

Forum:[Hack Forums](#)

Thread: [Ethereum is changing algorithms to Proof of Stake. Here is what it means for you!](#)

Kill Joy - June 12, 2017, 6:19 pm

Many of you probably have not heard of the news. Ethereum is moving from Proof of Work to Proof of Stake and plans to roll this out in late 2017 as of right now. A lot of you are probably asking, what even is Proof of Work and Proof of Stake? Why should I care? I am about to explain what these things are, why Ethereum is switching, and what this means for you. If you are too lazy to read or cannot comprehend the information in this article, please feel free to ask specific questions. :)

Ethereum & Proof of Work

The first version and also current version of Ethereum uses an algorithm called Proof of Work, which involves mining. To thoroughly explain what Proof of Work is, I am going to steal a section from a thread I wrote a few days ago.

Proof of Work is defined as an economic measure to deter denial of service attacks and other service abuses such as spam on a network by requiring some work from the service requester, usually meaning processing time by a computer. Proof of Work is not a new concept. For additionally reading on the history of it, read [here](#). Coins like Bitcoin use Proof of Work.

Simply put in terms of crypto currency, this means that calculations are required by the network nodes in order to form a distributed ledger. This process is called mining.

A distributed ledger is a decentralized system that can agree on and keep track of the correct amount a wallet has by providing a history of every single transaction.

The Purpose of Mining

Mining is the process in which Proof of Work is generated. Before we go into the exact purpose of mining, we need to address what a Block is. A block is a permanent storage of record that includes a group of data of all or some transactions that have not yet been included in previous blocks.

The main purpose of mining is to verify the legitimacy of a transaction and prove that it is not a double spend. A double spend is when the same coins are spent more than once. Since mining is a strenuous process, miners are rewarded for their work upon successful completion of mining a block. Rewards vary by coin and can change over time.

Explaining like I am five, here is what happens: A transaction is made and included with other transactions in a Block;

Miners verify every transaction in the block are legitimate;

In order to do this they must solve a mathematical problem;

Rewards are handed out to the miner that successfully solved the problem;

All legitimate transactions are stored in the mined block on the blockchain.

Due to the strenuous computation nature Proof of Work, it can become an expensive process.

Read my thread on different variations of Proof-of-X [here](#).

Ethereum & Proof of Stake

Proof of Stake is an alternative to Proof of Work and aims to achieve distributed consensus. The [idea was first discussed on bitcointalk](#) in 2011 and first used with [Peercoin](#). Instead of having miners prove each and every transaction is legitimate, proof of stake requires that a person stake (hold or lockup) coins and prove ownership. To become a validator, you can lock up (bond) some of your ethereum and send them to the Casper Contract. We'll talk about Casper shortly.

In the event that a user tries to cheat the system, the Casper protocol will punish them. Vitalik Buterin, Ethereum Co-Founder, explained it like this:

Quote: Imagine 100 people sitting around a circular table. One person has a bundle of papers, each with a different transaction history. The first participant picks up a pen and signs one, then passes it onto the next person, who makes a similar choice.

Each participant only gets \$1 if they sign the transaction history that most of the participants sign in the end. And if you sign one page and later sign a different page, your house burns down.

Read my thread on different variations of Proof-of-X [here](#).

Why is Ethereum Switching?

Ethereum developers believe that consensus Proof of Stake algorithms can provide a higher degree of security for a given amount of resource expenditure than Proof of Work algorithms.

In simpler terms, this means that Proof of Stake will be: Cheaper. There will no longer be a need for hardware and electricity costs.

Less Censored. Unlike Proof of Work blockchains, Ethereum plans on providing solutions for a more censor-friendly blockchain.

Scalable. Ethereum will become more more scalable allowing larger applications.

Proof of Stake however is not perfect. There are many flaws and Ethereum developers plan on tackling these flaws with a security-deposit based economic consensus protocol called Casper. There are many technicalities surrounding Casper, so I will try to bring a few to light.

Casper & The Casper Contract Hardware Mining will no longer exist. Virtual mining and validators will take its place. To become a validator, you must lock up some ETH for a specific amount of time, currently set for 4 months.

Lower Latency. Block times will become super fast. Ethereum developer Vlad Zamfir believes it can start at 4 seconds/block and be pushed down to 1 second/block.

[Finality](#). Ethereum will be able to quickly prove who owns what and how many. This will make it impossible for a random blockchain glitch to suddenly decide that the operation that made those assets theirs is now reverted and so their ownership claim over those assets is lost.

There are so many different paths and technicalities to talk about and it is hard to just pick a few to highlight and talk about in-depth. I am hoping for this thread to spark an interest in the actual technology of Ethereum and for you to do some reading and research on your own.

What does this mean for me?

Ethereum is not immediately switching from Proof of Work to Proof of Stake. They will be doing this in stages and temporarily have a hybrid system of the two in place. During the first stage in the switch, Proof of Stake will be used everyone 100 blocks as a checkpoint. This is done to further prove all the transactions are legitimate. Review [Finality](#). Smart contracts for Casper will be issued where users will be able to become a validator. This will become default when it is fully incorporated with the Casper daemon and Ethereum client. Stage two is just a much larger scale of this. Keep

your eye out on the [Ethereum Blog](#) for further Development.

The beginning stages of the transition are currently targeted for the end of 2017. This is subject to change.

Key Changes Mining will no longer exist in a sense. Hardware mining will disappear. Mining will now be conducted in the form of validating.

Proof of Stake and the absence of miners mean less coins coming into supply. Inflation will now be initiated.

Total ETH supply will be around 100M. Target ETH at stake is 10M. Target ROI for validators is 8%; therefore, the annual inflation will be around 0.8%.

Block times will start around 1 block/4 seconds and eventually become 1 block/second.

Further Reading

[Proof of Stake FAQ](#)

[Introducing Casper "the Friendly Ghost"](#)

[The History of Casper — Chapter 1](#)

[The History of Casper – Chapter 2](#)

[Proof-Of-Stake: Vitalik Buterin Shares Casper Contract Code](#)

[Where's Casper? Inside Ethereum's Race to Reinvent its Blockchain](#)

Like I stated at the beginning of this thread, if you are lazy, overwhelmed, or confused by any of this, then feel free to ask any questions!

