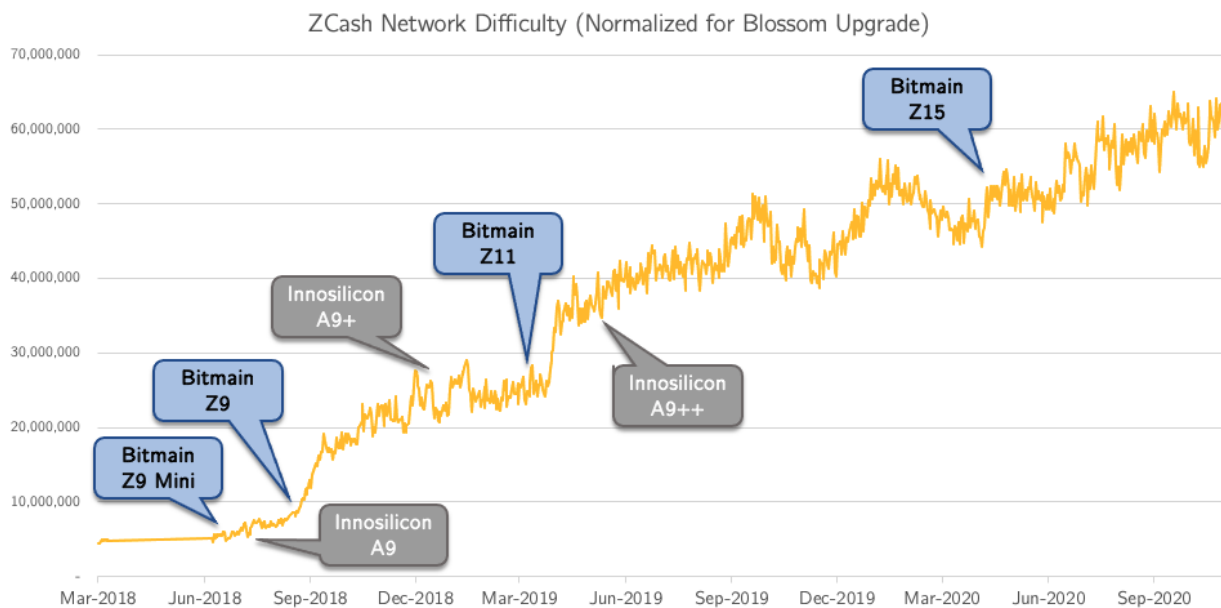


Equihash Mining Bible

Exploring new and old frontiers in crypto mining

Written by Ethan Vera and Thomas Heller
Jan-2021



Foreword	2
Equihash Algorithm	2
Technology	2
ASIC Resistance	2
Major Chains	3
ZCash (\$ZEC)	3
Horizen (\$ZEN)	4
Komodo (\$KMD)	4
Pirate (\$ARRR)	5
History and Outlook of Equihash Mining	5
History of Mining	5
Mining Outlook	6
ASIC Case Studies	6
Bitmain Antminer Z11	6
Buying and Hosting ZEC Miners Through Compass	8
Leveraging Luxor Switch	9
Profit Switching	9
Luxor Setup Process	10
Other Considerations	11
Financing Equihash ASICs	11
Viability in Mobile Mining Units	11
Third-party Custom Firmware	11
ASIC Management Software	11
Immersion Cooling	11
Conclusion	12

Foreword

Today's mining institutions predominantly focus on SHA256 and Bitcoin mining, yet there are many lucrative mining opportunities in other Proof-of-Work (PoW) algorithms. Equihash has proven to be one of the most profitable algorithms in recent years and has delivered strong risk-adjusted returns for miners.

Whether you are trying to stack more Bitcoin for your capital investment or you want to hodl copious amounts of altcoins, Equihash is a great algorithm to mine.

Equihash Algorithm

Technology

[Equihash](#) is a PoW algorithm based on a computer science and cryptography concept called the Generalized Birthday Problem.

Equihash is a memory-oriented PoW, which means your mining efficiency is mostly determined by how much RAM you have. It was originally designed to dissuade manufacturers from building purpose built hardware (ASICs) and instead only be mined by generalized hardware known as GPUs.

