WAVE
Financial

Ethereum 2.0 staking, a worthwhile investment?

Table of Contents

Background

The Ethereum network today is overrun with traffic, causing transaction fees to spike to levels that are not affordable for many use cases. This is partially due to the success of DeFi projects, where users don't mind paying the high transaction fees because of the financial value of the transactions being made. (In Ethereum, transaction fees are typically referred to as "gas" costs, since the fees do not just fund transactions but actual applications running on the Ethereum blockchain.) This is making it very difficult for non-finance dApps (decentralized applications built on top of Ethereum) to operate on Ethereum. A DeFi user may not mind paying $100 for a complex financial transaction to invest hundreds of thousands of dollars of cryptocurrency, but a gamer trying to trade a $5 in-game item doesn't want to pay $5 in transaction fees.

To ameliorate these issues, the Ethereum Foundation has been planning a very complex upgrade, Ethereum 2.0 (ETH2), to enhance the security, speed, efficiency, and scalability of the Ethereum network, so that it can process more transactions, ease bottlenecks, and fit more use cases, especially outside of finance.

The first phase of this multi-year upgrade to increase performance and improve security launched on December 1, 2020. ETH2 is a very complicated upgrade to an in-production blockchain already being used by many people and projects today. The developers need to make sure that all these applications continue to work during and after the transition. Because of this, the upgrade has been split into multiple phases over several years.

The question we ask and attempt to answer in this research paper is, *will buying the ETH token following this upgrade be a sound investment choice?* In doing so, we will also illustrate where Ethereum is heading, how far it has come, and what risks and rewards lie ahead.

A Little Background - Proof of Work vs Proof of Stake

Proof of Work

Mining capacity depends on computional power

Miners receive block rewards to solve a cryptographic puzzle

Hackers would need to have a computer powerful than 51% of the network to add a malicious block, leading to 51% attack

Proof of Stake

Validating capacity depends on the stake in the network

Validators do not receive a block reward, instead, they collect transaction fees as reward

Hacker would need to own 51% of all the cryptocurrency on the network, which is practically impossible and therefore, 51% attacks impossible

ETH2 brings with it the major improvements of Proof of Stake (PoS) and sharding. PoS is an alternative to Proof of Work (PoW) and is seen as a more energy efficient and secure consensus algorithm for blockchain protocols. PoW blockchains (such as Bitcoin and ETH1) reward miners for solving cryptographic puzzles in order to validate transactions and create new blocks. This secures the blockchain, but requires massive amounts of energy.

On the other hand, PoS blockchains use a mechanism called staking to secure the blockchain and produce new blocks. Staking is the process by which validators are selected to create a new block. The probability of being selected to produce/validate a block is proportional to how many coins the validator holds. Thus anyone with a minimum number of coins can participate in staking and earn more coins relative to their amount staked. Most new blockchains coming out are PoS from the beginning. Some other major PoS chains include Tezos, Cosmos, Cardano, EOS, PolkaDot, Algorand, Avalanche, Tron, and many more.

Additional info: What is PoS? (Ethereum Roadmap)

Getting into the Detail - Validators

To participate in ETH2 staking requires operating a validator yourself or lending your tokens to someone else. In ETH2, validators propose, verify, and vouch for the validity of blocks. In exchange, honest validators receive financial rewards. Validators need to post 32 ETH2 as collateral which will be slashed (forfeited) for producing bad blocks or going offline. This architecture was created to try to ensure decentralization of the network. Each 32 ETH2 requires another validator instance to be configured and deployed, although these instances can share resources. Those with less than this amount, or those that are not technically able or willing to run their own node, will need to lend their tokens to a pool (or leave them on an exchange), a process called delegation. Unfortunately, ETH2 is pure proof of stake, without delegation, a mechanism which allows a token holder to safely delegate tokens to a 3rd party for staking. Since delegation is not implemented by the protocol and must be added by 3rd party smart contracts, this results in additional security risks and high commissions. Most other modern PoS blockchains support delegation (non-custodial staking) natively, whereby a user can retain coins in his/her own wallet (and earn rewards directly) but delegate the block producing rights to a 3rd party without any security risk. It is worth noting that ETH2 has been designed to support hundreds of thousands of validators, far more than other blockchains, and an exceptional amount of decentralization.

The only way to get ETH2 tokens for validator collateral is to make a one-way ETH transaction to the deposit contract on the current Ethereum chain, which burns ETH1 and mints ETH2 tokens. (See more info below.) Technically, this generates a new token called BETH (Beacon Chain ETH) which exists only on the Ethereum 2 Beacon Chain, referred to simply as ETH2 in this report.

Validators have certain responsibilities. Those that actively participate in consensus receive rewards. Those that are offline are penalized. The penalties for being offline are equal to the rewards for actively participating, up to a maximum of 16 ETH (half the 32 ETH stake). If a validator keeps being penalized and its stake drops to 16 ETH, it will be rejected from the network, and funds will be locked until phase 2. Also, once a validator decides to quit, they cannot start again until phase 2, and funds will remain locked for this period (likely 2 years).

