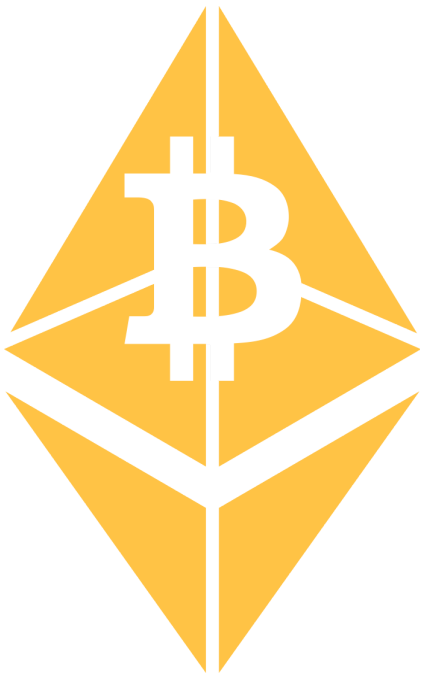


BITHEREUM

Two Chains, One Coin

Sachit Singh, Scott Wade, Dondrey Taylor

June 2018

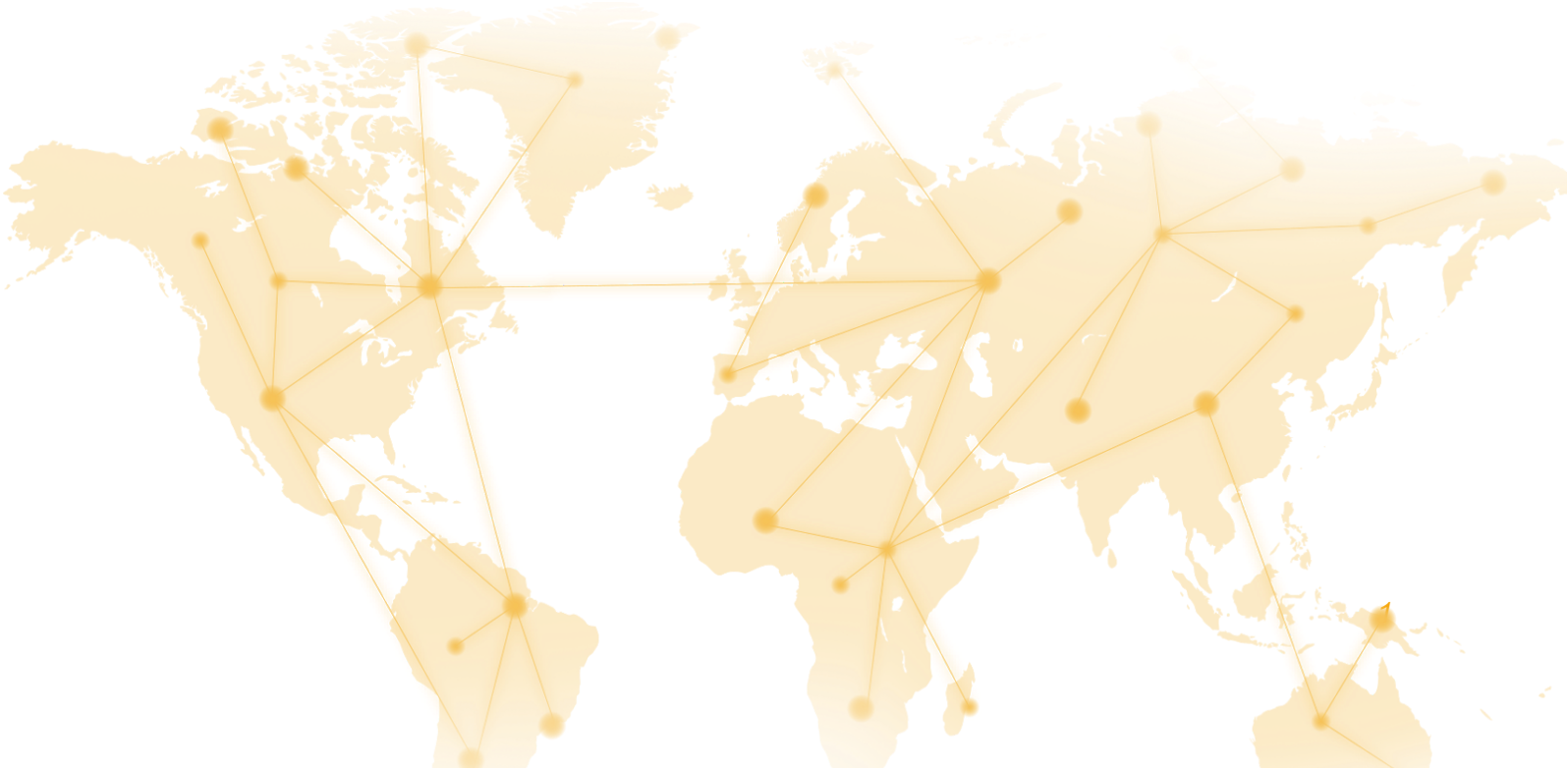


Table of Contents

1. *ABSTRACT*

Bithereum (BTH) is a coin that is created via forking the Bitcoin (BTC) blockchain. BTH will function as a peer-to-peer (P2P) electronic cash system similar to BTC, however it will fuse with the technological roadmap of Ethereum (ETH) to create a more advanced platform which is structured around Proof of Stake (PoS). BTH is a coin that will bring together the best aspects of all prior BTC forks, while also revolutionizing Bitcoin mining. Bithereum addresses the pain points that are prevalent in both of these past forks and also aims to implement a PoS mining model which would result in increased network security and lower equilibrium transaction fees, essentially making them insignificant in the long-run. This in turn would both increase the competitiveness of Bitcoin relative to other cryptos while also positively impacting Ethereum and lessening the excessive sell pressure, allowing that to focus on its entire ecosystem rather than A to B transactions.

2. INTRODUCTION

As the cryptocurrency industry has grown tremendously over the past year, the two leading currencies have both experienced their fair share of growing pains. To start, BTC which has long been touted as the most superior P2P currency, has seen it's networks slow down significantly in lieu of the major price upswing seen at the end of 2017. These points of inefficiency have not been addressed by the core development team and have resulted in a further divide in the community, resulting in numerous forks of the chain. Blockchain is built behind the idea of a consensus network, but the lack of this in BTC has resulted in a mining war for the foreseeable future. Bitcoin Cash and Bitcoin Gold have attempted to improve on multiple different issues that are present with Bitcoin, but in doing so, they've ignored other issues.

On the other side of the spectrum, ETH has experienced its own unique set of issues. Though it has benefitted from a boom in its ecosystem with the massive influx of dApps, ICO's have also acted as an anchor, weighing down ETH from its true value because of constant sell pressure. Although ICO's are a revolutionary way to raise capital for projects, ETH was designed to be used as a "fuel" on its platform, and not a P2P transactable coin. This may be a negative factor currently, however the technology of Ethereum remains stronger than ever. Transactions currently process at a rate of 15 times per second while transaction fees are insignificant in comparison to BTC.[1] In addition, the robust roadmap laid out by Vitalik Buterin points towards "Visa-scale transaction capacity", or up to 1000 transactions per second while simultaneously upgrading the Proof of Work model to Proof of Stake.[2] As of 6/3/18, Vitalik is confident Ethereum can scale to 1,000,000 transactions per second through various on-chain and off-chain implementations.[3] This proves the technological prowess inherent in ETH that puts it ahead of Bitcoin in terms of efficiency.

[1] https://www.coindesk.com/information/will-ethereum-scale/
[2] https://techcrunch.com/2017/09/18/ethereum-will-replace-visa-in-a-couple-of-years-says-founder/
[3] https://cryptoslate.com/vitalik-buterin-sharding-and-plasma-to-help-ethereum-reach-1-million-transactions-per-second/

The current form of consensus and transaction validation is known as Proof of Work (PoW), which was applied to Bitcoin by Satoshi during its inception in 2008. PoW is a requirement that mining be performed in order to verify groups of trustless transactions on the blockchain. With Proof of Work, the probability of mining a block depends on the work done by the miner. Though it has plenty of benefits, the PoW model also has a major downside: the exorbitant electricity costs and high computing power hardware that is necessary to profit. An alternative validation method known as Proof of Stake, first used by Peercoin in 2012, was birthed as a solution to these issues plaguing mining and has provided a cheaper and greener form of consensus. At its core, Proof of Stake is defined as a form of proof of ownership of the currency. The critical difference between the two forms of consensus is that with PoW, the probability of mining a block depends on the work done by the miner, while with PoS, the resource of importance is the amount of coins a miner holds. An inclusion of this technology into BTC would finally put it on par with the constantly evolving characteristics of Ethereum and the upcoming implementation of Casper.

Enter Bithereum, a coin that will function as a P2P currency similar to BTC, however it will fuse with the technological roadmap of Ethereum to create a more technologically advanced platform which is structured around Proof of Stake. BTH will incorporate Segregated Witness to increase network capacity, while also being mined via GPU mining as a PoW model, eventually transitioning into a full Proof of Stake model which would propel the original idea of BTC towards a groundbreaking technological upgrade that was previously unimaginable. PoS will essentially bring BTH leaps ahead of what BTC is and put it on the technological grounds of Ethereum while still functioning solely as a P2P currency. BTH will be redeemable by both BTC and ETH holders; the total supply of 31 million accounts for the additional coins that will be redeemable by all ETH holders at the ETH:BTC ratio at the time of the snapshot.

