Lumerin Protocol

White Paper

2021

Last updated: 11/30/2021

Table of Contents

Abstract

Cryptocurrency mining transforms electricity into the hashpower that is necessary for securing Bitcoin and the majority of blockchain networks. This hashpower has therefore become a new class of commodity in all but one very important aspect: it still lacks an effective and transparent means by which it can be bought, sold, and verified as authentic and available. The Titan network introduces a new protocol for provable hashpower. The result is a new blockchain platform for buying, selling, and delivering hashpower globally, creating a tradeable commodity while decentralizing the control of hashing power over time. A single, virtual marketplace gives miners more buyers for their crypto compute power. Companies or individuals with a lower risk profile can now invest and buy/sell compute power providing additional capital and investment for the entire mining industry. And through financial derivatives/futures and services for lending, custody, OTC, and trading, the entire mining ecosystem can achieve higher growth in revenues and investment than ever before.

Background

Hashpower Secures New Network Infrastructure

In 2008, Bitcoin introduced a consensus mechanism known as “Proof-of-Work” (PoW). PoW is a computationally-intensive verification process that secures groups of transactions and other data, known as “blocks.” This process secures most blockchain networks today. Specialists called “miners” perform this task and are incentivized by the cryptocurrency awarded for successfully validating these blocks. PoW creates a very high barrier against network attacks by periodically adjusting the difficulty of the verification process as miners add or remove hashing power to or from the network. As the value of the network grows, more miners are attracted to the system, which also makes it proportionally more difficult to produce a block and gain the rewards therefore the value of the network and the security of the network grow in ratio to one another.

As the Bitcoin network matured, the amount of hashing power required for a miner to remain competitive has grown by a factor of over 10 trillion. Bitcoin’s success sparked interest in blockchain technology and cryptocurrencies, and thus led to the creation of many other PoW networks. Today, blockchain technology is touted as an imminently fundamental part of the global public computing infrastructure.

Source
https://bitcoin.org/bitcoin.pdf
As of this writing, it would cost more than USD $800,000 per hour to attack the Bitcoin network. (Source: Crypto51.app, retrieved 2019-09-06 5:00 p.m. US Eastern Time.)
“FedEx exec: Blockchain will become a foundational layer for everything,” Computerworld, June 11, 2019 (Retrieved Sept 13, 2019)
“The Great Chain of Being Sure About Things,” The Economist, Oct. 31, 2015 (Retrieved Sept 13, 2019)

However, when it comes to mining, two key challenges have emerged:

» **Centralization**: The control of POW hashing power has become centralized in countries or regions with cheap abundant energy — a miner's greatest variable cost — and favorable government regulations.

» **Lack of transparency:** Unlike electricity, the source of hashpower is very difficult to prove. Ironically, the very technology that has redrawn the boundaries for how we think about trust lacks transparency in many important ways. Between miners, pools, cloud providers, and other participants, the source, stability, and provability of mining hashpower remains a black box.
Observers only see the output.

Tokenizing hashpower, and providing a path toward a decentralized protocol for trading it, makes it possible to put much-needed transparency into the mining marketplace. Further, it is also possible to decouple the geographical centralization of hashpower from the control of that hashpower.

Lumerin Project Phases

Lumerin as Marketplace — Managing Hashpower Distribution

Over time, smaller-tier miners will be able to participate in the hashower marketplace, buying and selling it as desired. This will apply to those who do not have any mining devices of their own.

This is how Titan, and our Lumerin Protocol, will mature from managing and shape the future of the Lumerin network.

Lumerin as Protocol — Global Integration of Hashpower and Distribution

With a goal of full decentralization, Lumerin will become a protocol that allows hashpower to be traded, distributed, and monitored on an open trustless network. Lumerin will mitigate the problems caused by mining centralization by moving control of the hashing power onto an open decentralized marketplace and governed by smart contracts.

For the first time, provable ownership and full control over a device's hashpower will not require possession of the device itself. (This is like a landlord owning a plot of land with condos on it but a homeowner owning one of the condos). Similarly, miners will be able to rent the hashpower from devices in such a manner that it is provably theirs.

The balance of this paper will focus on the Marketplace and its implementation at a high level.

Proving Hashpower

For hashpower to be tradeable, market participants must be assured that the hashpower they are buying and selling is real. Providing mathematical proof of the existence of the hashpower in a decentralized, trustless manner is arguably the hardest engineering problem that Titan solves.