Most of the blockchains built on Equihash adjust their difficulty after every block (DigiShield v3), a much more dynamic method than Bitcoin which adjusts every 2,016 blocks. Some blockchains such as Komodo can even adjust their difficulty during the block round through the use of [aPOW](#). In addition, block times are much faster than Bitcoin, usually targeted at 75 seconds.

In Equihash, hashrate is measured in *solutions* instead of *hashes*. It is functionally the same thing but mining operations will use [KSol and MSol](#) when referencing hashrate.

ASIC Resistance

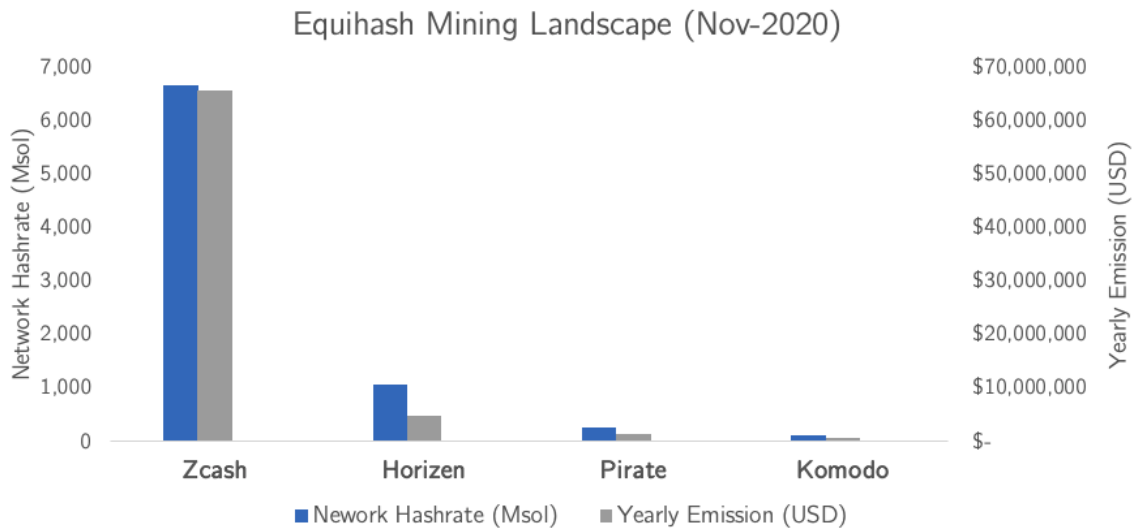
Bitmain started to dominate the ASIC and PoW networks as early as 2017. With rising market valuations (mining reward), the incentives to create ASICs increased, so the PoW blockchains needed to decide their stance on ASIC resistance. Some communities like Monero stood firm, but ZCash abandoned their original stance of resistance.

In May-2018, Bitmain released the first ASIC for Equihash, the Antminer Z9. This was followed shortly by Innosilicon releasing the A9 ZMaster. Zooko, the CEO of Electric Coin Company (ZCash), took a [neutral position](#) on ASIC resistance. The community also did a [survey](#) to reinforce his position. Since that point ASICs have dominated the industry.

Major Chains

There are over a dozen blockchains built using the Equihash algorithm. The largest by far is **ZCash** (#5 PoW), followed by **Horizen** (#11 PoW), **Pirate** (#46 PoW) and **Komodo** (#48 PoW).

The majority of Equihash hashrate goes to ZCash but a good portion is also used to secure Horizen, Pirate and Komodo as shown below.



ZCash (\$ZEC)

[ZCash](#), launched in 2016, aims to improve upon Bitcoin's original design. Bitcoin and most other cryptocurrencies expose your payment history to the public. ZCash was the first open, permission-less cryptocurrency that could fully protect the privacy of transactions using zero-knowledge cryptography.

One unique aspect of ZCash is that it utilizes two types of addresses, shielded and unshielded, to offer the option of anonymity to its users. Also, it provides the user to selectively disclose information about their private transactions. This allows for transparency for entities who must comply with audit obligations.

zk-SNARK stands for "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge". In layman's terms, zero-knowledge cryptography enables one to encrypt transaction metadata yet still maintain a secure ledger of balances without disclosing the parties or amounts involved. You can learn more about zk-SNARKs in the following [URL](#).