?dvertisement - June 12, 2017, 6:22 pm

Great post, lots of good information. Thanks for this.

I'm excited to see what PoS has to bring to Ethereum, lots of stuff to come.

Ramsey - June 12, 2017, 6:23 pm

My word...

This is a great in depth explanation! Hats off to you!

Didn't get the time to read everything but I will be back!

Thanks for this!

daymon - June 12, 2017, 6:25 pm

I haven't read too much up on the PoS system, but whats to combat if I hypothetically have control of a large amount of validators?

abc123xD - June 12, 2017, 6:29 pm

Will this affect transaction fees at all?

Kill Joy - June 12, 2017, 6:31 pm

(Jun 12, 2017 06:25 PM)Sin+ Wrote: [\[CITE\]](#) I haven't read too much up on the PoS system, but whats to combat if I hypothetically have control of a large amount of validators?

This is combated by the Casper Protocol. So far it is planned to have only 250 validators at any given time. Validators will want to follow the rules or they will be punished and lose their own money.

Example by Vitalik Butener:

Quote:Imagine 100 people sitting around a circular table. One person has a bundle of papers, each with a different transaction history. The first participant picks up a pen and signs one, then passes it onto the next person, who makes a similar choice.

Each participant only gets \$1 if they sign the transaction history that most of the participants sign in the end. And if you sign one page and later sign a different page, your house burns down.

Since it is early and there hasn't been a development post in a couple months, we can look forward to even more assurance that validators cannot be abused.

ASLR - June 12, 2017, 6:34 pm

This is exciting news. I hope that ETH overtakes bitcoin as this is much more environmentally responsible. The amount of energy spent mining coins is absurd

daymon - June 12, 2017, 6:35 pm

(Jun 12, 2017 06:31 PM)Kill Joy Wrote: [\[CITE\]](#) This is combated by the Casper Protocol. So far it is planned to have only 250 validators at any given time. Validators will want to follow the rules or they will be punished and lose their own money.

Example by Vitalik Butener:

Since it is early and there hasn't been a development post in a couple months, we can look forward to even more assurance that validators cannot be abused.

Yeah, but what if the majority of the validators are owned by me, and I have them "sign papers" of my choosing? I'm just a little confused on the specifics that would actually combat this. I mean, how would you know I was breaking the rules, if I make up the majority?

OnlyProfit - June 12, 2017, 6:39 pm

Don't get me wrong guys. I've read this through. To me it seems like PoW is much better for regular people like me and you as it seems like everyone has the same power if you can call it that. While PoS seem's like its like a banking system. Where 1 bank regulate's all transactions. I don't like this idea AT ALL. Unless i get something wrong here.

IPIKIN - June 12, 2017, 6:46 pm

Why won't we be able to mine ETH once it goes to POS?

Unexplained - June 12, 2017, 6:47 pm

Alright so after reading through this info here is what I gather. Please someone correct me if I am wrong.

- The speed of "confirming" transactions will be quicker and more secure.
- The current state of mining will go away.
- The fees could see a reduction from where they are now for ETH transactions.

Am I reading this correctly?

Kill Joy - June 12, 2017, 6:48 pm

(Jun 12, 2017 06:29 PM)abc123xD Wrote: [\[CITE\]](#) Will this affect transaction fees at all?

Yes. They will become very fast. We are talking about 1 block every 4 seconds or faster.

(Jun 12, 2017 06:35 PM)Sin+ Wrote: [\[CITE\]](#) Yeah, but what if the majority of the validators are owned by me, and I have them "sign papers" of my choosing? I'm just a little confused on the specifics that would actually combat this. I mean, how would you know I was breaking the rules, if I make up the majority?

I just wrote a shit ton out, then some coding in the post triggered a firewall. Gonna cut this short since I am about to get dinner.

Basically there are two ways to solve an attack. Economic consensus (best interest of the market) and social consensus (best interest of the users).

Since my post got blocked, I'm just going to paste some relevant information from the github. This talks about a few attacks and solutions to them.

Quote:What would the equivalent of a 51% attack against Casper look like?

The most basic form of "51% attack" is a simple finality reversion: validators that already finalized block A then finalize some competing block A', thereby breaking the blockchain's finality guarantee. In this case, there now exist two incompatible finalized histories, creating a split of the blockchain, that full nodes would be willing to accept, and so it is up to the community to coordinate out of band to focus on one of the branches and ignore the other(s).

This coordination could take place on social media, through private channels between block explorer providers, businesses and exchanges, various online discussion forms, and the like. The principle according to which the decision would be made is "whichever one was finalized first is the real one". Another alternative is to rely on "market consensus": both branches would be briefly being traded on exchanges for a very short period of time, until network effects rapidly make one branch much more valuable with the others. In this case, the "first finalized chain wins" principle would be a Schelling point for what the market would choose. It's very possible that a combination of both approaches will get used in practice.

Once there is consensus on which chain is real, users (ie. validators and light and full node operators) would be able to manually insert the winning block hash into their client software through a special option in the interface, and their nodes would then ignore all other chains. No matter which chain wins, there exists evidence that can immediately be used to destroy at least 1/3 of the validators' deposits.

Another kind of attack is liveness denial: instead of trying to revert blocks, a cartel of $\geq 34\%$ of validators could simply refuse to finalize any more blocks. In this case, blocks would never finalize. Casper uses a hybrid chain/BFT-style consensus, and so the blockchain would still grow, but it would have a much lower level of security. If no blocks are finalized for some long period of time (eg. 1 day), then there are several options:

The protocol can include an automatic feature to rotate the validator set. Blocks under the new validator set would finalize, but clients would get an indication that the new finalized blocks are in some sense suspect, as it's very possible that the old validator set will resume operating and finalize some other blocks. Clients could then manually override this warning once it's clear that the old validator set is not coming back online. There would be a protocol rule that under such an event all old validators that did not try to participate in the consensus process take a large penalty to their deposits.