The Lumerin roadmap will accomplish this in three stages of progressive decentralization:

Stage 1: Hashrate Oracles

In the first stage, hashrate will be proven by oracles. These oracles host TCP proxy servers, and act as intermediaries between the hashrate provider/seller and the hashrate consumer/buyer. All work being done by a miner would be sent through the proxy, where it will be authenticated and then broadcast to the network (Fig. 1).

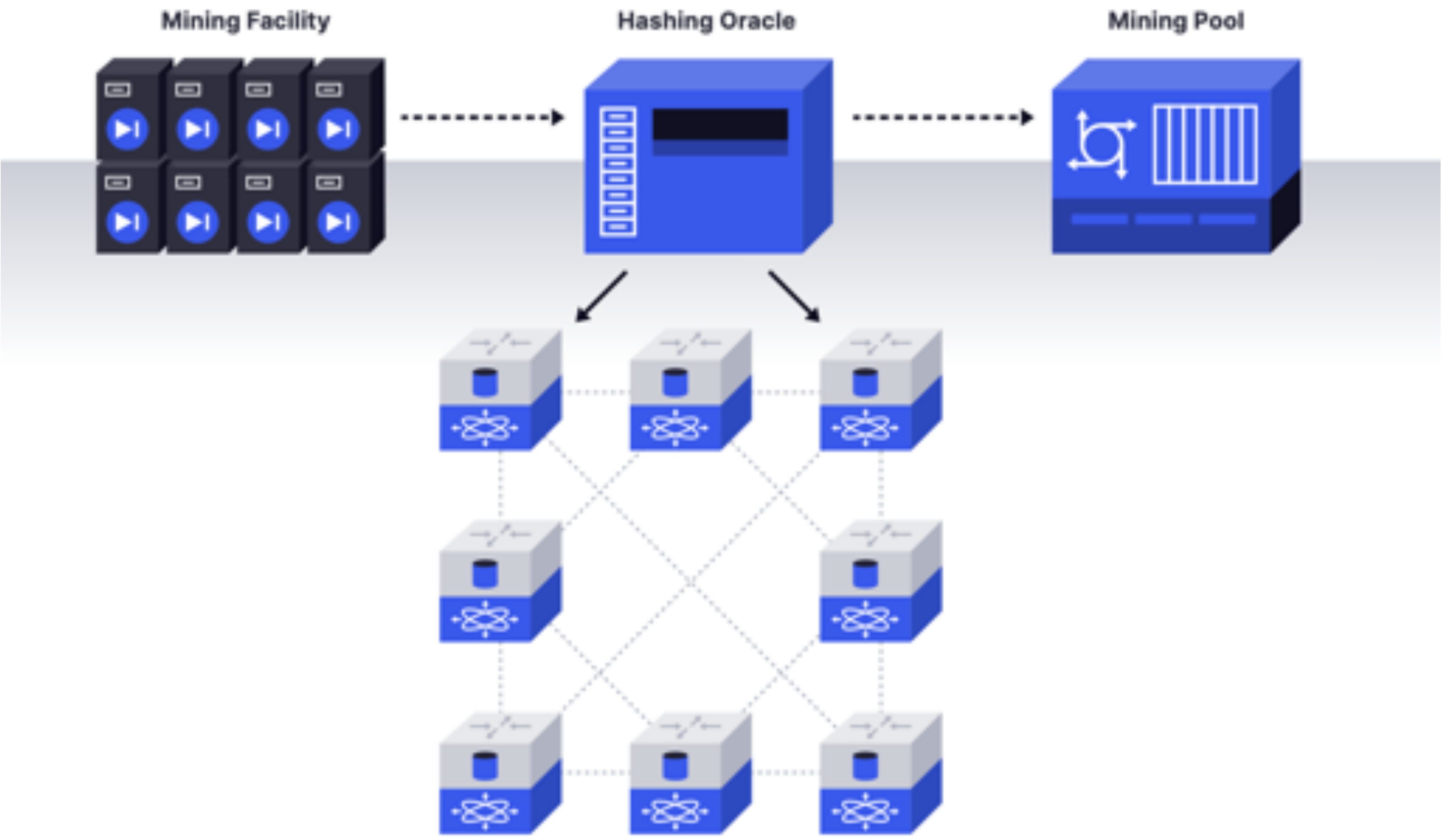

Figure 1: The mining facility sends its work to the hashing oracle, which will verify it and broadcast it to the network.