[Luxor & Compass](#)

ZEC is traded on most exchanges and is one of the most well known privacy coins. In Jan-2021, Bittrex announced they were delisting support for ZEC (along with other privacy coins). Since that point there has been speculation that the majority of regulated US exchanges will delist privacy coins given the risk associated with them.

Horizen (\$ZEN)

[Horizen](#) (former Zencash) originated in May 2017 as a fork of ZClassic (itself a fork of ZCash). The network is similar to ZCash in that it uses a zero-knowledge proof algorithm (zk-SNARKS) to solve privacy and fungibility problems experienced by other coins, however, it contains some fundamentally different features.

Horizen was created to provide a secure platform with transaction funding, media, and messaging capabilities. One of the most exciting and promising developments within the Horizen ecosystem has been the prevalence of distributed applications (DApps), which are applications that can be built on the blockchain network. Horizen's DApps include ZenChat, a secure messaging platform, ZenPub, an anonymous document publisher, and ZenHide, a domain fronting platform. ZenChat provides the ability to incorporate encrypted messages alongside verified ledger transactions, encrypted using AES-256 and the Perfect Forward Secrecy protocol. Horizon also leverages Shielded and Unshielded Transactions and Secure Nodes & Super Nodes.

Digital Currency Group (DCG) is a big supporter of the project and even Grayscale has a [trust for ZEN](#).

Komodo (\$KMD)

[Komodo](#)'s development dates back to 2014. The Komodo Platform was built on top of both Bitcoin and ZCash. Komodo is an independent asset-chain secured by dPoW (Delayed PoW). Basically, dPoW consists of attaching a backup of the Komodo chain to the Bitcoin blockchain. This is done by inserting a block hash from a block in the Komodo chain into a block on the Bitcoin blockchain.

Every 10 minutes a "backup" is made, transactions completed before that point are protected with the power of Bitcoin's hashrate. In order to perform a successful attack, you would need to overpower the Bitcoin network to destroy the backup before attempting to alter the Komodo chain. This makes security against double spends and hostile takeovers nearly impossible.

Komodo is developing a new scaling feature called Cross-Chain Smart Contracts. This means that multiple blockchains can work in unison to function as a single chain. AtomicDEX is their new secure wallet and non-custodial decentralized exchange rolled into one.

Pirate (\$ARRR)

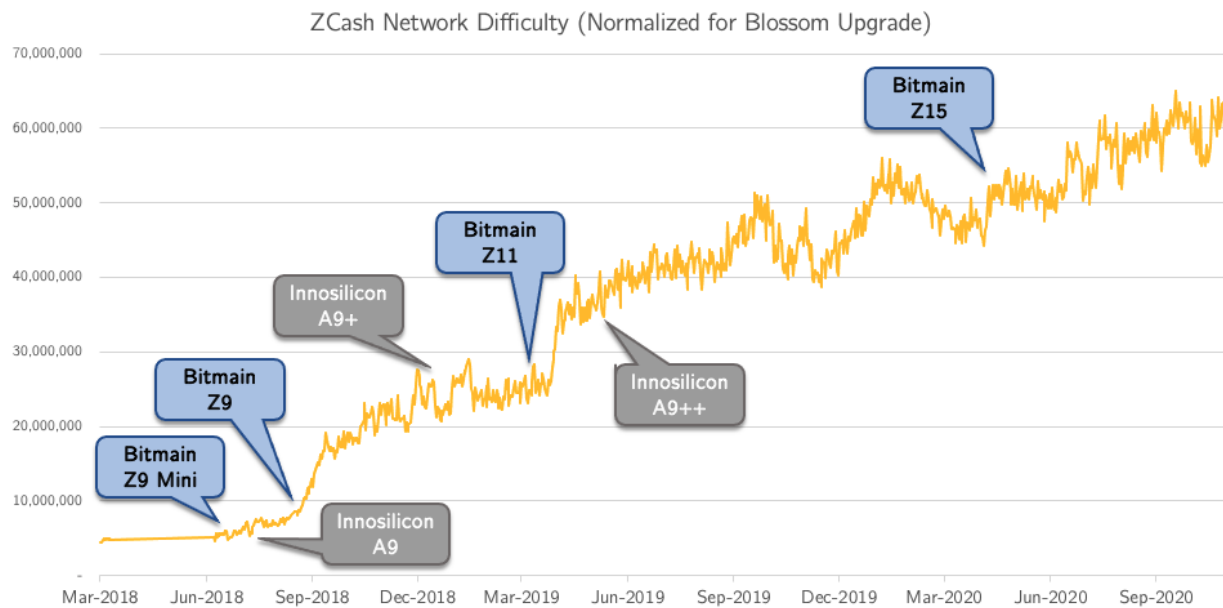
PirateChain, launched in August 2018, enforces users to make private transactions. Pirate uses ZK-Snarks to shield 100% of the peer to peer transactions on the blockchain. Unlike ZCash which has the option for shielded and unshielded. Pirate is an independent asset-chain launched on Komodo secured by dPoW.