3. PROBLEM

Scalability

Bitcoin, throughout its 9 year life, has seen a particular issue gradually grow more and more glaring, to the point that the discussion of its solution has become inevitable amongst the community over the last year. This issue is scalability. When BTC was released in 2009, its ethos centered around speed, ease, and cheapness in transacting across borders. As traffic and volume has increased substantially over time, these three features of the coin have become a far cry from what they originally were. Transactions on BTC are currently processed at an average rate of 4 transactions per second, dragging the time to complete the transaction up to 3 days.[4] In relation to this, transaction costs have also skyrocketed; people have seen up to $19 fees for a single transaction.[5]

For being the progenitor of cryptocurrencies along with the most valuable, BTC has fell behind many other coins in terms of functionality. The core team has failed to integrate any meaningful updates to the block size, and the networks continue to be clogged. Many developers believe that BTC has

[4] https://blockchain.info/charts/transactions-per-second?timespan=30days
[5] https://bitinfocharts.com/comparison/bitcoin-transactionfees.html

become a store of value comparable to gold, rather than the easily-transactable P2P currency as it was once believed to be. Consequently, a group of developers decided they had enough with the excessive fees and slow speeds, and ultimately created Bitcoin Cash as a solution in August 2017. They achieved this solution by expanding the block size from 1MB to 8MB, an attempt at reducing the network congestion.

The results have spoken for themselves thus far: as of November 23rd, 2017, average BTC transaction fees were around $6.18, while average BCH transactions costed only 19 cents.[6] In addition, at the time of this writing, BTC is facing a backlog of 216,870 unconfirmed transactions.[7] These fees only continued to increase through the next month and reached a peak in December when BTC reached its all-time high in price. Suddenly, following mid-December, both the fees and amount of transactions per day began drastically reducing. At Deconomy in early April, Roger Ver provided a chart during his presentation that showed BTC usage rising linearly, but then falling after hitting the 1MB limit and losing out on projected adoption beyond that limit.[8] This can be further substantiated by looking at multiple different BTC charts. On 12/13/18, there were 490,644 confirmed transactions in the day as BTC was approaching its all-time high of around $20K. By 4/7/18 however, the amount of confirmed transactions in the day had dropped to 138,535. This shows that over three times the transactions were taking place in December, when fees also hit their ATH, compared to months later. Furthermore, the costs per transaction went from as high as $162 on 12/25/17, down to $71 on 4/8/18.

It would seem that many people have moved away from the BTC network due to the unreasonably high fees and transaction backlogs that had been reached by BTC's peak in price, and a multitude of examples have supported this theory. For example, according to CoinDesk, Payment processor Stripe stopped accepting bitcoin in January payments due to the high fees, and BitPay, a startup that offers payment services over Bitcoin has differentiated into supporting multiple protocols for its merchants.[9] Steam also stopped accepting BTC in December for the same reasons. Samson Mow, who opposes Roger Ver's beliefs in regards to block size, has stated "I don't think block size limits impede usage. If you go to a restaurant and it's full, you wait".[10] This is not a sound assumption to go by, as Vitalik pointed out, in that one would many times just go to a different restaurant if its too full, which is an analogy comparable to what has been happening with the decreasing usage of the BTC network.

While BTC has remained idle through these issues, other currencies have risen to the occasion and have prioritized scalability. Ethereum has actively been working on scaling through its Raiden Network, while Dash has experimented with increased block sizes for a true on-chain scaling solution. It is quite plausible that BTC can eventually lose its spot as the top cryptocurrency if they don't find a way to scale.

[6] https://seekingalpha.com/article/4128248-bitcoin-vs-bitcoin-cash-bitcoins-civil-war
[7] https://blockchain.info/unconfirmed-transactions
[8] https://twitter.com/VitalikButerin/status/981078979191844865
[9] https://www.coindesk.com/bitcoin-low-fees-why-happening-why-matters/
[10] https://twitter.com/VitalikButerin/status/981091104928837632

Community Schism

As the issues around BTC scaling have exacerbated over the last few months, the community has consequently seen a deep ideological divide form. Due to the long-standing issue of scaling, many users have wrestled over how to solve the issue. The debate about this has resulted in multiple factions who each view the opposing argument as incompetent. This personal infighting was previously unimaginable, as the group that developed this world-changing technology years ago were always viewed as tight-knit. Now, there is a firm argument between two major sides: should BTC be used for daily payments on everyday items or should BTC basically function as a store of value like digital gold?[11] Both sides of the argument sport opposing Reddit forums where they often lash out at each other and spread fear, uncertainty, and doubt. Due to the fact that BTC has no leader, the only ones with the power to bring about change are the miners. Many of the miners, who used to center around the Core team due to trust, have lost faith. These various examples of the community schism have manifested themselves in multiple ways over the last year, specifically in the form of hard-forks.

Recently, two groups formed a coalition together, headed by CEOs including Jihan Wu, Mike Belshe, Jeff Garzik and more to solve the issue through a hard-fork, however their stance directly competed with the stance of BTC's main developers. This fork was known as Segwit2x and it was meant to create two competing chains, ultimately overtaking the original chain and becoming the dominant coin. This effort completely fell apart in the recent weeks due to a lack of consensus; specifically, this fork failed to obtain acceptance from all but 15% of the BTC community.[12] The lead developer of Segwit2x, subsequently released a statement explaining that the current path of action would further divide the community and that it would cause an overall setback to BTC's growth. This solution of an increased block size therefore remained unsolved on the main chain and other forks of BTC began to gain substantial traction.

The two forks of BTC that have gained prominence are Bitcoin Cash (BCH) and Bitcoin Gold (BTG). BCH immediately raised the block size limit to 8MB as part of a massive on-chain scaling approach, resulting in low fees and fast confirmations versus BTC users having to wait up to days for confirmations[13]. Though BCH improved these aspects, they have not addressed the monopoly that the dominant ASICs have over mining. On the other hand, BTG has focused solely on the democratization of mining but have kept the block size identical to BTC, which fails to address high transaction fees and clogged networks. Though they each improved on a specific area of weakness within BTC, they failed to address more than one major issue.

The growing issue of the deep ideological divide within the BTC community reared its head again at Deconomy on April 3rd, 2018. This particular confrontation manifested during a question-and-answer segment following a panel called "Bitcoin, Controversy over Principle", featuring Roger Ver, Craig

---

[11] http://www.slate.com/articles/technology/future_tense/2017/06/internal_conflict_could_split_bitcoin_in_half.html

[12] https://www.forbes.com/sites/laurashin/2017/11/08/bitcoin-hard-fork-called-off-averting-major-disruptions-and-turbulence-in-cryptocurrency/#4826f4375303

[13] https://www.bitcoincash.org/#about

Wright, and Samson Mow.[14] This session was live-tweeted by Vitalik Buterin, along with his own technical critiques of the discussion. At a certain point in the panel, Roger Ver indirectly called out the BTC core team by asking "What would I do if I wanted to stop bitcoin? Advocate for 1 MB blocks to intentionally create high fees, slow confirmations, unreliable transactions".[15]

Roger Ver, a prominent figure in BCH, has showed his opposition to the 1MB block size for quite some time. On the other hand, Samson Mow, the CEO of Blockstream and advocate of Lightning Network and SegWit, is more in-line with the BTC core vision and believes in scaling via sidechains rather than increasing the block size. The conversation between Ver and Mow was the epitome of the ideological divide, as Ver states that BTC's approach to scaling has resulted in greatly lost adoption. Samson, conversely, believes that BCH's approach of increasing the block size is a dead end rather than a long-term solution. By the end of the discussion, the conversation began moving towards the clear animosity between both parties. Roger Ver explained that the reason for this is that the core BTC devs have shifted the vision of the project in a disagreeable way, specifically referring to its current use as a "store of value" rather than the peer-to-peer payment system it was created to be, to which Vitalik agreed with. He also stated that the core devs belittled and censored those with opposing opinions from them, further spiraling the animosity beyond fixing. Samson then responded and attacked BCH for giving their coin that name, all the while ironically saying that there no longer needs to be any animosity. All in all, this panel session has showed that there has been little improvement in the discourse between the two parties, and that the divide remains as deep as ever.

Proof-of-Work and the Rise of the Mining Cartel

The current transaction validation method for Bitcoin is Proof of Work, which essentially means that machines, called miners, burn electricity to solve complex cryptographic puzzles in order to create blocks and validate transactions. All miners are competing against each other to be the first one to solve the problem, and the miner who solves it first gets to create the new block and gets rewarded in newly minted Bitcoin for their efforts. All of the other nodes verify this new block to make sure it's legitimate and follows protocol. If this is the case, the new block gets confirmed and the process repeats itself for the next block. If it turns out the new block is illegitimate, the block becomes invalid, and the miner who created the block receives zero reward.

The more mining and hashpower that a blockchain has in PoW increases the difficulty which makes the network more secure by making it harder to try and cheat the network. There are economic incentives in place to encourage anyone in the world to mine and secure the network, which means there is no central point of failure. However, there are factors that are currently plaguing the Bitcoin PoW model which can be detrimental to the long term security of the network.

First let us discuss the creation of high powered miners that utilize Application-Specific Integrated Circuits (ASICs). The algorithm that was chosen by Satoshi Nakamoto to run the PoW model is known as SHA256, which provides anyone with a CPU or GPU, which are found in almost every common computer, the ability to participate in mining. These ASICs miners were then created to

[14] http://www.businessinsider.com/ethereum-founder-vitalik-buterin-calls-supposed-bitcoin-inventor-craig-wright-a-fraud-2018-4
[15] https://twitter.com/VitalikButerin/status/981077602294050818

perform the algorithm exponentially faster, giving one of these miners a tremendously higher chance of creating the next block, basically rendering all other miners obsolete. On one hand, you can look at this as a fair technological advancement, but on the other hand the use of these leads down a rocky road, leading to an unfavorable destination.