Stage 2: Staked Hashrate Validators

Stage 2 will move the task of hashrate validation away from a centralized oracle, and distribute it among a federated group of validators. These validators will stake a bounty as collateral to incentivize good behavior. As payment for their services, validators will be entitled to a small fee from each hashing contract they monitor (Fig. 2).

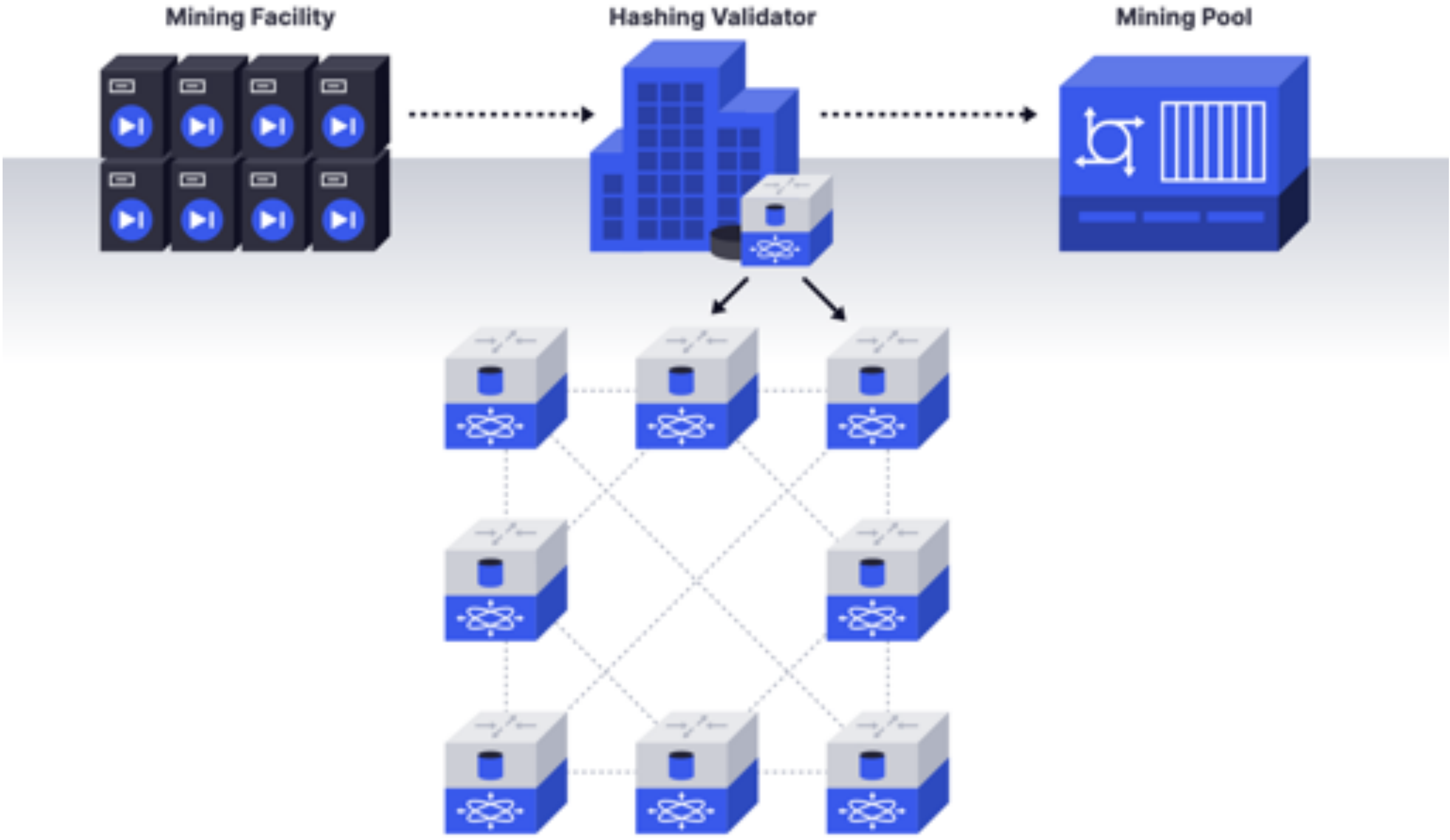

Figure II: Hashing validators will monitor the hashing power coming from the mines, and pass it on to customers.