History and Outlook of Equihash Mining

History of Mining

Just over 2 years ago, Equihash coins were being mined solely by GPUs. Since the release of the Antminer Z9 mini, more and more ASICs have been deployed to the various Equihash networks achieving a staggering 12x growth in average network difficulties.

Bitmain has added the most hardware to the market and is responsible for the first major increase in Sep-2018 and again in Mar-2019. Innosilicon also contributed a significant amount of hashrate to the network.



Most of these rigs were sold to Chinese mining farms, and even today the majority 80%+ of Equihash hashrate resides in China. There are notable exceptions such as [Argo](#) that mine it in the West.

Mining Outlook

Even the oldest Equihash miners are still profitable at our estimated average cost of hosted electricity of 3.5 cents per kWh*. That means that even with the Z15s adding a considerable amount of hashrate to the network there is likely still a strong presence of old machines and it will be that way for some time.

Mining revenue can fall by as much as 43% before the Z9 Minis start turning off. And even then many of the producers at 3.5 cents will start selling the equipment to producers with a lower cost. We call this the *Machine Slide*. As profitability declines, higher-cost miners will try to salvage some value for their rigs by selling them. Rarely do ASICs go months offline or get thrown away all-together if they can break a profit at > 1 cent per kWh.

	Estimated % of the Network	Release Date	Profitability Threshold (kWh)	Buffer in Mining Profitability*
Bitmain Z9 Mini	7.5%	Jun-18	\$ 0.05	43%
Innosilicon A9	3.5%	Jun-18	\$ 0.15	329%
Bitmain Z9	24.1%	Sep-18	\$ 0.07	100%
Innosilicon A9+	3.5%	Jan-19	\$ 0.15	329%
Bitmain Z11	33.4%	Apr-19	\$ 0.20	471%
Innosilicon A9++	8.5%	May-19	\$ 0.18	414%
Bitmain Z15	19.5%	Jun-20	\$ 0.53	1414%

We expect Bitmain to continue shipping Z15 batches and hashrate to increase even further in the foreseeable future. It is rumoured that thousands are shipping in Q1 2021. It was over a year period between the Z11 and Z15 so we aren't expecting a new miner on the network soon unless there is a major bull run.