A hard fork is used to add in new validators and delete the attackers' balances.

In case (2), the fork would once again be coordinated via social consensus and possibly via market consensus (ie. the branch with the old and new validator set briefly both being traded on exchanges). In the latter case, there is a strong argument that the market would want to choose the branch where "the good guys win", as such a chain has validators that have demonstrated their goodwill (or at least, their alignment with the interest of the users) and so is a more useful chain for application developers.

Note that there is a spectrum of response strategies here between social coordination and in-protocol automation, and it is generally considered desirable to push as far toward automated resolution as possible so as to minimize the risk of simultaneous 51% attacks and attacks on the

social layer (and market consensus tools such as exchanges). One can imagine an implementation of (1) where nodes automatically accept a switch to a new validator set if they do not see a new block being committed for a long enough time, which would reduce the need for social coordination but at the cost of requiring those nodes that do not wish to rely on social coordination to remain constantly online. In either case, a solution can be designed where attackers take a large hit to their deposits.

A more insidious kind of attack is a censorship attack, where $\geq 34\%$ of validators refuse to finalize blocks that contain certain kinds of transactions that they do not like, but otherwise the blockchain keeps going and blocks keep getting finalized. This could range from a mild censorship attack which only censors to interfere with a few specific applications (eg. selectively censoring transactions in something like Raiden or the lightning network is a fairly easy way for a cartel to steal money) to an attack that blocks all transactions.

There are two sub-cases. The first is where the attacker has 34-67% of the stake. Here, we can program validators to refuse to finalize or build on blocks that they subjectively believe are clearly censoring transactions, which turns this kind of attack into a more standard liveness attack. The more dangerous case is where the attacker has more than 67% of the stake. Here, the attacker can freely block any transactions they wish to block and refuse to build on any blocks that do contain such transactions.

There are two lines of defense. First, because Ethereum is Turing-complete it is naturally somewhat resistant to censorship as censoring transactions that have a certain effect is in some ways similar to solving the halting problem. Because there is a gas limit, it is not literally impossible, though the "easy" ways to do it do open up denial-of-service attack vulnerabilities.

This resistance is not perfect, and there are ways to improve it. The most interesting approach is to add in-protocol features where transactions can automatically schedule future events, as it would be extremely difficult to try to foresee what the result of executing scheduled events and the events resulting from those scheduled events would be ahead of time. Validators could then use obfuscated sequences of scheduled events to deposit their ether, and dilute the attacker to below 33%.

Second, one can introduce the notion of an "active fork choice rule", where part of the process for determining whether or not a given chain is valid is trying to interact with it and verifying that it is not trying to censor you. The most effective way to do this would be for nodes to repeatedly send a transaction to schedule depositing their ether and then cancel the deposit at the last moment. If nodes detect censorship, they could then follow through with the deposit, and so temporarily join the validator pool en masse, diluting the attacker to below 33%. If the validator cartel censors their attempts to deposit, then nodes running this "active fork choice rule" would not recognize the chain as valid; this would collapse the censorship attack into a liveness denial attack, at which point it can be resolved through the same means as other liveness denial attacks.

<https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ>

(Jun 12, 2017 06:39 PM)OnlyProfit Wrote: [\[CITE\]](#) Don't get me wrong guys. I've read this through. To me it seems like PoW is much better for regular people like me and you as it seems like everyone has the same power if you can call it that. While PoS seems like it's like a banking system. Where 1 bank regulates all transactions. I don't like this idea AT ALL. Unless I get something wrong here.

PoW requires a lot of money to buy hardware and pay for electricity costs. Not everyone has the same power like you said. This eliminates the need for hardware.

(Jun 12, 2017 06:46 PM)IPIKIN Wrote: [\[CITE\]](#) Why won't we be able to mine ETH once it goes to POS?

Proof of Work (what Ethereum is using) uses hashing to confirm legitimate transactions. Hashing requires hardware. Proof of Stake uses locked up amounts of Ethereum to verify transactions instead of using hashing, this is called staking. Mining isn't exactly gone, as staking is considered a form of mining.

(Jun 12, 2017 06:47 PM)TheBanker Wrote: [\[CITE\]](#) Alright so after reading through this info here is what I gather. Please someone correct me if I am wrong.

- The speed of "confirming" transactions will be quicker and more secure.
- The current state of mining will go away.
- The fees could see a reduction from where they are now for ETH transactions.

Am I reading this correctly?
This is all correct.

I am getting dinner. Will be back soon to answer more questions.

Tren Ace - June 12, 2017, 6:58 pm

When you say only 250 validators, does that mean only 250 are eligible to gain ETH on what they stake?

Kill Joy - June 12, 2017, 7:19 pm

(Jun 12, 2017 06:58 PM)Tren Ace Wrote: [\[CITE\]](#) When you say only 250 validators, does that mean only 250 are eligible to gain ETH on what they stake?

Yes, but there is a catch. It all depends on the gas limits and how much ETH will need to be staked in order to make a profit. 2 months ago, Buterin said he was thinking of making a gas limit of ~200000. You will have to deposit a ton of ETH in order to even profit from it.

Links:

<https://steemit.com/ethereum/@keysikg/ethereum-proof-of-stake-vitalik-buterin-shares-casper-contract-code>

https://www.reddit.com/r/ethereum/comments/634pwq/a_not_so_sneak_peek_at_the_current_version_of_the/

jujuger - June 12, 2017, 7:21 pm

POS should also inflate the value of ETH even higher.
This will be interesting

hq thrad

Kill Joy - June 12, 2017, 7:28 pm

(Jun 12, 2017 07:21 PM)jujuger Wrote: [\[CITE\]](#) POS should also inflate the value of ETH even higher.
This will be interesting

hq thrad

This thread will interest you:

https://www.reddit.com/r/ethereum/comments/5izcf5/lets_talk_about_the_projected_coin_supply_over/

Top comment is from Buterin.