This leaves individuals without an ASIC miner with two choices. The first choice would be to purchase an ASIC machine, which can be purchased on average for $1500, not taking into account the power supply and replacement costs for when the chips burn out. Data from a study done in August 2017 shows the profitability numbers for an Antminer S9. At an exchange rate of $11,180.47 USD/BTC, an Antminer S9 would only generate around $757.63 per month, while factoring in energy costs and pool fees.[16] Thus, the total amount generated in one year would be $9,091.56, however after taking out the initial expense of the mining rig and power supply, this total is reduced to about $7,476.56. Furthermore, higher powered machines are constantly being introduced as well which would require an individual to upgrade in just a few months time to keep up. These upfront costs would be enough of a deterrent for an average individual to mine other coins.

The second choice would be to join a mining pool. Mining pools were designed for miners to combine their hashpower, giving the pools a greater chance of creating the next block, then the rewards are split up amongst the pool based on how much hashpower each miner is contributing. This seems like the logical choice, however it's a catch-22, because as mining pools get bigger and their hashrate increases, new miners who join the fray are incentivized to join the pools with a lot of hashpower to increase their odds of creating new blocks. The hashrate then starts to condense into fewer and fewer pools, to the point where currently for Bitcoin 61% of the hashrate is attributed to just 4 mining pools.[17]

Keep in mind that mining pools are controlled by someone or an entity, and when you join a pool you allow that entity to control your hashpower. That means that 4 entities have control of 61% of the hashpower in Bitcoin, which we referred to as the Mining Cartel. As of June 23, 2018, the situation has turned far more alarming as it has been confirmed that Bitmain alone controls nearly 42% of the network hashrate[18]. In addition, they also control about 20% of the hashrate for BCH, which shares the same algorithm as BTC; if these miners were to be switched onto the BTC network, the ensuing results could have grave implications for the coin.

This is an issue because it only takes 51% hashpower to essentially take control of the network, called a 51% attack.[19] If these mining pools decided to team together to form a monopoly, they would have the power to decide which transactions get approved, and could allow their own coins to be spent multiple times. If they maintained this control, confidence in Bitcoin would plummet and the purchasing power would collapse.[20] As a result, these mining pools have the ability to consolidate all of the power amongst them to the point that they are consistently able to manipulate price, fees, and even voting in the community.

[16] https://99bitcoins.com/bitcoin-mining-profitable-beginners-explanation/
[17] https://blockchain.info/pools
[18] https://www.trustnodes.com/2018/06/23/bitmain-nears-51-bitcoins-network-hashrate
[19] https://learncryptography.com/cryptocurrency/51-attack
[20] https://en.bitcoin.it/wiki/Proof_of_Stake

The biggest defense of this issue is that the large mining pools have no incentive to deliberately attack/manipulate the network because then Bitcoin would lose its value to the point that it's worthless, and all of the electricity/energy consumed to maintain the network would have gone to waste. However true this may be, the fact of the matter is that we're leaving the network up to 4 entities, trusting that they have the best interest of the network in mind at all times. This completely defeats the purpose of creating a network that was meant to be trustless and decentralized. As much as we like to think that the ones in control are acting favorably, history has proven us otherwise.

These types of 51% attacks have actually begun occuring starting in May 2018 and have become far less costly to execute than ever before. The primary target of 51% attacks are small to mid-level market cap coins because of the fact that many of them share similar hash algorithms, allowing big mining pools to switch their efforts over to hijack another chain temporarily and execute double spend attacks via exchanges. For years, this issue has been foreseen however it has always been believed to be too costly due to the barriers of entry inherent in mining. The barriers of entry centered around purchasing miners, setting up a farm, along with all of the logistics involved, ultimately feeding into the perception that it's simply too expensive and to do so. But, over the last year, there have been many new PoW coins that have emerged which share similar hash algorithms but have far less total hash power than the biggest coins, creating clear vulnerabilities[21]. In addition, to further exacerbate the issue, cloud mining marketplaces such as NiceHash have begun gaining an immense amount of traction, allowing anyone to buy/rent hashing power through NiceHash's platform. These attacks can now be conducted at a fraction of the costs as before, and malicious parties have wasted no time in taking advantage of the situation.

As of June 8, 2018, a handful of coins have already been attacked including Monacoin, Bitcoin Gold, Zencash, Verge, and Litecoin Cash[22].The most common algorithm that has been targeted as of late is equihash, as this is the algorithm used by ZCash along with many forks which also utilize GPU mining. Attackers have been able to take over 51% of the total hash power of these coins for a brief time period and rearrange transactions and blocks so that they could do double spend attacks and cash out through exchanges with high liquidity. Exchanges initially only required five confirmations when the BTG attack took place, allowing the attacker to send two massive transactions to the exchange totaling to around $18 million of BTG. As a response, exchanges have been increasing the amount of confirmations required to make the funds harder to steal in this type of attack.

To add another layer of complexity to this issue and issue of the mining cartel as a whole, is Bitmain's release of a new ASIC Antminer z9, to be used to mine on Equihash[23]. These ASICs would directly stifle the GPU mining of many coins, and essentially to these coins what ASICs did to Bitcoin, once again centralizing the mining efforts. These ASICs can also further worsen the situation regarding 51% attacks and make it even easier for small parties to hijack a network.

Another direct consequence of the rise of advanced and costly miners has been the massive spike in energy consumption. For example, a recent finding states that one BTC transaction required the

[21] https://medium.com/@HusamABBOUD/the-realistic-lucrative-case-of-ethereum-classic-attack-with-1mm-today-8fa0430a7c25
[22] https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular/
[23] https://www.coinbureau.com/mining/battle-against-asics-antminer-z9-zcash/

same amount of electricity as powering nine American households for one day. By February 2020, studies show that BTC transactions may end up consuming as much electricity as Denmark.[24] These expenses have caused mining by individuals to become unprofitable, while those with the most-costly ASICs miners and largest plants have monopolized mining profits.

Furthermore, there is also the issue with Bitcoin's current PoW model in that it will eventually come across an economic problem called Tragedy of the Commons.[25] This is a market failure scenario where a common good is produced in lower quantities than the public desires, or consumed in greater quantities than desired. Bitcoin will come across this issue in the future when block rewards for mining approach near zero, in which miners will only be rewarded in transaction fees. At this point, users will pay lower and lower fees because they know that miners will have to accept anything in order to profit from mining blocks. It's likely that the incentives for mining will be so drastically reduced that it won't even be worth it based on the energy consumption and miner participation will diminish. This will cause for lower difficulty, and the network security will severely drop. Although this won't be a concern until the future, this is something we must prepare for.

BTG came along a few months ago with a proposition of democratizing mining to fulfill the initial vision of Satoshi Nakamoto's "one CPU, one vote" mantra.[26] BTG essentially aimed to add more people into the mining pie. Though these ideas certainly address multiple issues with BTC, they fail to encompass more than one major issue respectively, let alone add further value and innovation to the chain, ultimately pushing it further behind Ethereum technologically.

4. SOLUTION

Proof of Stake

We've discussed the many issues of the current PoW model and here we will explain why implementing a Proof of Stake model based on Ethereum's Casper protocol will positively impact the long term success of Bithereum. Proof of Stake was discussed among Bitcoin circles on forums as early as 2011.[27]At its core, PoS is a consensus algorithm in which the creator of a new block is selected based on the amount of currency they have staked. The critical difference between the two forms of consensus is that with Proof of Work, the probability of mining a block depends on the work done by the miner, while with PoS, the resource of importance is the amount of coins a miner stakes.

This means block creation isn't dependent on miners racing to solve a complex cryptographic puzzle burning energy in the process, but instead they are selected in a random, nondeterministic way based on how much currency they have staked. These miners are known as validators, and get to

[24] https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/
[25] https://en.bitcoin.it/wiki/Tragedy_of_the_Commons
[26] https://btcgpu.org/wp-content/uploads/2017/10/BitcoinGold-Roadmap.pdf
[27] https://peercoin.net/assets/paper/peercoin-paper.pdf

vote on the creation of new blocks and get rewarded in proportion to how much they have staked.[28] Major benefits come from PoS which are reduced energy consumption, reduced risks of centralization, increased network security, lower equilibrium transaction fees, and increased transaction speed.

This method drastically reduces energy consumption and the need for expensive mining hardware. Since all miners won't be racing to create each block, energy will only be consumed by the validators who get selected. Under current PoW, you can be burning energy to mine and never receive a reward if your machine is obsolete or you aren't in a mining pool. Then, instead of miners needing to upgrade to more expensive machines to compete, they can reinvest the rewards for further staking or use the money saved/earned on processors that will increase transaction speed.

In PoS, your influence on the network is dependent on how much you have staked, so in order for an individual or an entity to control the network, they would need to have at least 51% of all staked coins. Currently the Bitcoin wallet with the most coins has 169,321 BTC, which is less than 1% of the max supply.[29] The probability of someone or entity or cartel to obtain 51% of all coins is infinitesimal. Although possible, it's exponentially more expensive than obtaining 51% hashpower in PoW, thus increasing network security and reducing the risk of centralization.

Another benefit of PoS is lower equilibrium transaction fees. In PoW, transaction fees are based on the miner's electricity costs, mining equipment depreciation, mining labor, and a market rate of return on mining capital, and miners will elect to add the transactions to blocks that have fees to where they profit. The more miners in the fray, the higher the difficulty, the more hashpower required, the more electricity burned, the higher the fee. In PoS, transaction fees will only be needed to compensate labor involved in maintaining bandwidth and storage space, meaning fees will be exceptionally low. This will yield especially beneficial to the Tragedy of Commons problem the current PoW model will face, since validators won't be disincentivized to participate due to the negligible costs required.