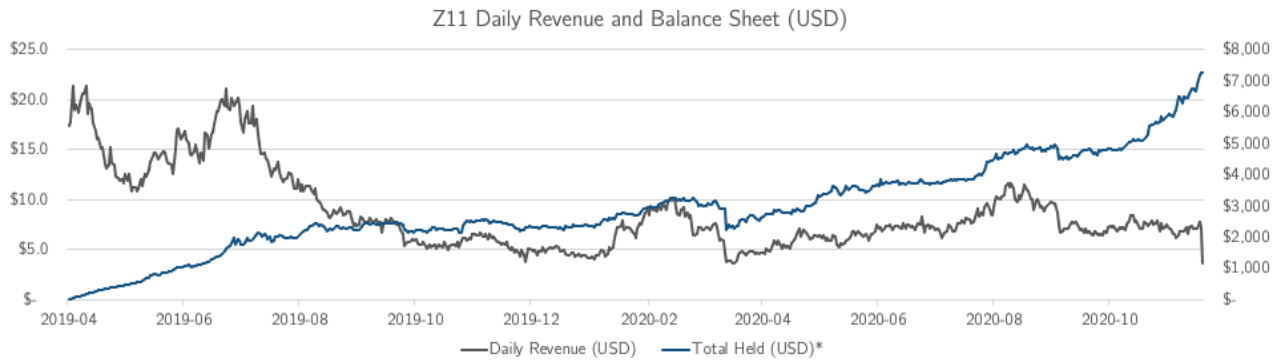
ASIC Case Studies

Bitmain Antminer Z11

The Bitmain Antminer Z11 was released in March of 2019. Luxor's first US-based miners started receiving their rigs in mid-April 2019. The first batch sold out in less than 20 minutes. After that, you had to go through a reseller.

The Z11 came out about ten months after the release of its predecessor the Z9. At an efficiency of 10.5 j/ksol, it was over twice as efficient as the Z9 (23.1 j/ksol). The initial batch sold in the range of \$1,048 and \$1,384 depending on when you got it.


After the release announcement of the Z11's, ZEC's price had sustained positive price movement as the community reacted favorably to the news.




Over the course of the next 19 months miners with 4 cent power, and holding 60% of their balance sheet in Bitcoin accumulated \$6,425 per rig. A total return on investment of 535%, or just under 200% annualized, making it one of the most profitable mining rigs of all time.

		Total Return on Investment (ROI)				
		% of Profit Held in Bitcoin				
		20.0%	40.0%	60.0%	80.0%	100.0%
Electricity Cost (kWh)	\$ 0.050	385%	447%	509%	571%	633%
	\$ 0.045	395%	459%	522%	586%	649%
	\$ 0.040	405%	470%	535%	601%	666%
	\$ 0.035	415%	482%	549%	615%	682%
	\$ 0.030	425%	493%	562%	630%	699%

Buying and Hosting ZEC Miners Through Compass

 EQUIHASH ASIC MINERS				
MINER	HASHRATE	POWER	PRODUCTION	DAILY REVENUE
Antminer Z15	420 ksol/s	1510 watts	0.15493 ZEC	\$9.79
Antminer Z11	135 ksol/s	1418 watts	0.04979 ZEC	\$3.15
Innosilicon A9++	140 ksol/s	1550 watts	0.05164 ZEC	\$3.26

hashr8.com 

The Antminer Z15 and Z11 are currently the most popular Equihash ASIC miners on the market. Bitmain is producing limited amounts of new Z15's and releasing them each month, while there are reasonable amounts of second-hand Z11's and 15's available. After the recent ZEC and ZEN halvings, significant quantities of miners are changing hands on the ASIC secondary markets as mining for some miners is no longer profitable with their electricity prices.

Compass offers [ASIC miners for sale](#) through their website. You can browse their available hardware and learn more about the purchase, such as ASIC specifications, shipping dates and the condition of the machine.

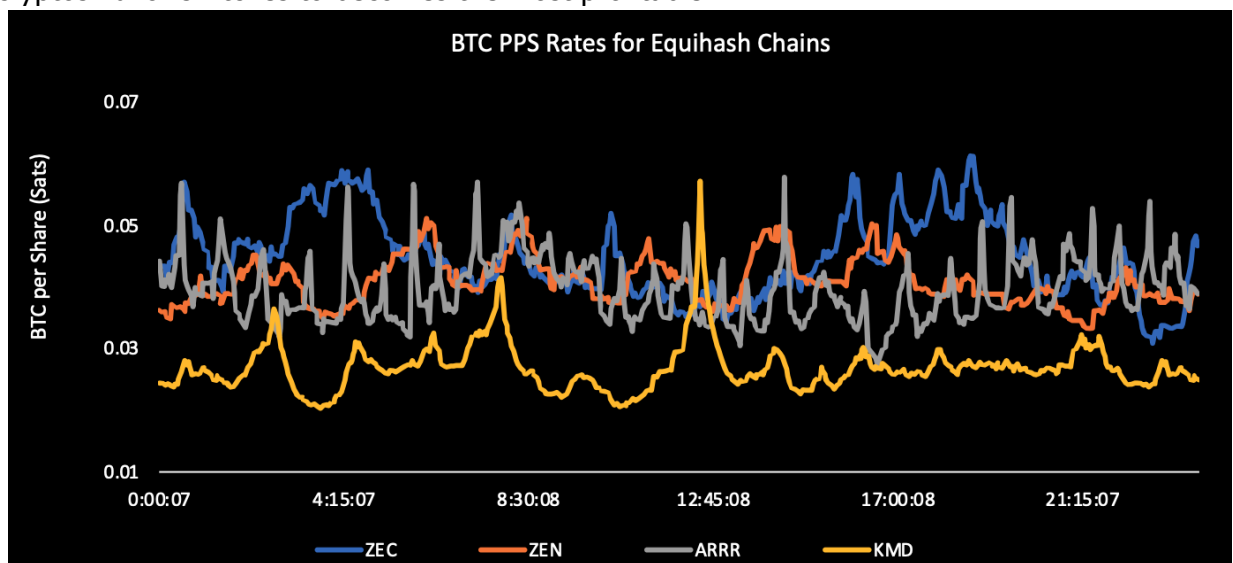
It's also important to choose the right facility to host your miner. For most people, mining at home is no longer profitable due to residential electricity costs. Most small to medium sized miners opt to "host" their miners in a professionally managed data center. [Browse mining facilities](#) through Compass to choose the most suitable one for your miners. Key factors include price, location, uptime and type of facility.