Quote: So here is a thought. Currently, because of the PoW ice age, the block time is scheduled to start increasing in mid-2017, and past around 2019 the increase is going to grow exponentially. The mining reward does NOT increase proportionately. Hence, there is already an exponential slowdown in the growth of the ETH supply built into the protocol; my script shows:

Block 3000000, approx ETH supply 87962556, time '2017-01-16 00:38:33.067775' blocktime 14.86
Block 3500000, approx ETH supply 90612556, time '2017-04-11 18:09:34.273529' blocktime 15.27
Block 4000000, approx ETH supply 93262556, time '2017-08-15 18:20:24.642729' blocktime 30.01
Block 4500000, approx ETH supply 95912556, time '2018-11-03 05:55:48.912370' blocktime 136.71

Block 5000000, approx ETH supply 98562556, time '2025-10-02 11:47:30.658317' blocktime 835.81

Block 5500000, approx ETH supply 101212556, time '2128-03-20 09:14:16.483692' blocktime 17183.83

Block 6000000, approx ETH supply 103862556, time '5189-09-26 20:57:59.367004' blocktime 520901.19

Hence, in the foreseeable future, the supply will not go far above 100 million.

PoS is likely to lead to quite low issuance rates; I am not comfortable promising zero, but if it is not much less than the current PoW then there is little point in making the switch in any case. If the community wishes to, while PoW is in play, it's possible to agree that any delay to the ice age bomb should also respect this general ETH supply growth curve, so in a situation where at time X if current ethereum would have a 75s block time, the ice age patch would set the block time to 15s and the block reward to 1 ETH (and adjust uncle/nephew rewards proportionately).

That said, issuance is a key economic parameter and I personally don't feel I or the foundation or client developers have the authority to dictate this; perhaps it's worth some kind of vote.

Mircale - June 12, 2017, 7:29 pm

Great info man , Thanks for sharing.

Giga - June 12, 2017, 7:29 pm

Another HQ contribution. Great read with a lot of useful information. Thanks again Kill Joy.

CBHF - June 12, 2017, 8:04 pm

Would you recommend not to buy any mining hardware at this point in time? Very good article 10/10. I'm not necessarily sure how I feel about PoS yet as I have seen it on Stratis previously, can't hurt to give it a try!

?dvertisement - June 12, 2017, 8:10 pm

(Jun 12, 2017 08:04 PM)CBHF Wrote: [\[CITE\]](#) Would you recommend not to buy any mining hardware at this point in time? Very good article 10/10. I'm not necessarily sure how I feel about PoS yet as I have seen it on Stratis previously, can't hurt to give it a try!

There will always be coins to mine.

Kill Joy - June 12, 2017, 8:21 pm

(Jun 12, 2017 08:04 PM)CBHF Wrote: [\[CITE\]](#) Would you recommend not to buy any mining hardware at this point in time? Very good article 10/10. I'm not necessarily sure how I feel about PoS yet as I have seen it on Stratis previously, can't hurt to give it a try!

You still have time to mine Ethereum and make a good profit on it. Like Advertisement said, there will always be other coins to mine that will make a good profit.

IPIKIN - June 12, 2017, 8:36 pm

So if they use both POW and POS for the beginning, will we still be able to mine ETH?

Kill Joy - June 12, 2017, 8:45 pm

(Jun 12, 2017 08:36 PM)IPIKIN Wrote: [\[CITE\]](#) So if they use both POW and POS for the beginning, will we still be able to mine ETH?

From what I remember reading in the blog posts from Buterin, he wants to use PoS as a checkpoint every 100 blocks. I would imagine hardware mining will still be a thing. Coins that use PoS and have a PoW checkpoint at x amount of blocks don't reward anything to the miner, rendering mining pretty much useless.

It all depends on what they decide to implement.

IPIKIN - June 12, 2017, 9:41 pm

(Jun 12, 2017 08:45 PM)Kill Joy Wrote: [\[CITE\]](#) From what I remember reading in the blog posts from Buterin, he wants to use PoS as a checkpoint every 100 blocks. I would imagine hardware mining will still be a thing. Coins that use PoS and have a PoW checkpoint at x amount of blocks don't reward anything to the miner, rendering mining pretty much useless.

It all depends on what they decide to implement.

Interesting times ahead to say the least.

Even if mining ETH becomes obsolete at least there are other coins to mine with a pretty good income.

Mr. WAVES - June 12, 2017, 9:58 pm

Very useful read! Thanks a lot for the info!

Watch the Throne - June 12, 2017, 10:10 pm

Been reading up almost nonstop for the past few weeks about this coin or that coin. Invested in ETH back in November '16, so my \$500 investment was WELL worth it. I'm curious what will happen to the current coins that are sitting in wallets. Are they just going to stay there, able to be traded and moved around for whatever purpose one might have?

I understand the general hope that this change will improve the speed and scalability - which were two things that definitely needed to be solved. It will impact mining, but I'm not concerned with that. Long term I'm wondering if they are hoping to do something to combat the increased prices ETH. If not, contracts that were supposed to be cheap to process will be quite expensive. Unless I'm way off base here.

VirtualMon3y - June 12, 2017, 11:27 pm

Very informative thread. Nice to have you back contributing with quality like this.

FaberCastell - June 13, 2017, 1:29 am

What if miners continue to mine the old chain?

I've heard somewhere that the difficulty is supposed to increase so the mining will not be worth it anymore, thus the network not being secure anymore. But is it true? Can they continue to mine the old chain and we get a new coin ETHpow?

Gizmo - June 13, 2017, 1:35 am

Damn Kill Joy, you got a lot of knowledge regarding blockchain. I like it. Please keep sharing useful information like this with us!

I also enjoy it how you answer each question on this thread. Thanks ?

ubbelol - June 13, 2017, 1:48 am

(Jun 12, 2017 06:58 PM)Tren Ace Wrote: [\[CITE\]](#) When you say only 250 validators, does that mean only 250 are eligible to gain ETH on what they stake?