There is however a caveat in PoS that Ethereum addresses with their Casper protocol and its slashing conditions. In most PoS models, there are only rewards for validators creating new blocks, without any penalties. This creates the "nothing at stake" problem.[30] This problem essentially means that while validating blocks, there might be multiple competing blocks and instead of choosing one, the validator will decide to approve all of them just to be sure. This can cause a chain reaction of multiple forks stemming off the main chain, making it hard to determine what the real chain is. Enter slashing conditions, which are created to ensure that validators act in line with protocol or else their stake will be "slashed" and they lose their staked coins. Since no one wants to lose their staked coins, they will act in line with the protocol and be forced to only vote the block they think is accurate. With slashing conditions, this PoS model follows Nash equilibrium principles since based on all possible outcomes, the optimal decision is to behave benevolently.

All in all, Proof of Stake is a transaction validation method that will make the network faster, more efficient, cheaper to run, and more secure. It eliminates the need for expensive hardware, mitigates

[28] https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs#what-is-weak-subjectivity
[29] https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html
[30] https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs#what-is-the-nothing-at-stake-problem-and-how-can-it-be-fixed

high energy costs, prevents both ASICs/large pools from dominating, and increases the network security from 51% attacks. Issues faced in common PoS protocols are alleviated through Ethereum's Casper protocol and its slashing conditions. With this implemented into Bithereum, the benefits of this technology will positively affect Bitcoin's issues and ensure its long term success.

GPU Mining

Though Proof of Stake will take some time to implement, even in the case of Ethereum, it is on the horizon of completion. Bithereum, however, will begin mining prior to its completion through a Proof of Work algorithm known as Equihash. This democratized method of mining places Bithereum in an optimal position to shift into Proof of Stake while benefiting its early miners with additional coins to stake for when the model is implemented.

Satoshi's original vision of "one-CPU-one-vote" has been lost in the PoW mining model, and has basically turned into a "one-ASIC-one-vote" system.[31] Equihash, a newer PoW algorithm, is a direct solution to this issue as it strongly resists ASIC mining. Zcash founder Zooko Wilcox and engineer Jack Grigg define Equihash as "a memory-oriented Proof-of-Work, which means how much mining you can do is mostly determined by how much RAM you have".[32] Furthermore, they stated their doubt in whether anyone will ever be able to build cost-effective ASICs miners, thus furthering the benefits of Equihash.

The main benefit of this algorithm is that it can be solved the most efficiently through GPUs rather than physical mining rigs. GPUs are used by the majority of the society as they have become mainstream over the last few decades. This brings the mining process into the hands of any individual with a GPU; anyone with a graphics card would be able to mine BTH using just their home computer and smartphone hardware. This is because the algorithm itself is a memory-hard problem, meaning that general home computers with a surplus of memory are far more suited for the task than specialized hardware chips.

Once the developments for Proof of Stake are complete, the model will be implemented into BTH and mining will shift out of Equihash. All miners who had been performing GPU mining will then immediately have the ability to stake the BTH coins they have mined thus far. This would give them a further advantage over regular BTH holders, as they would have more to stake. GPU mining is the perfect segway into Proof of Stake due to the already democratized structure.

Segregated Witness

One of the most concerning issues with Bitcoin, Ethereum, and all cryptocurrencies for mainstream adoption is scalability. As more and more people use the network and initiate transactions, the

[31] Tasca, Paolo, et al. "Misunderstanding the Threats ." Banking Beyond Banks and Money: A Guide to Banking Services in the Twenty-First Century, Springer, 2016.
[32] https://bitcoinmagazine.com/articles/how-equihash-algorithm-could-democratize-zcash-mining/

network gets clogged with the large influx of transactions. At its current state, Bitcoin is not equipped to handle these large volumes of transactions, and with the goal to be a globally used peer-to-peer form of payment, it falls short. One way to help scale the network is incorporating Segregated Witness.

Each block contains data about the hash from the previous block, i.e. the sender and receiver's public keys, and a time signature. As more transactions are processed, the blocks become data heavy and become clogged. Segregated Witness is a protocol that essentially breaks down each block into two parts. The original part contains the sender and receiver information, and the extended part contains all other data including the hash and signature. This allows for more data and transactions to be stored in each block.

Bitcoin implemented Segwit in August of 2017, which Bitcoin Cash refused to do. Segregated Witness allows for layer two solutions to be implemented, such as Lightning Network, however Bitcoin Cash solely believes in on-chain scaling solutions, rather than using a combination.

SegWit2x has been proposed by the Bitcoin community but ultimately couldn't be implemented due to a lack of consensus. Whereas SegWit is a soft fork and is compatible with the current chain, SegWit2x is a hard fork that is not backwards compatible and would need all of the miners and the nodes to update to the new protocol. SegWit2x is the same as SegWit, breaking down the block into two parts, however it also increases the block size from 1MB to 2MB, allowing even more data to be stored in each block.[33]

Lightning Network

Due to the computing power necessary to validate transactions, it is clear that this process is in need of an improvement. Lightning Network is another protocol co-designed by Joseph Poon, who is also working on Plasma with Vitalik Buterin to help solve the scalability issue for Ethereum. To summarize, Lightning Network sets out to increase transaction speed by moving transactions off the main chain into channels which report back to the main chain periodically.[34]

Each peer would have a private payment channel between them and each of the peers they transact with. In addition, each peer would have one channel open to the Bitcoin network in order to broadcast the final transaction to the blockchain. Miners would then have far less transactions to confirm than they currently do, freeing up the congested network as a result. The blockchain would no longer have every single transaction posted, as only the final results between peers would be recorded. The data limit issue would be mitigated, especially with the addition of Segregated Witness, and data will be stored into the blocks with more efficiency. The speed gains that would be attained by cutting out the middle-man of mining rigs/digital wallets would allow BTC to "be used at retail point-of-sale terminals, with user device-to-device transactions, or anywhere instant payments are needed", according to developers of the network.[35]

[33] https://thenextweb.com/contributors/2017/09/13/fork-segwit-everything-need-know-bitcoin-scaling/
[34] https://cointelegraph.com/explained/lightning-network-explained
[35] https://www.investopedia.com/news/bitcoin-lightning-network/

This process is analogous to opening a tab at bar. Throughout the night as you order drinks, each transaction gets recorded locally. Once you close out your tab, all of the transactions get added up and you pay one transaction. So with the Lightning Network, two parties can make transactions off-chain which will then get added to the main chain when they are done conducting trades (closing out the bar tab). This will clear up more space allowing a greater amount of data to be stored on each block, reducing transaction times while also lowering transaction costs.

As of 12/6/17, the completion of version 1.0 RC of the Lightning Network protocol has been announced with mainnet Beta implementations on the horizon. The tests performed thus far have yielded positive results and have reaffirmed the protocol's ability to instantly transact payments. Elizabeth Stark, the CEO of Lightning Labs, has indicated that this scaling solution will be ready for widespread usage sometime in 2018.[36]

On 3/15/18, Lightning Network beta was official launched on mainnet, and was a huge accomplishment for everyone involved. As of April 10th, 2018, there are 1,725 nodes operating on the network, with over 5,800 channels, and a network capacity of almost 14 BTC in total.[37] The network has rapidly grown stronger since its mainnet launch and we will closely be following it's progression to mainstream adoption.

There's no doubt that both on-chain and off-chain scaling solutions will both be needed to scale for worldwide usage. Ethereum's plan to implement both will allow it to achieve 1,000,000 transactions per second according to studies.

5. IMPLEMENTATION

Proof of Stake (Casper)

We've discussed the many benefits of Proof of Stake consensus, specifically Ethereum's Casper protocol, and will implement a Casper-like protocol atop a modified version of Bitcoin.

Ethereum's Casper FFG (Friendly Finality Gadget) at its core creates a structure in the mining network that rewards miners who stay in line with the protocol while imposing harsh punishments to miners that choose to carry out nefarious actions.[38] In Casper, the mining process starts with nodes called validators, which each stake a portion of their ETH to the Casper smart contract for the validation of the blocks they are working on. That is, when a miner finds a block it first must place a bet on how confident they feel the block will be added to the chain. If the network has decided that the block the validator staked should be added to the chain, the validator will receive a reward proportional to the amount of their stake.

Furthermore, if the miner decides to be malicious and stakes nothing, then the result of their mining efforts will yield them no reward, and their ETH holding will be drastically reduced. Casper takes

[36] https://coinjournal.net/bitcoins-lightning-network-version-1-rc-mainnet-beta-implementations-way/
[37] https://1ml.com
[38] https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/

penalization even further by reprimanding miners who do things like go offline, or prevent certain transactions from being broadcasted.

Since a Casper contract can be created using Ethereum smart contracts, which is not the case with Bitcoin, Bithereum will leverage various opcodes and introduce new opcodes with built in functionality that mimics Casper-like Proof of Stake. The existing opcodes that will be leveraged are OP_CHECKLOCKTIMEVERIFY from BIP 65, along with the proposed OP_GROUP in BCH. Additional new opcodes to be introduced will be as follows: OP_VALIDATORSELECT, OP_RANDAO, and OP_SLASH.

We will first need to create the designated address, called the Bithereum Staking Address, to be built into the network in which users will be able to stake their coins to be selected as validators. The opcode OP_CHECKLOCKTIMEVERIFY will be leveraged in order to freeze the funds in the Bithereum Staking Address for X amount of time, as defined by our staking guidelines at the time of the release.