The validators will need to prove hashing difficulty for each accepted pool share and submit proof of the work completed to the network contract. If it can be proven that a validator has failed or become a bad actor, that validator's stake will be forfeited and divided among the whistleblower and the contract participants. This will allow the network to verify whether validators are fulfilling their duty. The model of validators with stakes should operate in a trustless and provable manner.

Stage 3: Staked TCP Proxy Nodes

At its highest degree of decentralization, each node will independently broadcast its hashing work to the rest of the network. Every share passed through a node to the pool will be verifiable by other nodes (Fig. 3).

After a node submits a share, other nodes will need the following information to verify it:

- Hashing algorithm (e.g., SHA256)
- Difficulty target set by the pool
- Work assigned from the pool
- The share solution submitted by the miner
- A signed message from the pool validating acceptance

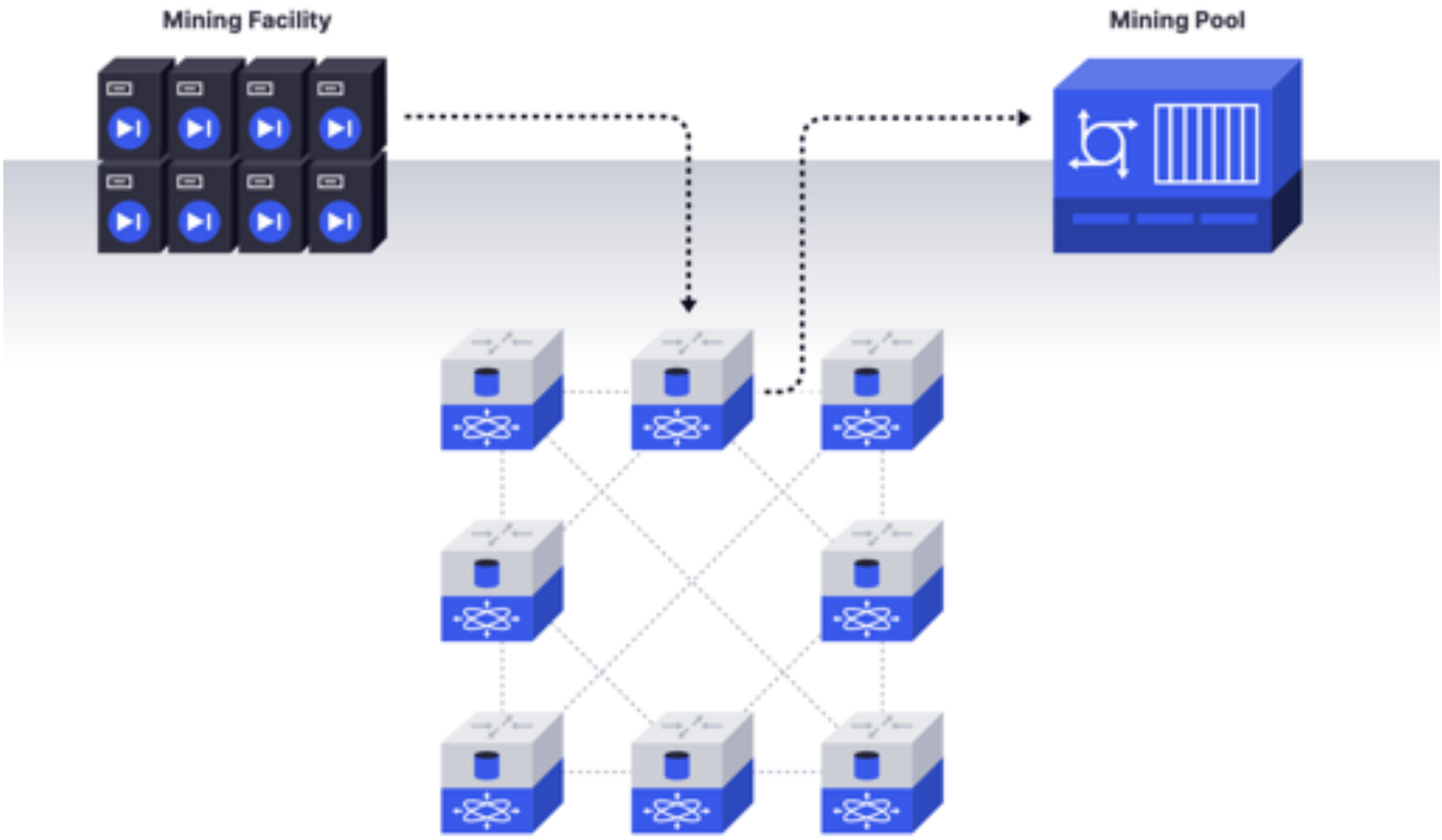

Figure III: At the final, most decentralized stage of hashpower provability, all shares passed through any one node are verifiable by all other nodes.

When all these pieces are known, nodes will be able to verify that the submission they received was valid, above the difficulty target, and accepted by the buyer's pool.

Finally, the system needs a way to penalize bad actors. For example, if a dishonest buyer collaborates with a dishonest pool, the buyer could receive valid shares (which will earn him pool payouts), but broadcast them as rejected to the network (so that he doesn't have to pay for them). To mitigate this attack, each hashing contract in this phase will include a means of staking a bounty from the buyer. This bounty will only be released when the network can verify that the pool received and paid out the declared work.