I'd imagine some of those 250 will create pools similar to mining pools where you lock up your ETH in a smart contract and receive a fair share of the total staking reward.

Banadmin - June 13, 2017, 5:24 am

Awesome. This will make transactions a lot quicker, right? Even more reason to use ETH.

SirAndrew - June 13, 2017, 5:27 am

Thanks a lot for this extremely informative post! Answered a lot of questions I had and will help me out somewhat with a current project. Thanks again!

Kill Joy - June 13, 2017, 6:12 am

(Jun 12, 2017 10:10 PM)Its Royalty Wrote: [\[CITE\]](#) Been reading up almost nonstop for the past few weeks about this coin or that coin. Invested in ETH back in November '16, so my \$500 investment was WELL worth it. I'm curious what will happen to the current coins that are sitting in wallets. Are they just going to stay there, able to be traded and moved around for whatever purpose one might have?

I understand the general hope that this change will improve the speed and scalability - which were two things that definitely needed to be solved. It will impact mining, but I'm not concerned with that. Long term I'm wondering if they are hoping to do something to combat the increased prices ETH. If not, contracts that were supposed to be cheap to process will be quite expensive. Unless I'm way off base here.

Nothing will happen to the coins. The only things that change is the blockchain and algorithms.

(Jun 13, 2017 01:29 AM)FaberCastell Wrote: [\[CITE\]](#) What if miners continue to mine the old chain?

I've heard somewhere that the difficulty is supposed to increase so the mining will not be worth it anymore, thus the network not being secure anymore. But is it true? Can they continue to mine the old chain and we get a new coin ETHpow?

Probably only if Ethereum wants to allow that, but they probably won't. The nodes will change. I don't know an exact answer for this question right now.

(Jun 13, 2017 01:48 AM)ubbelol Wrote: [\[CITE\]](#) I'd imagine some of those 250 will create pools similar to mining pools where you lock up your ETH in a smart contract and receive a fair share of the total staking reward.

This is exactly what will happen.

(Jun 13, 2017 05:24 AM)Banadmin Wrote: [\[CITE\]](#) Awesome. This will make transactions a lot quicker, right? Even more reason to use ETH.

Yes, they will become a lot quicker.

BaldCunt - June 13, 2017, 9:22 am

I wonder what will happen to my cloud mining investments </3

webdev77 - June 13, 2017, 9:23 am

(Jun 12, 2017 06:46 PM)IPIKIN Wrote: [\[CITE\]](#) Why won't we be able to mine ETH once it goes to POS?

Because mining won't do anything for the network anymore. You don't get rewarded any coins for mining.

EziNet - June 13, 2017, 9:23 am

So Ethereum will pass Bitcoin after this?

webdev77 - June 13, 2017, 9:26 am

(Jun 13, 2017 09:23 AM)BitMoney Wrote: [\[CITE\]](#) So Ethereum will pass Bitcoin after this?

Probably that or tank because all the miners will cash out and leave. This system makes it very hard for regular people without thousands invested to make anything.

Eagerkid - June 13, 2017, 10:37 am

This sounds like it will be very good for ETH, I will be looking more into the links you have posted. Thanks !

Tay-K - June 13, 2017, 10:41 am

Some killer info here. Liking this concept and hope it helps out Ether!

NurSpec - June 13, 2017, 10:42 am

OP is one of the smartest members we have on HackForums when it comes to crypto currencies and technology. Fantastic write-up, thanks for sharing all of the information you have gathered. I hope the mining aspect doesn't make ETH tank, although I doubt it and can only see this being a positive move.

Kill Joy - June 13, 2017, 1:21 pm

(Jun 13, 2017 09:23 AM)BitMoney Wrote: [\[CITE\]](#) So Ethereum will pass Bitcoin after this? Ethereum is already on track to pass bitcoin regardless.

(Jun 13, 2017 10:42 AM)NurSpec Wrote: [\[CITE\]](#) OP is one of the smartest members we have on HackForums when it comes to crypto currencies and technology. Fantastic write-up, thanks for sharing all of the information you have gathered. I hope the mining aspect doesn't make ETH tank, although I doubt it and can only see this being a positive move.

I don't think it will tank. Initially, likely, but it'll go back on track as normal. There will be less ETH coming into circulation. Low supply, high demand = higher price.

metaph0rbia - June 13, 2017, 2:18 pm

OP i didnt read all of the pages of replies so forgive me if you answered this already but is there a date set for POS? I heard late this year but i also hear it could get pushed until next year. So please can u link source for ETA of POS. Also do you think it might change with the sudden influx in crypto currencies across the world, ETH doing so well do you think that they will wait because y'know...why mess with a good thing? While we are at it, even people getting into mining now its worth because you will hit ROI before POS happens so be quick. Also do you think the soft fork and the hard fork will cause a bump in ETH or decrease?

Kill Joy - June 13, 2017, 2:43 pm

(Jun 13, 2017 02:18 PM)metaph0rbia Wrote: [\[CITE\]](#) OP i didnt read all of the pages of replies so forgive me if you answered this already but is there a date set for POS? I heard late this year but i also hear it could get pushed until next year. So please can u link source for ETA of POS. Also do you think it might change with the sudden influx in crypto currencies across the world, ETH doing so well do you think that they will wait because y'know...why mess with a good thing? While we are at it, even people getting into mining now its worth because you will hit ROI before POS happens so be quick. Also do you think the soft fork and the hard fork will cause a bump in ETH or decrease?

Ethereum wasn't meant to exactly be used as money. They're wanting to expand and improve their technology. This is the most innovating coin there is right now. I don't think the forks will have any impacts besides maybe a 24 hour period where it dips.

As for an official date.. Late 2017. I can't find an official source from Buterin on my phone. I'll update this post when I find it.