For Bithereum, OP_GROUP will be utilized for the initialization of the staking process in each round, and work in conjunction with other opcodes to facilitate Bithereum's PoS model. In October 2017, Andrew Stone issued a proposal for a new opcode to be implemented to Bitcoin Cash, referred to as OP_Group. What this opcode creates is a system of representative money in which certain tokens can be "colored" to create additional native tokens to represent something specific. As elaborated by Stone, OP_GROUP colored coins allow direct representation of assets as satoshis and embed the colored coin transfer and validation into the Bitcoin scripting language in a manner that allows colored coins to take advantage of scripting and that makes them very easy to implement for existing Bitcoin Cash implementations.[39] Coins are essentially colored, or "minted", when a certain amount of the token is associated with a unique ID (color). Only the creator of this particular color has the ability to mint additional ones, as well as un-color, or burn the unique ID to change it back to the native token. The colored coins are going to inherit all the features normal bitcoins have, you can lock them, you can send them freely to anyone and you can use more advanced scripting options on them.[40]

To begin the staking process, each individual will have to first mint their own unique Bithereum colored coins for the total amount he/she plans to stake, and then send them to the designated staking address. As Bithereum will begin as a PoS hybrid, and validators will only be chosen every 100th block, validator selection will be triggered upon the completion of the 99th block. The validator selection process will be done via the opcode OP_VALIDATORSELECT, which will contain Bithereum's staking guidelines based on coinage as well as additional randomization methods that will be detailed at a further time, in order to pick 5 validators.

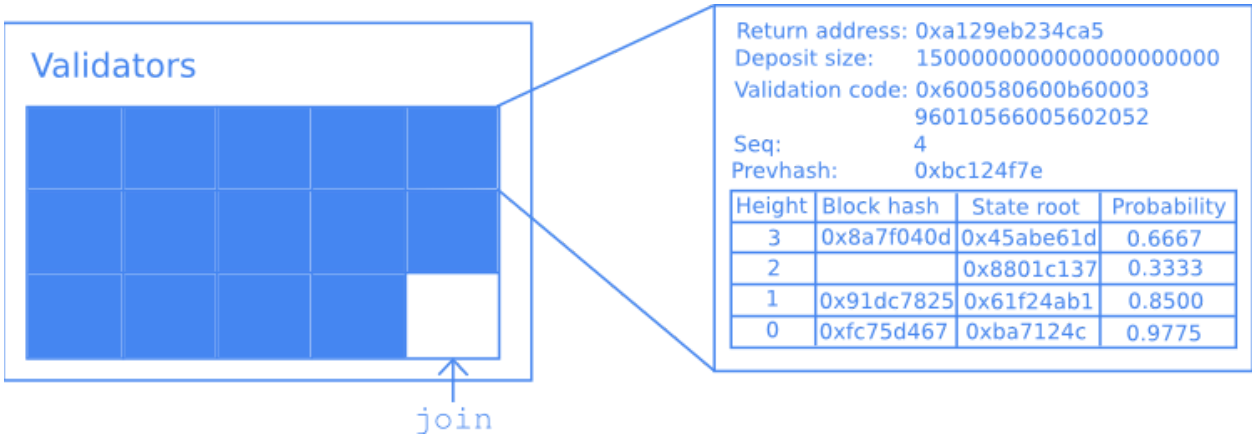
To specify, this new opcode will be added through a soft fork and will allow for the selection of various validators from the Bithereum Staking Address. Validators will be selected in a random, nondeterministic way with varying probabilities based on coinage. This makes for pre-planned attacks far more difficult. Coinage is calculated by N*D, where N is the number of coins you have staked, and D is the number of days those coins have been staked. There will be a maximum number of days you can have your coins staked in one go, which will prevent validators with large stakes from dominating.

[39] https://medium.com/@g.andrew.stone/bitcoin-scripting-applications-representative-tokens-ece42de81285
[40] https://www.yours.org/content/an-independent-opinion-on-op_group-e4c0ed0b265d

As this above process is occuring, another process will be occurring simultaneously via the opcode, OP_RANDAO.[41] Like Casper, we will be using RANDAO to verify that validators get selected. How this works, is that when a validator sends their stake to the Bithereum Staking Address, they will receive a private, random number S that will be associated with their stake. After the selection process takes place, the selected validators are required to display their unique random number. This verifies that (a) that validator is the one who was selected and (b) that validator is the owner of the address connected to that stake, since no one else can replicate this random number. Validators who fail to display their random number upon selection will have their BTH slashed, and a replacement validator will be selected. There will also be a requirement for the number of participants, if it fails to collect enough random numbers, staking will not occur at this block height.

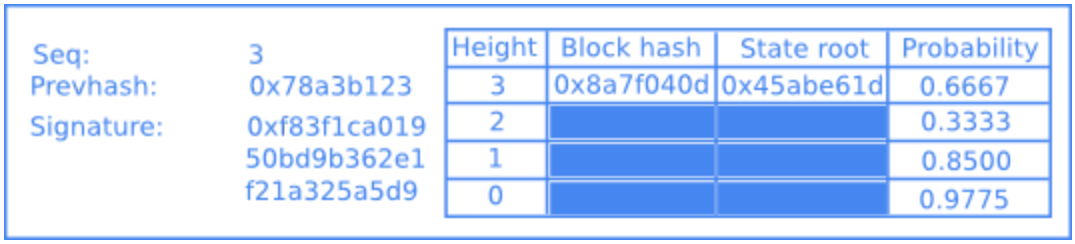
Once the validators have been selected and each staker has presented their unique S variable from RANDAO successfully, the selected validators' coin colors (unique IDs) will be broadcasted via the blockchain explorer. The validators are then ready to proceed with the creation of the 100th block where they vote in order to create the checkpoint of finality in which everything prior to the block becomes irreversible. At this point, the new opcode OP_SLASH is then utilized to ensure that each validator is displaying honest behavior, and if not, the particular malicious actor's stake is lost/slashed immediately, also excluding them from any mining reward pertaining to their participation in validation. Once the block has been validated post-slashing, the validators receive the block rewards in proportion to the amount each of them staked. This entire process is then repeated again after the next 100 blocks and so forth.

As staking begins, Bithereum will also have a built-in algorithm that is associated with the interval of blocks that will need to pass before staking takes place. As mentioned above, the validation checkpoint for staking will occur every 100 blocks to start, but this interval will be slashed in half every 2 months, for the most part. It will begin as every 100 blocks, but will reduce to 50 blocks after 2 months and keep on reducing as such. After a year, validators will be chosen after every 6 blocks. Once a year passes, the blocks will reduce 2 more times, once into 3 and finally into every block. In conjunction with this staking halving interval, a difficulty bomb will be implemented into the PoW mining efforts; as time passes, mining PoW blocks will become more difficult, ultimately pushing everyone into a pure-PoS system.



Vitalik Buterin/Ethereum.org - Structure of Casper contract[42]

[41] https://github.com/randao/randao
[42] https://blog.ethereum.org/2015/12/28/understanding-serenity-part-2-casper/



Vitalik Buterin/Ethereum.org - Keeping track of bets[43]

Equihash <144,5>

To address the centralization in mining, Bithereum will utilize Equihash (GPU) mining together with Proof of Stake, to bring a level of uniformity that simply isn't present in Bitcoin.

Devised by Dr. Dmitry Khovratovich and Alex Biryukov[44], Equihash is a memory-based mining algorithm that will allow anyone to participate in mining by preventing the division of mining loads and restricting proofs to memory (known as **memory hardness**). Essentially, the more Random Access Memory (RAM) a particular mining node has, the more effective they can mine. In this sense, Equihash serves as a great resistor to specialized network ASICs because a person with multiple processors and more memory can outperform optimized mining chips designed for pure hash computing. Equihash consists of a class of Proof of Work schemes with parameters d, n, and k, which decides the equihash scheme as well as the memory and time puzzle for the individual solving it. Equihash uses a seed to ensure that each puzzle is different and every possible solution for each problem is unique and incompatible.

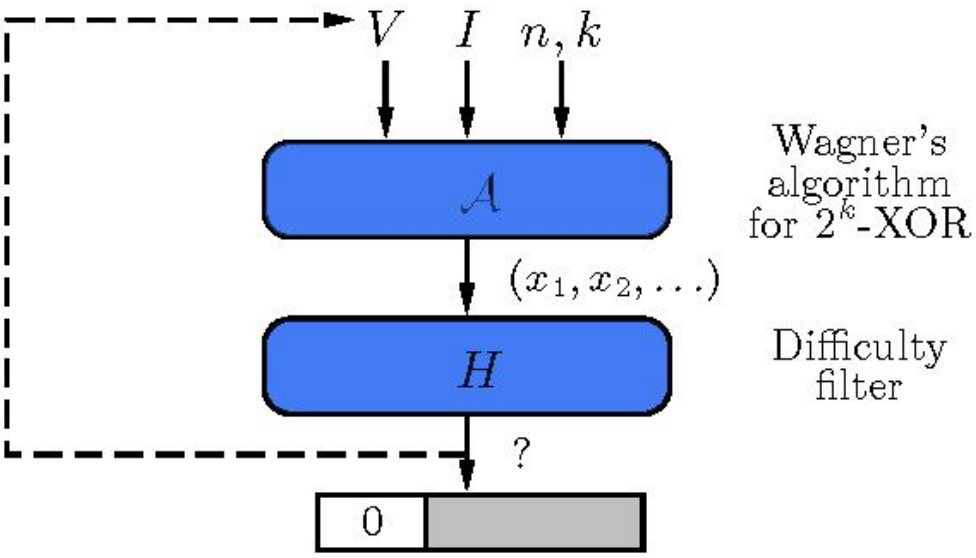
Though Equihash is the name of the algorithm, there are several ways this algorithm could be tweaked depending on two parameters in the code, *N* and *K*. These parameters directly affect the time it takes different combinations of processing power and memory, as well as how memory-intensive finding the solution is. Typically, *N*=200 and *K*=9, but it turns out that these numbers aren't effective in terms of either resisting ASICs or the mining cartel, as has been displayed through all of the 51% attacks on Equihash coins. The primary reason for this has to do with memory hardness; the optimal amount of memory for the 200,9 parameters is window of 50MB to 144MB. The issue is that the Antminer z9 has the ability to mine this effectively, rendering its purpose of being ASIC resistant as obsolete. However, when the parameters are adjusted to *N*=144 and *K*=5, the optimal amount of memory needed is window between 700MB to 2.5GB, making it far more costly to build an ASIC to combat this, as it is 17x more memory intensive[45].