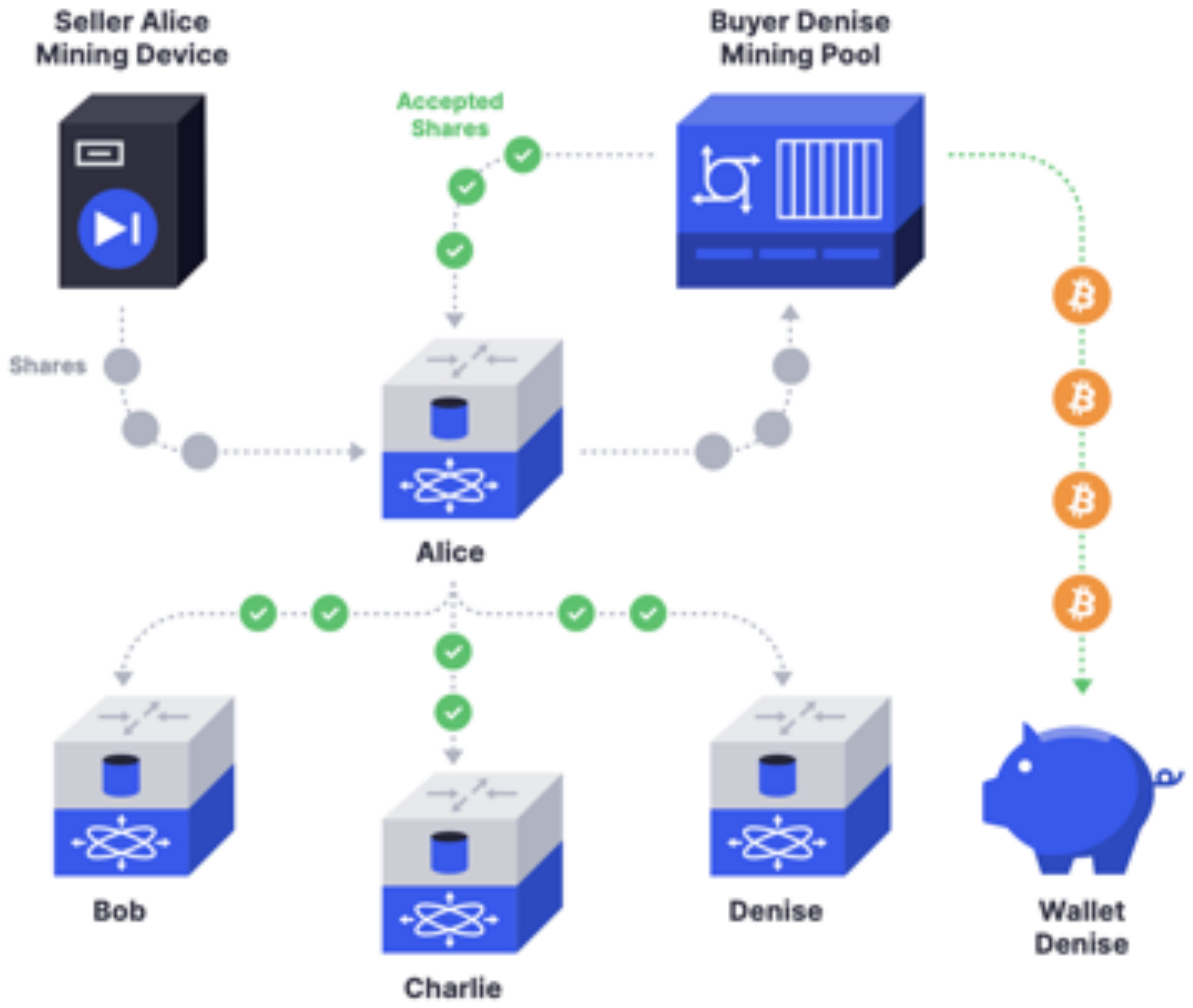

Figure IV: Alice's mining rig finds shares for buyer Denise's pool and broadcasts them to a network. The smart contract validates the submitted and accepted shares and releases Denise's payment to Alice. The pool pays out to Denise.

Pool Participation

The role of mining pools in the Lumerin network requires special consideration.

In order to complete a trustless exchange between buyer and seller, the pool involved in the transaction will need to provide proof to both the buyer and seller that the hashrate was provided and valid. The pool will be able to do this by signing valid shares with a Lumerin private key only known by the pool operator. The pool's Lumerin public key will be saved in the contract when the buyer purchases it. This will ensure that both buyer and seller can verify that the pool listed in the contract both received the hashrate and accepted valid work (Fig. 5).