Mr Kewl - June 13, 2017, 2:49 pm

Keep up the good work buddy.

metaph0rbia - June 13, 2017, 2:54 pm

(Jun 13, 2017 02:43 PM)Kill Joy Wrote: [\[CITE\]](#) Ethereum wasn't meant to exactly be used as money. They're wanting to expand and improve their technology. This is the most innovating coin there is right now. I don't think the forks will have any impacts besides maybe a 24 hour period where it dips.

As for an official date.. Late 2017. I can't find an official source from Buterin on my phone. I'll update this post when I find it.

Sounds good, good post btw

NightForce - June 13, 2017, 3:20 pm

Great read, thanks for the solid info OP.

Kill Joy - June 13, 2017, 4:24 pm

If anyone has any questions I'll be back at my computer in about 2 hours to answer them all.

SLY - June 13, 2017, 4:32 pm

HQ post thanks for the share OP.

Kill Joy - June 13, 2017, 7:03 pm

(Jun 13, 2017 02:54 PM)metaph0rbia Wrote: [\[CITE\]](#) Sounds good, good post btw
Looking back at it, I can't find anything where Buterin talks about a general timeframe. I know I read I think on reddit somewhere, but even then he said he wasn't 100% sure when either.

<https://steemit.com/ethereum/@bunny/ethereum-to-switch-to-pos-before-november-1-2017>

<https://cointelegraph.com/news/ethereums-2017-roadmap-flexibility-pow-to-pos-improving-ecosystem>

Doesn't give a real good source.

His reddit name is /u/vbuterin

Yell - June 13, 2017, 7:09 pm

What exactly are my coins doing / where are they when I stake them? What are returns like on staked ETH?

Marv48 - June 13, 2017, 7:14 pm

This is a great post, I knew some of it but it filled in where I didn't know much. Thanks again.

Kill Joy - June 13, 2017, 7:18 pm

(Jun 13, 2017 07:09 PM)Yell Wrote: [\[CITE\]](#) What exactly are my coins doing / where are they when I stake them? What are returns like on staked ETH?

Your coins are locked (bonded) and sent to the Casper Contract (smart contract) where they will be "virtually mining" verifying the blocks. As of right now, I think the plan is to have the contracts last 4 months, but I also read somewhere they would like to give the option for people to pullout early.

Gizmo - June 14, 2017, 1:22 pm

This thread is on the 5th page already? What... So much useful information.

Kill Joy - June 14, 2017, 4:34 pm

If anyone has questions about this topic, feel free to PM me or ask here, I'll give you answers with official sources. I'm not pulling any of this out of my ass.

POLY MATH - June 17, 2017, 8:48 am

Consensus member here. Great guide from another.

Stay tuned for more quality informational and tutorial thread.

Kill Joy - June 18, 2017, 9:09 am

Knowledge is power. Writing today about the upcoming BTC fork as some people have asked about it.

Amp - June 18, 2017, 9:57 am

Thank you for this thread and the information.

Danny Khalifa - June 18, 2017, 9:58 am

Thank you for this information. Much appreciated.

QoL?? - June 18, 2017, 10:05 am

I'm interested in seeing how the Casper system works once they provide more information.

Alek Shieldhart - June 18, 2017, 11:29 am

Great post. I am new to this and haven't built a rig yet but I have some questions.

Since ETH is moving from PoW to PoS, how do you exactly "mine" coins with PoS?

Also, how long or when will they move to PoS?

I mean, if I build a rig now, ROI would be in a few months but if they suddenly change before that, then what are we to do with the GPU's from the mining rig?

Kill Joy - June 18, 2017, 11:47 am

(Jun 18, 2017 11:29 AM)Alek Shieldhart Wrote: [\[CITE\]](#) Great post. I am new to this and haven't built a rig yet but I have some questions.

Since ETH is moving from PoW to PoS, how do you exactly "mine" coins with PoS?

Also, how long or when will they move to PoS?

I mean, if I build a rig now, ROI would be in a few months but if they suddenly change before that, then what are we to do with the GPU's from the mining rig?

Staking would become the new sort of mining. You would get your money back before it completely happens. There is no exact date other than general time to start the switch at the end of 2017. They are not making the switch in one full go, there will be a hybrid system in place. When it's fully switched, you can go mine other coins that us PoW. This is all detailed in the OP.

Alek Shieldhart - June 18, 2017, 12:03 pm

(Jun 18, 2017 11:47 AM)Kill Joy Wrote: [\[CITE\]](#) Staking would become the new sort of mining. You would get your money back before it completely happens. There is no exact date other than general time to start the switch at the end of 2017. They are not making the switch in one full go, there will be a hybrid system in place. When it's fully switched, you can go mine other coins that us PoW. This is all detailed in the OP.

I see. I read about the hybrid thing but didn't know exactly when in terms of months are they gonna start to implement it. Thanks for your informational answer.

Now I need to start looking for some cheap ones.

Kill Joy - June 19, 2017, 3:45 pm

(Jun 18, 2017 12:03 PM)Alek Shieldhart Wrote: [\[CITE\]](#) I see. I read about the hybrid thing but didn't know exactly when in terms of months are they gonna start to implement it. Thanks for your informational answer.

Now I need to start looking for some cheap ones.

It'll be an interesting transition. I hope it all goes smoothly, but I think we can expect a few bumps in the road but nothing bad.

Jura55 - June 19, 2017, 4:18 pm

So correct me if I'm wrong, but from what I read and understand PoS is basically you putting in your own coins to mine you more coins?

There will still be a way to profit IF you possess eth?

Thanks for posting this btw!

Kill Joy - June 19, 2017, 4:40 pm

(Jun 19, 2017 04:18 PM)Jura55 Wrote: [\[CITE\]](#) So correct me if I'm wrong, but from what I read and understand PoS is basically you putting in your own coins to mine you more coins?

There will still be a way to profit IF you possess eth?

Thanks for posting this btw!

Yes, but you would need a very large amount of coins in order to make a profit. Like 1000-4000 coins.

Nick Elite - June 19, 2017, 7:14 pm

Yeah but we could mine other coins? no? like maybe ethereum classic? zcash??