Another benefit of this algorithm, specifically the 144,5 implementation, is that it separates the mining efforts from the ZCash miners, whom use the 200,9 implementation. Having a relatively unique algorithm is effective in combating 51% attacks for the short to intermediate-term because it

[43] https://blog.ethereum.org/2015/12/28/understanding-serenity-part-2-casper/
[44] https://www.cryptolux.org/images/b/b9/Equihash.pdf
[45] https://bitcoingold.org/equihash-btg/

places the coins into a new pool of power. While Bithereum will be starting off like this, the main goal is to implement a hybrid Proof of Stake into the chain as soon as possible, as it is clear that ASICs cannot be stopped forever no matter how many times the hash algorithm is adjusted.

What makes Equihash particularly appealing to Bithereum, is that it is a memory adjustable technique that can introduce penalties for variable memory usage. At the same time, Equihash is capable of producing proofs that are fairly quick to generate, prevent cost amortization, and account for parallelized mining activity by proving that memory bandwidth constraints such activity[46].



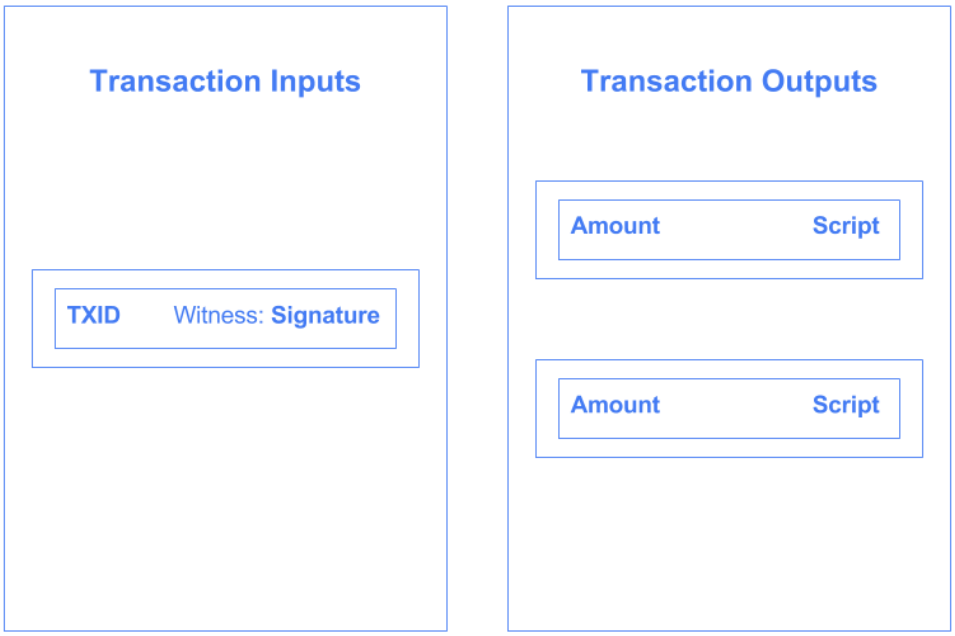
Equihash: proof-of-work based on the generalized birthday problem[47]

Increased Block Size & Segregated Witness

As stated earlier Segregated Witness allows for more transactions to be included in each block by adjusting the maximum block size. Unlike Bitcoin, Bithereum will integrate Segregated Witness from the beginning and will have a set block size of 2 megabytes (also known as **SegWit2MB**). Originally proposed for Bitcoin in the BIP 141[48], and created by Dr. Pieter Wuille, Segregated Witness separates a transaction's signature, which takes up the vast majority of the block size, from the rest of the transactions' data. Transactions would still consist of references to prior transactions, however with Segregated Witness, signatures would be moved to separate ("segregated") space at the end of the transaction ("witness") as shown by the following diagram. Rather than define the block size in terms of bytes, each byte within a block is assigned a weight. The Segregated Witness is assigned a

[46] https://ledger.pitt.edu/ojs/index.php/ledger/article/view/48/65
[47] http://orbilu.uni.lu/bitstream/10993/22277/2/946.pdf
[48] https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

weight of 1 and each block thereafter is assigned a weight of 2, for a maximum of 2 million- allowing an increase in the maximum block size to 2 MB.



Revised transaction data with segregated witness

The route Bithereum will be going in terms of block size is the same as BCH, 32 MB blocks. BCH underwent a network upgrade in May 2018, to increase their block size from 8 MB to this new 32 MB number, allowing the network to handle up to 10 million transactions a day at 100 transactions per second[49]. Another major benefit of this increase is that it provides the ability to enable previously disabled opcodes. These are codes that perform specific operations using a stack language known as Script[50]. As detailed in the Proof of Stake implementation section, Bithereum will be utilizing several existing opcodes as well as a few new ones, so the 32 MB block size takes these future updates into consideration.

Lightning Network

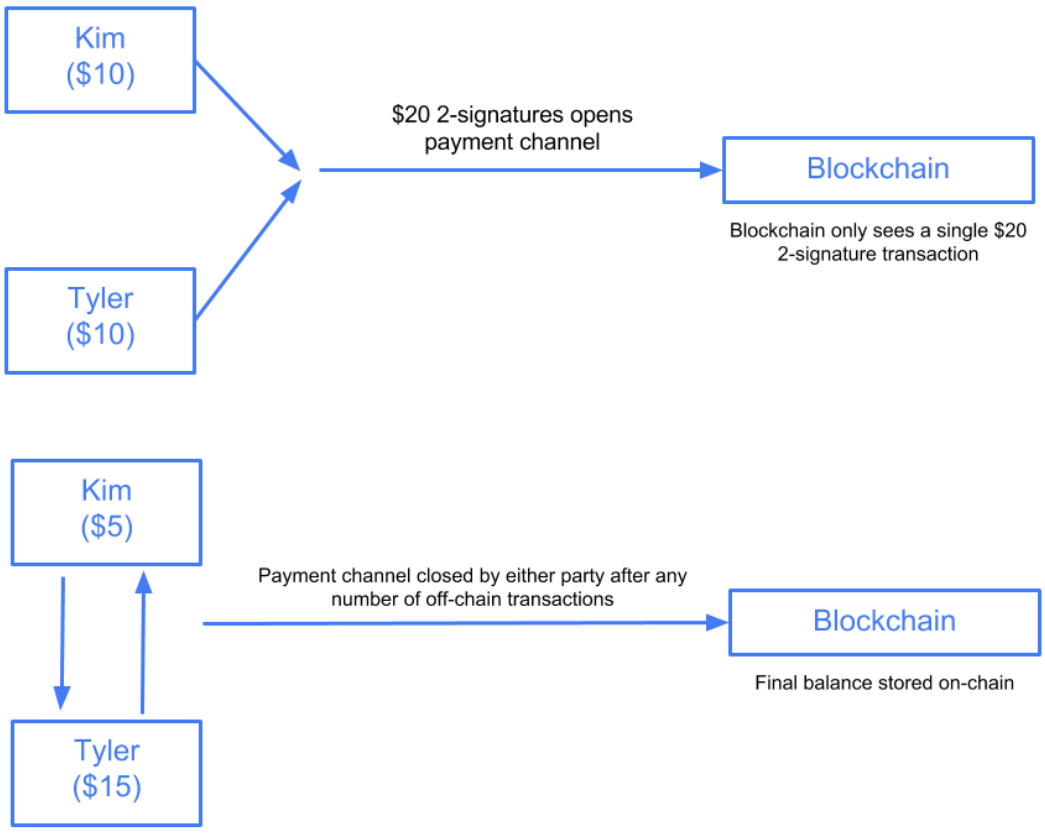
With transaction fees sky rocketing on Bitcoin, it is seemingly impossible to send any amount of Bitcoin without getting stuck with a rather large transaction fee. A big part of this, as was stated earlier is because of the overwhelming amount of transactions that need to take place. Lightning Network is a solution to this issue.

Bithereum will use the Lightning Network to establish payment channels that can perform transactions very quickly and with little to no fees once the channel has been established. Lightning Network will work by using Bitcoin's scripting language to create multi signature contracts, developed using Bitcoin's various opcodes to simulate a payment channel between users[51].

[49] https://www.trustnodes.com/2018/05/16/bitcoin-cash-successfully-upgrades-32-mb-new-op_codes
[50] https://news.bitcoin.com/bitcoin-cash-upgrade-milestone-complete-32mb-and-new-features/
[51] https://lightning.network/

Lighting network will be implemented in the following way:

Bithereum coins are first sent by both parties to a multisig (referred to as a **channel**) address. The multisig or channel serves as the gateway to the public chain and initiates the link between transacting parties. Once both parties have agreed on the starting balance of the channel, all parties can begin to transact on the Lightning Network. It is important to note that while two parties are required to open a payment channel, only one is needed to exit or close a payment channel. Only until the payment network is completely closed does the transaction persist to the chain.