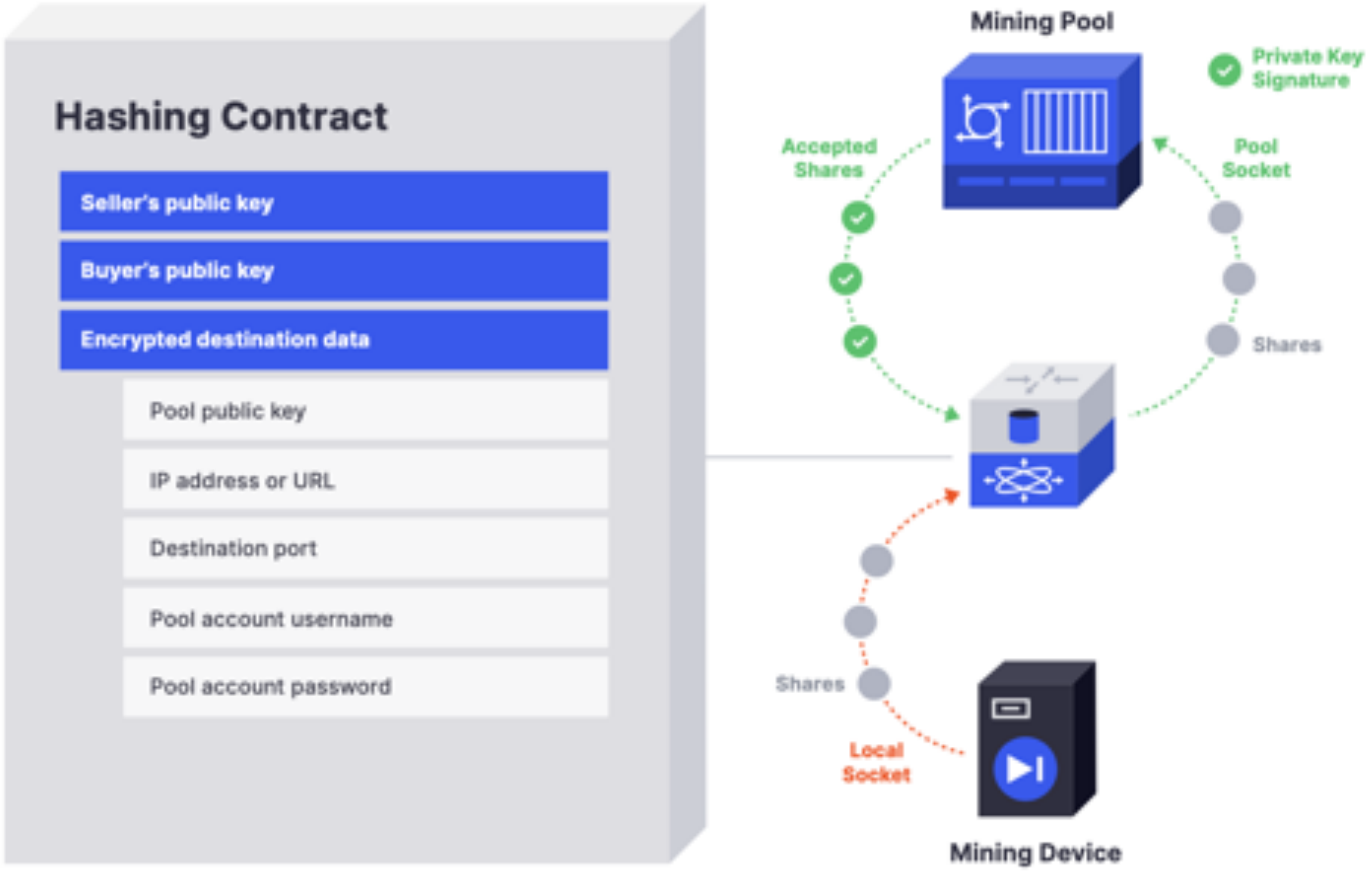

Figure V: Here, a smart contract on the Lumerin network will assure the buyer and seller that the hashrate traded was valid.

Stratum Alterations

To help facilitate the share signature process some minor adjustments may be needed to the stratum protocol. These adjustments may include additional parameters in the pool's share response string. All stratum alterations would need to be done in a way that ensures legacy compatibility.

Risk Assessment and Governance

In order to receive a payout, the seller must supply valid shares to the designated pool. In the event that a pool attempts to cheat the seller by not responding to valid share submissions there should be adequate incentive for the pool to remain trustworthy. While the exact game mechanics of this process will most likely be settled in an iterative and community driven effort it is important to note that there may be a need for a pool registration contract to help facilitate.

A pool registration contract would act as a governance vehicle for listing registered pool information, collecting staked collateral, and settling grievances against bad actors.

Conclusion

The Lumerin Protocol supports a peer-to-peer and decentralized, trustless platform for the buying and selling of mining hashpower as a commodity, essentially a DEX/DeFi for Hashpower. This new commodity, once proveable in a distributed trustless system, can be controlled in a transparent way and even turned into many derivative products that can be bought, sold, and traded through smart contracts.

While the specific game mechanics of this procedure will most likely be determined through an iterative and community-driven process, it is crucial to note that a pool registration contract may be required to help smooth the process.

Legal Disclaimer

The purpose of this preliminary technical whitepaper (Whitepaper) is for information purposes only and may be subject to change or update without notice in the sole and absolute discretion of Lumerin. This Whitepaper is a preliminary concept release intended solely for review and discussion by the blockchain and cryptocurrency communities regarding the technological merits of the potential system outlined herein.