Kill Joy - June 19, 2017, 8:02 pm

(Jun 19, 2017 07:14 PM)Spermie Wrote: [\[CITE\]](#) Yeah but we could mine other coins? no? like maybe ethereum classic? zcash??

Yes. No one is stopping you from switching to mining something else and still turning a profit.

Kill Joy - June 25, 2017, 2:20 pm

If anyone has any questions about this, let me know and I'll answer them. :)

Mezzishere - June 25, 2017, 10:57 pm

So what happens when people stop mining a certain coin that uses proof of work? Who verifies the transactions then?

That-1-Guy - June 26, 2017, 3:45 pm

if i had like 300 eth coins is there a way to calculate on average someone staking would make?

webdev77 - June 26, 2017, 4:15 pm

(Jun 26, 2017 03:45 PM)That-1-Guy Wrote: [\[CITE\]](#) if i had like 300 eth coins is there a way to calculate on average someone staking would make?

100% impossible to even estimate until the switch is made.

Kill Joy - June 26, 2017, 9:45 pm

(Jun 25, 2017 10:57 PM)Mezzishere Wrote: [\[CITE\]](#) So what happens when people stop mining a certain coin that uses proof of work? Who verifies the transactions then?

No one verifies them. Without verification it wouldn't be accepted by anyone. But if no one was mining, the blockchain is pretty much dead. When a coin's blockchain splits, economic majority or user majority will decide what chain they want to accept and eventually the other chain will die because it would not be beneficial to mine that chain anymore.

(Jun 26, 2017 04:15 PM)webdev77 Wrote: [\[CITE\]](#) 100% impossible to even estimate until the switch is made.

This is correct; however, Buterin himself suggested that in order to make a profit, one would need to stake 1000-4000 ETH.

Mr Kewl - June 27, 2017, 1:44 am

(Jun 26, 2017 09:45 PM)Kill Joy Wrote: [\[CITE\]](#) This is correct; however, Buterin himself suggested that in order to make a profit, one would need to stake 1000-4000 ETH.

That's a huge amount of Ethereum, but then you need large amount of coins for POS.

Kill Joy - June 29, 2017, 7:15 am

(Jun 27, 2017 01:44 AM)Mr Kewl Wrote: [\[CITE\]](#) That's a huge amount of Ethereum, but then you need large amount of coins for POS.

Yeah. I think miners will switch to ETC though. I'm thinking about buying a lot of them before autumn.

FaberCastell - July 1, 2017, 5:05 am

(Jun 13, 2017 06:12 AM)Kill Joy Wrote: [\[CITE\]](#) Probably only if Ethereum wants to allow that, but they probably won't. The nodes will change. I don't know an exact answer for this question right now.

Looked it up. Casper will have both POW+POS, and the goal is to gradually increase difficulty to get rid of the miners over time and scale up POS.

Because if it straight up went to POS, miners would continue mining the old chain and there would be a hard fork.

Kill Joy - July 9, 2017, 5:40 pm

(Jul 1, 2017 05:05 AM)FaberCastell Wrote: [\[CITE\]](#) Looked it up. Casper will have both POW+POS, and the goal is to gradually increase difficulty to get rid of the miners over time and scale up POS.

Because if it straight up went to POS, miners would continue mining the old chain and there would be a hard fork.

This is exactly right.

Kill Joy - July 13, 2017, 9:10 am

<https://www.ethnews.com/the-casper-proof-of-stake-algorithm-prepare-to-commit>

Very good article about Ethereum, Proof of Stake, and the Casper contract. May make a separate thread for this.

Kill Joy - July 25, 2017, 9:52 pm

Let's not forget about other coins while BTC is dominating the headlines. :)

Tomorrow I am starting a whole thread dedicated to the Casper Contract. It's amazing.

Undefined - July 26, 2017, 12:26 pm

I understand that Ethereum switching to PoS is important and exciting, but I am sad they're going away from PoW.

MODERN - July 26, 2017, 12:32 pm

My biggest question would what will this do to the current value of ETH?

I bought in at around \$6 so I've been quite well off with my investment, should I pull my ETH out though before this goes into play or will the value not change much?

Kill Joy - September 1, 2017, 11:44 pm

Bringing this back up. Part two is being written now.

Breekee - September 2, 2017, 10:48 am

(Sep 1, 2017 11:44 PM)Kill Joy Wrote: [\[CITE\]](#) Bringing this back up. Part two is being written now.

Thanks for keeping us up to date mate,you are amazing

Death - September 2, 2017, 10:48 am

Great in depth explanation! Hats off to you!

Kill Joy - September 2, 2017, 11:29 am

(Sep 2, 2017 10:48 AM)Breekee Wrote: [\[CITE\]](#) Thanks for keeping us up to date mate,you are amazing

Part 2 is here: <https://hackforums.net/showthread.php?tid=5708874>

BaldCunt - February 4, 2021, 3:04 am

I think there will be a dip after pre-release as people tend to panic when huge changes come.

BalleJatta - February 4, 2021, 5:20 am

late 2017! dam they missed the deadline by couple years

Itachi Uchiha - February 4, 2021, 7:30 am

(Feb 4, 2021 03:52 AM)Focus Broken Wrote: [\[CITE\]](#) Exciting news! ?

Thanks [Kill Joy](#) ! I'm a bit confused but I'm glad you are here to answer my questions. Here's a couple that need important answers:

First question: What is the underlying consensus mechanism in the current implementation that determines the PoS checkpoint in a decentralized way?

Second question: How does proof of stake make transactions quicker? PoS is a consensus mechanism, not a scaling mechanism.

Third question: Don't you think it's sinister that Ethereum would "not allow" the PoW chain they sold to investors to compete with the PoS chain?

You really went digging for this one bud lol

Marvelous - February 4, 2021, 9:52 am

(Feb 4, 2021 03:52 AM)Focus Broken Wrote: [\[CITE\]](#) Exciting news! ?

Thanks [Kill Joy](#) ! I'm a bit confused but I'm glad you are here to answer my questions. Here's a couple that need important answers:

First question: What is the underlying consensus mechanism in the current implementation that determines the PoS checkpoint in a decentralized way?