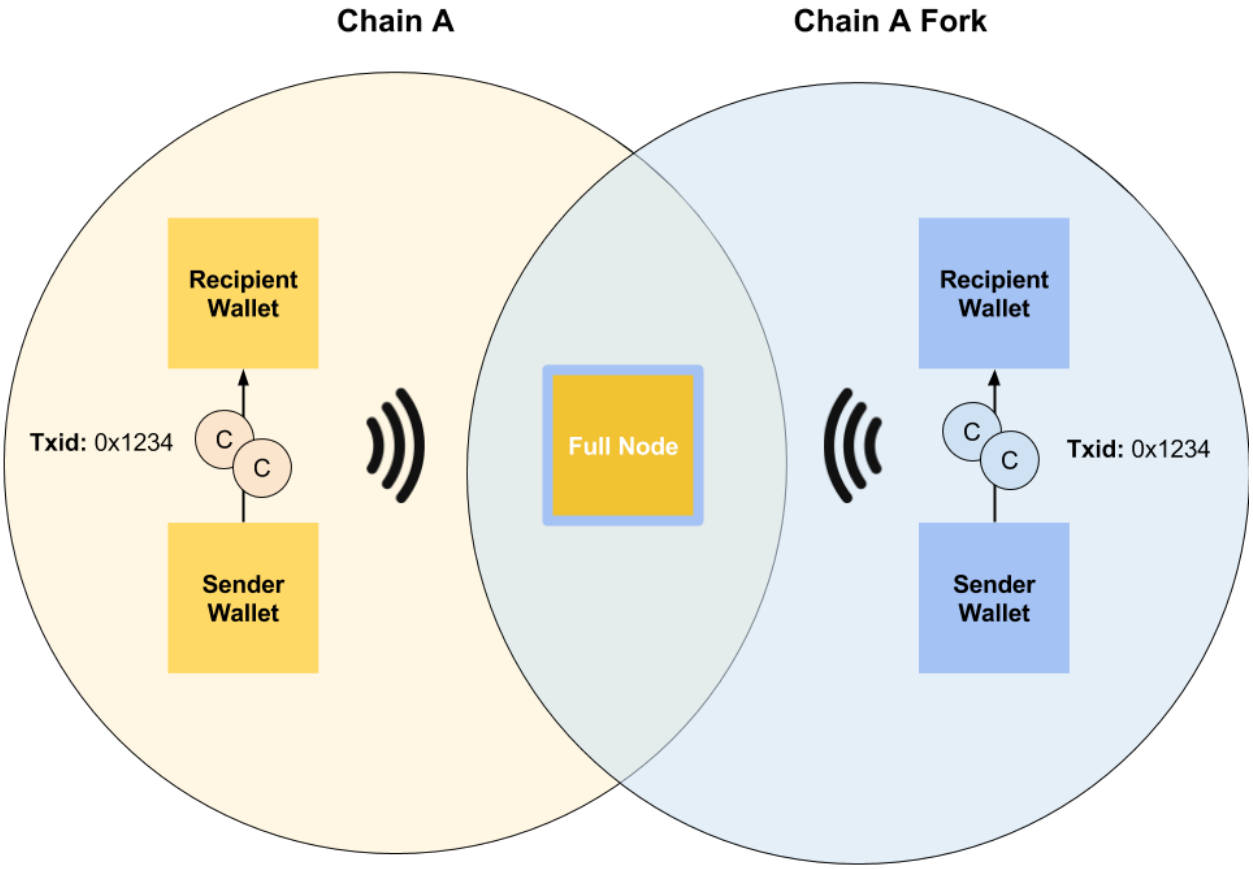
Payment Channel example using lightning network

Replay Protection

Reply protection is a crucial component of any cryptocurrency fork because it ensures that a transaction (“a play”) on either chain does not inadvertently move (“replay”) on the original or forked blockchain. Simply put, a transaction is considered replayed when the initiator transacts on a duplicate or forked blockchain on which the transaction history and balances are the same, triggering the exact same transaction to take place on the copied chain, or vice versa.

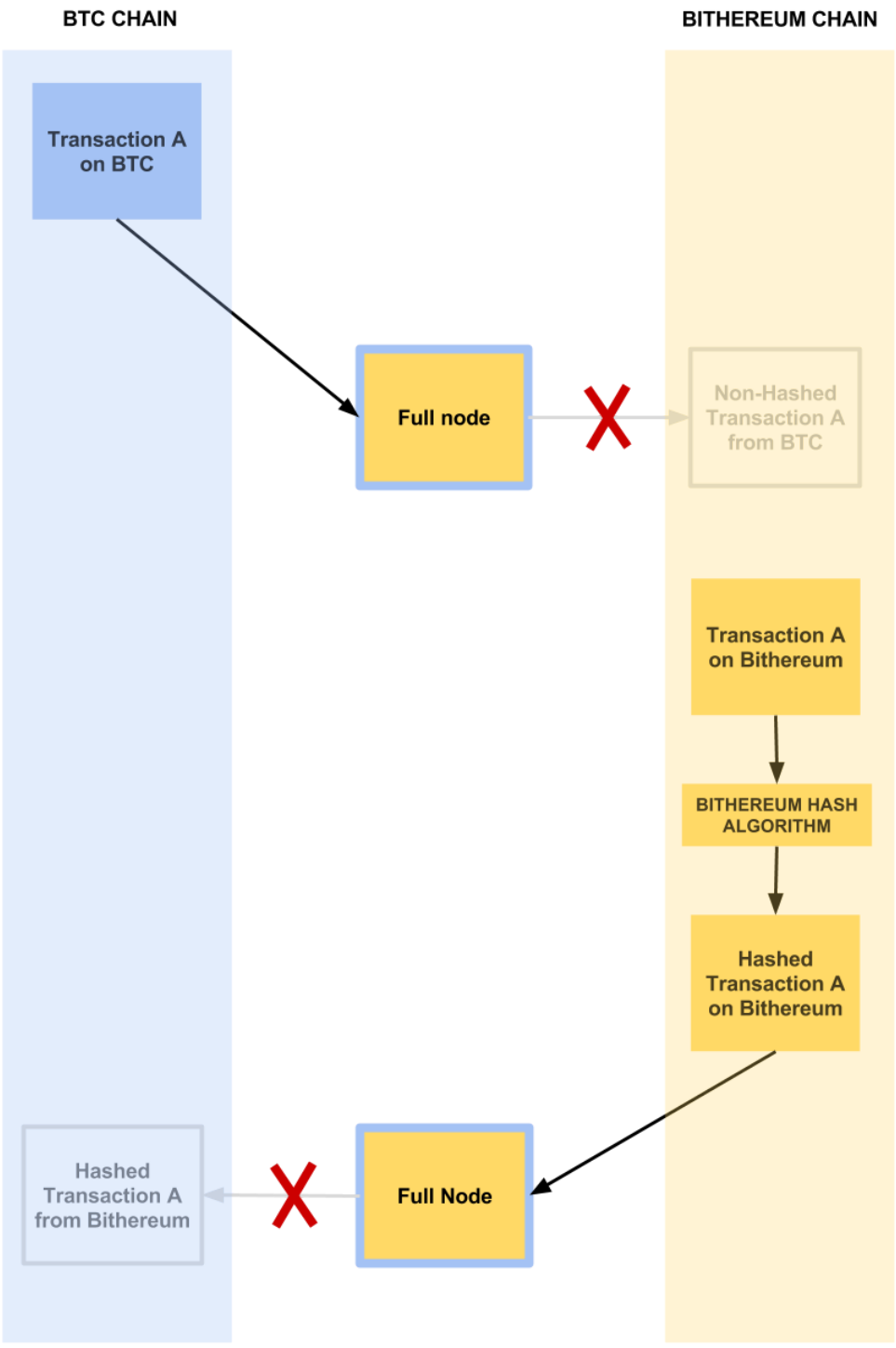
From a miner's perspective (as shown in the below figure) the broadcasted transaction is technically valid on both chains. That is, because the balances on each chain refer to the same UTXOs that have been verified on both chains that the miner is mining on- the miner will opt to include the

transactions that take place on either chain in the next block being created on both chains simultaneously, causing a replay.



To prevent replays, Bithereum will implement a complete two-way replay protection mechanism that will ensure that holders of Bithereum do not inadvertently move BTC when moving Bithereum coins and vice versa.

The way this will be accomplished is by utilizing a Bithereum specific hashing algorithm to compute the hash of each Bithereum transaction. As a result, transactions that take place on Bithereum post-fork will be invalid if broadcasted to the BTC chain. Similarly, any BTC transactions that take place post-fork on the BTC chain, will be invalid when broadcasted to the Bithereum chain. The following diagram is a simplified illustration of how the Bithereum hash algorithm helps to serve as an effective two-way replay protection mechanism, whereby transactions broadcasted to the opposite chain are considered invalid because of a hash mismatch.