Leveraging Luxor Switch

Profit Switching

[Luxor](#) Switch is a profit-switching algorithm that increases the value of a miner's hashrate by switching between the Equihash chains. Equihash Switch has been on average 5% more profitable than mining straight ZCash. Your rewards are also paid in Bitcoin so you do not need to worry about handling multiple altcoin wallets.

During a 24-hour period, there are on average 85 different intervals in which one of the four cryptos Luxor switches to becomes the most profitable.



Luxor switches at the pool level (jobs behind the scene). It is advantageous to do this switching at the pool level because the pool can switch the jobs behind the scenes meaning that the connection between your ASIC and the pool is never broken. If you were to keep switching between pools it would lose minutes every time it had to reconnect.

Luxor automatically assigns work to your machine and collects your Equihash share. The pool then submits the share to the chosen Equihash coin's network. This way the miner is paid out for the share they submit, at a higher (or equal to) payout than a normal ZEC/ZEN pool.

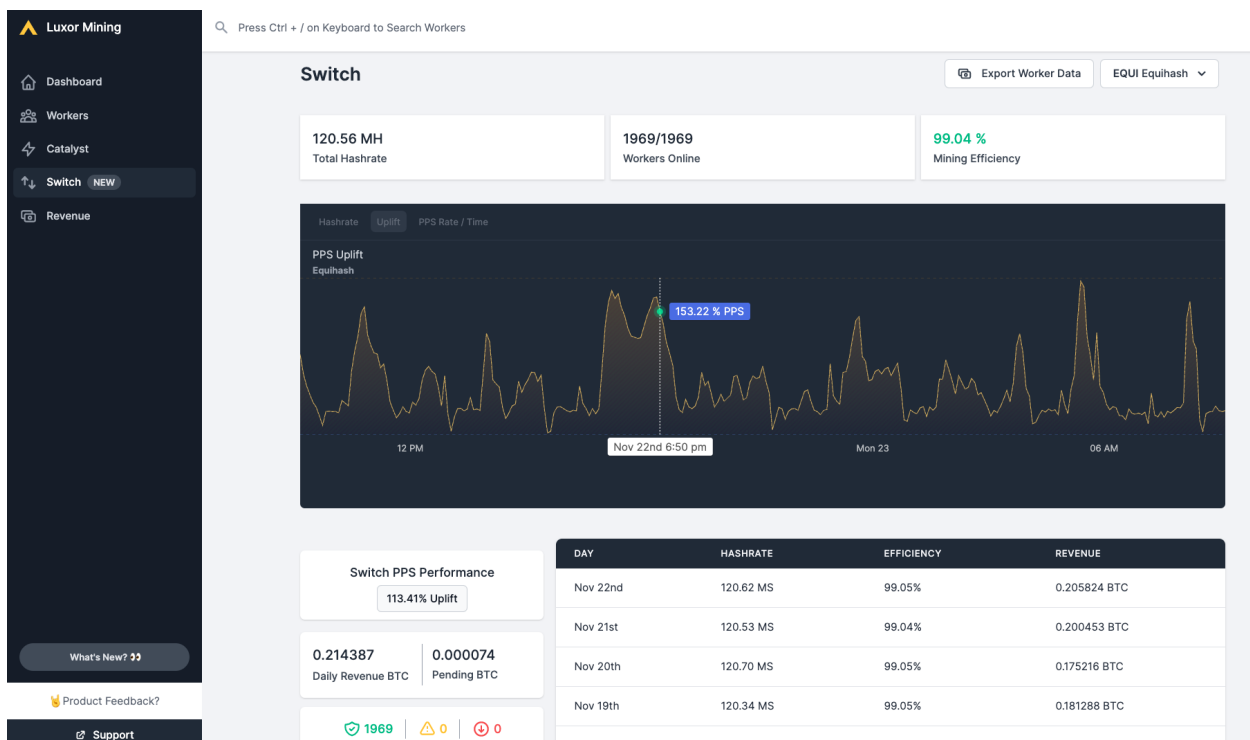
Measuring coin "profitability" isn't as straightforward as looking at the network difficulty, emission rate and coin price. There are other considerations such as liquidity fees to get the altcoin back to Bitcoin, network fees and moving the market. Switch is nimble enough to get the higher reward from the smaller chains but not too large that it ratchets up the difficulty levels.