Second question: How does proof of stake make transactions quicker? PoS is a consensus mechanism, not a scaling mechanism.

Third question: Don't you think it's sinister that Ethereum would "not allow" the PoW chain they sold to investors to compete with the PoS chain? As soon as I seen the title of this thread, then I seen this thread is from 2017. I knew it was you that would bump this shit. You really need a better hobby.. or a life.

T0Bi - February 4, 2021, 10:07 am

I'm pretty sure you already know all the answers, but for all the newcomers, here we go:

(Feb 4, 2021 03:52 AM)Focus Broken Wrote: [\[CITE\]](#) First question: What is the underlying consensus mechanism in the current implementation that determines the PoS checkpoint in a decentralized way?

The first block of an epoch is a checkpoint for the blocks of the prior epoch (1 epoch = 32 Blocks). It's hardcoded. Every node can count to 32.

Not sure if I understand your question.. You're usually expecting an answer you already know in order to spread misinformation or whatever but if it's a serious question, please rephrase it.

You can read more about it here: <https://ethos.dev/beacon-chain/>

(Feb 4, 2021 03:52 AM)Focus Broken Wrote: [\[CITE\]](#) Second question: How does proof of stake make transactions quicker? PoS is a consensus mechanism, not a scaling mechanism.

The PoW consensus mechanism has two parts for mining a block. Validate transactions and put them in a block. Guess random numbers for X Minutes/Seconds (Bitcoin: ~10min, ETH: ~14sec).

The first part is the same in proof of stake, the second isn't. You vote with your stake, not your electricity.

Hence a theoretically lower possible block time leading to higher tx/sec.

Afaik the blocktime for Eth 2.0 (beaconchain) is set to 12 seconds.

The real improvement comes through sharding, which means 64 parallel blockchains and therefore higher throughput.

(Feb 4, 2021 03:52 AM)Focus Broken Wrote: [\[CITE\]](#) Third question: Don't you think it's sinister that Ethereum would "not allow" the PoW chain they sold to investors to compete with the PoS chain? No one can allow or prohibit anything and you know that.

If you're talking about the ice age / difficulty bomb, well if people/miners don't like it they can always fork away. That's the beauty of decentralization and open source code. We saw it with Ethereum Classic and Bitcoin Cash.

So if there would actually be demand for the PoW chain, miners can simply continue it. No one would use it obviously, but if they like to, why not.

THE RULER - February 4, 2021, 4:27 pm

(Feb 4, 2021 05:23 PM)Focus Broken Wrote: [\[CITE\]](#) There's plenty more too. This forum has been obsessed with Ethereum for years... until it comes time to justify the technical claims made by the developers, then you won't hear a single word. Here's the best example:
<https://hackforums.net/showthread.php?tid=5751418&highlight=bitcoin>

?

Feel free to bump all of my wrong calls or false technical claims. Go back as far as you want, you won't find any.

I don't know all the answers about Ethereum, I'm genuinely curious as to how the "byzantine generals problem" and the "nothing at stake problem" can be solved by anything other than proof of work. But just because I don't know all the answers doesn't mean I can't spot one that's clearly wrong, if the answer is right, then it can be explained in a logical manner and I would be convinced to switch. Keep in mind that PoS is an OLDER theoretical consensus mechanism than PoW, PoW was the groundbreaking technology that made decentralized currency possible.

Okay I'll rephrase it: Checkpoints don't create consensus, it only pushes consensus back 32 blocks. How does your node decide which chain to add blocks to when it is presented two chains with checkpoints at the same block height?

^ This concern also ignores the fact that adding a checkpoint (on PoW chains too) makes it so a new user can no longer trust chain history that was created between genesis block and the latest checkpoint unless they were online at that time to validate it themselves.

Damn that a was long read.

There's no "two parts" for mining a block in PoW, validating transactions on your node and generating hashes on a miner are completely independent. Everything you just said was completely made up Imfao, there's no "theoretically" about it, here's Satoshi Nakamoto explaining that you are wrong back in 2010:

So now you have 64 shards to fully validate. That's not "scaling", you just increased your technological burden by a factor of 64.

Why would you intentionally put a killswitch in a "decentralized" blockchain in the first place? The very existence of the difficulty bomb is DESIGNED to be a centralizing factor.

Absolutely slaughtered

Kill Joy - February 6, 2021, 9:23 am

(Feb 5, 2021 05:04 AM)Focus Broken Wrote: [\[CITE\]](#) Yeah, people take for granted how secure PoW is. If you don't understand how PoW reaches consensus, then you won't be able to spot the unavoidable vulnerabilities in PoS.

Narrator: He was pulling it out of his ass:

Really shitty of the OP to shill people a broken product that he invested in, and then disappear when consumers find out the product they bought was defective the whole time.

The product isn't the same as it was planned and laid out to be 4 years ago. I lost interest in caring about it overtime and things have gotten way too technical for me to keep up with and understand it.

All you do is pick apart people on this forum for your entertainment and to humiliate them. Why should I keep watching you quote me from 3-4 years ago? It's annoying as hell and like kicking a dog who's asleep.

Omniscient - February 6, 2021, 1:36 pm

(Feb 6, 2021 12:00 PM)Focus Broken Wrote: [\[CITE\]](#) I've been asking you these same questions for the past 4 years and you've been dodging them for 4 years... I'm not saying you have to admit any fault, I'm just continuing to ask: Why won't anyone hold Vitalik accountable for this???

People are STILL continuing to defend Vitalik. WHY??? The coin he advertised in the ICO was a proof of stake (e.g. inflation free) product that was scalable, and "unstoppable". What investors got was inflated 58% (so far) from PoW, unscalable, and censored by Vitalik himself.

I got you on ignore for a reason. You're a cunt.

I advise everyone to ignore you.

But to address your bullshit question about holding Vitalik accountable. What the hell does that even mean? Should we arrest him?

You gotta just STFU. We're all sick and tired of your bullshit.