Further, this Whitepaper does not constitute an offer to sell or a solicitation of an offer to buy securities. Any such offer or solicitation will be made only by means of offering materials and in accordance with the terms of all applicable securities and other laws. None of the information presented is intended to form the basis for any investment decision, and no specific recommendations are intended. Lumerin expressly disclaims any and all responsibility for any direct, indirect, consequential or other loss or damage of any kind whatsoever arising directly or indirectly from (i) reliance on any information contained in this presentation, (ii) any error, omission or inaccuracy in any such information or (iii) any action resulting therefrom

This Whitepaper may contain references to third party data and industry publications. As far as we are aware, the information reproduced in this Whitepaper is accurate and the estimates and assumptions contained herein are reasonable. However, we offer no assurances as to the accuracy or completeness of this data. Further, this Whitepaper contains forward-looking statements and there can be no assurances that such statements will prove to be accurate as actual results and future events could differ materially from those anticipated in such statements. Except as required by law, we assume no obligation to update any forward-looking statements or to update the reasons actual results could differ materially from those anticipated in any forward-looking statements, even if new information becomes available in the future

This Whitepaper may also contain projections for consideration purposes only. Any such projections may include forecasts, targeted user acquisition metrics and other predictive statements that represent our assumptions and expectations in light of currently available information. Any such forecasts are based on industry trends, and they involve risks, variables and uncertainties. Our actual performance results may differ from those projected in any such forecasts. Consequently, no guarantee is presented or implied as to the accuracy of any specific forecasts, projections or predictive statements contained therein.