Because it would be hard to manage 4 different Altcoins, Switch quotes your hashrate directly in BTC. You will see your Bitcoin balance increasing every few minutes.

Luxor Setup Process

Getting setup is simple:

- 1. Setup User Account**
 - a. Create a Luxor Account [here](#).
- 2. Setup Workers**
 - a. Use a scanning tool like [AngryIP](#) that allows you to scan every device on your network and see its IP address. After getting your miner's IP address, plug it into your browser and you are ready for configuration. If you are hosting through Compass you can get them to help with this step.
- 3. Configure Pool**
 - a. stratum+tcp://equihash.luxor.tech:700
 - b. Worker: LuxorUsername.WorkerName [workername can be anything]
 - c. Password: 123
- 4. Monitor Results**
 - a. Head to the Switch tab and Revenue tab to monitor your performance. You can see your uplift chart and past 24hours uplift in earnings.



Other Considerations

Financing Equihash ASICs

ASIC financing is starting to become more widely available for miners in the West. Companies such as [Blockfills](#) have started issuing equipment based financing packages for miners to buy more machines upfront. This financing tool is still relatively new, and unfortunately not many ASIC financiers have moved into other algorithms beyond SHA256 yet. As Equihash mining continues to deliver outsized risk-adjusted returns and companies like Argo highlight its strength, this financing avenue may become available to miners.

Viability in Mobile Mining Units

The Bitmain and Innosilicon Equihash miners are a similar form factor to SHA256 miners. They also have a similar power draw to the mid and old gen SHA256 miners. So it is very viable to put them in any type of facility including [mobile units](#). The Antminers run a little bit smoother than the A9s so they would probably be better suited for remote areas where maintenance is not as easy.

Third-party Custom Firmware

At this point in time there is no credible [firmware](#) for Equihash miners. In the past there has been firmware for the Antminer Z9 and Z11 for overclocking, but there are mixed reviews and we would recommend people to do their own detailed research into the risks of running it.

ASIC Management Software

Most [ASIC Management Software](#) platforms like Minerstat will integrate with all Equihash rigs. If you have built a custom solution for your farm, adding these rigs should not be very different than adding new SHA256 miners.

Immersion Cooling

The Antminer and A9s can both run in immersion cooling environments. Companies like [Elite Mining](#) deploy their A9s into immersion and have good success with it.

Conclusion

Investing in the Equihash mining ecosystem requires some level of conviction in ZCash and Horizen over your investment period. If you think that their privacy improvements will be valuable in a crypto ecosystem that is quickly being targeted by firms like Chainalysis then it may be the right opportunity for you. That being said there is a high risk of government enforcement on privacy coins.

Miners who invested in the Bitmain-Z series and Innosilicon A9 series saw extremely lucrative returns for their capital. It appears that these rigs will continue to make outsized returns and the Z15 will remain one of the best rigs in all PoW.