BTC CHAIN
BITHEREUM CHAIN
Transaction A on BTC
Full node
Non-Hashed Transaction A from BTC
Transaction A on Bithereum
BITHEREUM HASH ALGORITHM
Hashed Transaction A on Bithereum
Hashed Transaction A from Bithereum
Full Node

Hard Spork (hard fork + hard spoon) Specifics

Hard forks have been the topic of discussion as of late as more Bitcoin forks have entered the scene. However, hard forks can either be contentious or non-contentious. The definition of a hard fork of a blockchain can be seen as “an alteration to the protocol which includes changing block structure, difficulty rules, or increasing the set of valid transactions, therefore requiring users to upgrade.”[52] These protocol changes are critical for network upgrades, as we have seen with Ethereum’s hard fork “Byzantium”. All of the nodes were upgraded to the new code and this would be considered a non-contentious fork. This example is what Bithereum will do when implementing PoS. Contentious forks, like BCH and BTG, are caused when there is a change to the protocol, however not all of the users upgrade to the new chain, thus creating a new coin.

There is also a term that some might not be familiar with called the “hard spoon”. This term was originated by the Cosmos team and is defined as a meta-protocol change that “occurs when a new cryptocurrency is minted by replicating the account balances of an existing cryptocurrency.”[53] A hard spoon is non-contentious, meaning that it is in no way attempting to compete with or take market share from the blockchain who’s balance it’s inheriting.

Bithereum aims to do what no other hard fork has done, by fusing the visions of both Bitcoin and Ethereum. Bithereum will blend these two terms together to create the first “hard spork” of the Bitcoin and Ethereum blockchains. In this case, we will be hard forking Bitcoin to make changes to the protocol that will allow it to be a more technologically advanced form of peer-to-peer currency, while hard spooning Ethereum by taking a snapshot of the existing account balances of ETH holders to award them in Bithereum. By doing this we will effectively improve the Bitcoin protocol while implementing Ethereum’s ideals minus the sell-pressure from ICO’s. As BTH utilizes a significant portion of Ethereum’s vision, unlike all of the other BTC forks, we will also be awarding all ETH holders with coins, giving them the ability to stake their coins in the future as well. This is an excellent way of keeping both the Bitcoin and Ethereum communities on board to help develop the ecosystem.

6. REDEMPTION

Redeeming Bithereum (ETH Holders)

Since Ethereum and Bitcoin interact with transactions on entirely different blockchain implementations and with completely dissimilar address spaces; Bithereum will introduce a mechanism that will give both BTC and ETH holders the ability to redeem BTH regardless of which chain their holdings reside on and with minimal work for each holder. All BTC will be redeemable on a 1:1 ratio with BTH (i.e if you have 1 BTC you can redeem 1 BTH), whereas all ETH will be redeemable at a price ratio of ETH:BTC at the time of the spork.

[52] https://en.bitcoin.it/wiki/Hardfork
[53] https://blog.cosmos.network/introducing-the-hard-spoon-4a9288d3f0df

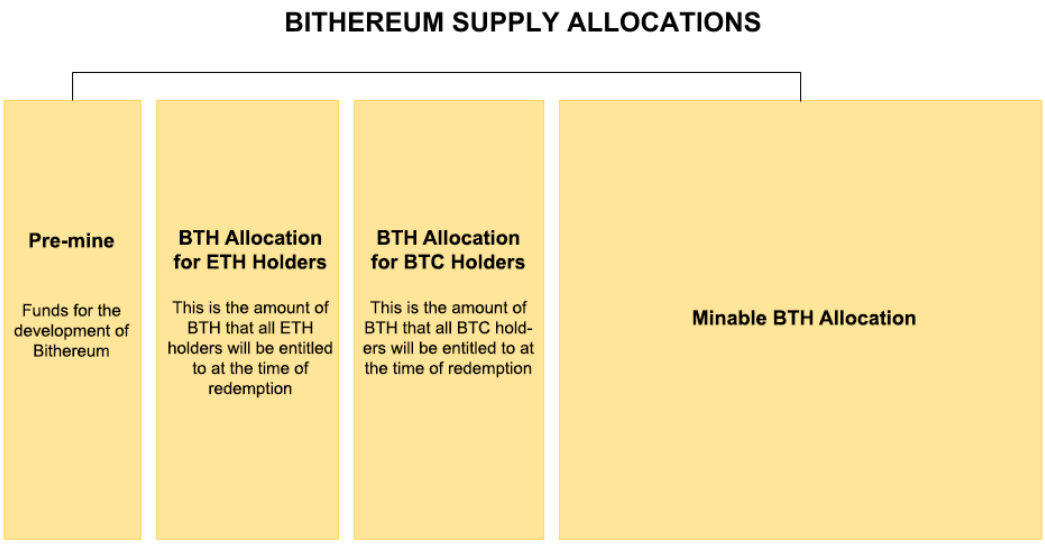
Update: The hard spoon snapshot was taken on December 12th, at exactly 19:00 UTC or Ethereum block number 6,874,581. The ETH to BTC ratio at the time was 38 ETH to 1 BTC (ETH at $91.60 and BTC at $3,506.62), so ETH holders will be able to redeem BTH at the same ratio of 38 ETH to 1 BTH. The total amount of BTH that will be set aside for ETH holder redemption is 2,730,450 BTH. By taking this hard spoon snapshot, the total max supply of BTH has also been finalized and will be 30,886,000 BTH.

To ensure redemption of BTH as an ETH holder, one must send a 0 (zero) ETH transaction to our ETH Redemption Smart Contract with the public key to their newly created Bithereum wallet in the data field. For anyone with ETH in multiple wallets, this process must be repeated for each address, however you can provide the same Bithereum address in the data field for the corresponding BTH to be released into the same wallet.

The ETH redemption smart contract pairs your ETH address to your BTH address and is referenced by the Bithereum oracle after the fork. The Bithereum oracle triggers the issuance of BTH from the ETH holder BTH allocation generated from the Bithereum genesis block.

Once the spork happens, the BTH transferred by the Bithereum oracle to the BTH address (specified in your zero ETH transaction) will be proportional to the balance of your ETH address directly prior to the spork block. For example, if you have a balance of 3 ETH when you send the 0 ETH transaction to the redemption smart contract and decide to send 1 ETH to another ETH address; the amount of BTH you will receive to your BTH address will be proportional to 2 ETH. In other words, the ETH redemption process must be completed for all ETH addresses with an Ether balance prior to the spork block.

Once an ETH address has gone through the redemption process, it will be removed from Bithereum's oracle that includes each ETH address in existence prior to the spork block, along with the balances. This is so that no address can be redeemed more than once.



Redeeming Bithereum (BTC Holder)

Since BTH will start out as a direct descendent of BTC, all BTC holders will be able to claim their BTH in the same way they would with any other hard fork of Bitcoin.

To get started with obtaining BTH, it is advised that all BTC holders should move their BTC to an entirely new wallet as this prevents any scenarios where coins are lost by spending on either chain. With the Bitcoins safely moved to a new address (created after the spork block) the private key associated with the old BTC wallet can be exported and then imported into a Bithereum wallet.

With the BTC holder's old BTC wallet imported into the BTH wallet client, a BTC holder will be able to see how much BTH they have based on their BTC balance prior to the spork block. The Bithereum Supply Allocation diagram in the prior section shows how the total supply will account for BTH set aside for BTC Holders.

7. ROADMAP

Milestones

December 2017 - Conceptualization
February 2018 - Company set-up in Dubai
March 2018 to July 2018 - Completion of White Paper v1, Launch of website
August 2018 - Marketing/Development Bounties, early redemption sign-up
September 2018 to November 2018- Pre-fork Development, testing via mining rigs, deployment of testnet code, product refinement
December 2018 - Execution of hard spoon
January 2019 - Execution of hard spork
February to March 2019 - Team expansion, Community building
Q2 2019 - R&D of Proof of Stake and Lightning Network
Q3 2019 - Begin testing of upcoming implementations
Q4 2019 - Begin implementation of Lightning Network
Q1 2020 - Begin implementation of PoS mining, will start as hybrid
Q2 2020 - Possible additional hard fork to incorporate Sharding/Plasma

8. USE OF FUNDS

Pre-mine of Funds

Contrary to many opinions, forks can be costly to develop, and there are no direct avenues of raising money such as with ICO's. Therefore, a pre-mine is one of the few ways to support a fork's development, especially to offset costs that took place prior to the fork (Wallet development,

Mining/Pools, Nodes, System/Security maintenance, etc.). There will be a pre-mine of around 3% of the supply for the team, and around 7% of the supply for the project to be primarily used to encourage early developers, invest in the BTH ecosystem, and ensure the success of the future technological developments for Bithereum while also providing incentives for full nodes.

General & Administrative

Refers to costs of operating the business such as building rent, consultant fees, depreciation on office equipment, supplies, subscriptions and utilities, as well as managerial compensation.

Development

Refers to costs of building and maintaining the product, such as developer salaries, server costs, and development tools.

Marketing

Refers to costs of communicating and delivering the company's value to its users, such as general outreach through various channels, public relations, media coverage, community building/management, and advertising.

Legal

Refers to the company's ongoing legal expenses, due to company setup, and any and all legal advice.

Miscellaneous

Refers to incidental expenses which cannot be classified such as travel, lodging, and attending conferences.

9. CONCLUSION

Bithereum is a coin that is created via forking the Bitcoin blockchain in combination with Ethereum's technological roadmap. A Proof of Stake consensus model will not only be an economical advancement by increasing transaction speed and reducing fees, it will also be an ecological advancement by lowering the excessive energy consumption used by Proof of Work mining. Bithereum essentially creates an outlet for both Bitcoin and Ethereum, allowing Bitcoin to take on its new role as a store of value, and allowing Ethereum to be used for its true purpose as a worldwide computer that can contain a vast ecosystem of dApps on its platform. With Ethereum's technology and Bitcoin's vision, Bithereum will bring together the best of the two leading cryptocurrencies to create an unparalleled peer-to-peer digital currency.