See also: Official ETH2 calculator / Validator FAQ

Building the New Ethereum Protocol - ETH2 Phases

It's important to remember that the current launch of ETH2 is just the start of a multi-year upgrade with, despite the naming, four distinct phases.
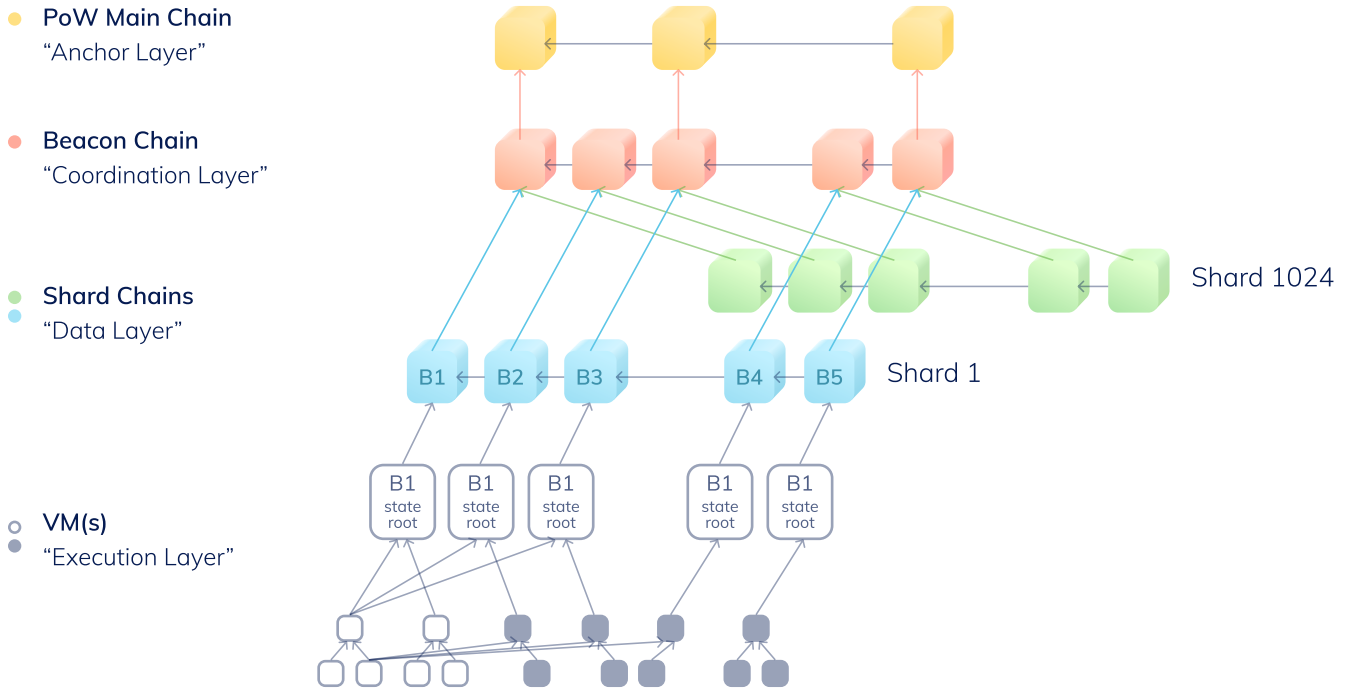
How they relate: ETH1x, ETH2, & Rollups

Phases not shown to scale - graphic by @trent_vanepps

ETH1x - existing user data, dapps

Rollups (external to protocol)

Shard 1

Shard ...

ETH1x Shard

Ethereum
In the future, it will all just be called Ethereum

Deposit contract state bootstraps Phase 0 Genesis

Phase 0

Proof of Stake Beacon Chain starts and lives on its own for a bit. Rollups can leverage ETH1x for Data Availability ↑

Phase 1

Data Sharding - Shards anchored to the Beacon Chain, but without native transaction execution. Rollups / L2 can now use Shards for Data Availability ↑ very useful for offchain scaling.

Phase 1.5

ETH1x gets slotted into the Beacon Chain architecture as a single shard. This connects existing ETH1x user state to PoS consensus, replacing miners and PoW

Phase 2

Existing Shard gain the ability to execute transactions natively ↕. Research continues on the optimal integration of this feature.

Source: @trent_vanepps Tweet

Phase 0 – Beacon Chain (December 2020)

Basically it is just PoS with nothing else. It is not particularly useful. One advantage over ETH1 is that it will support finality, which is especially useful in financial applications. (A full discussion of finality is outside the scope of this report, but here are some comments about finality from Vitalik Buterin in 2016.) It's called the Beacon Chain because it will be used for all the shards to communicate in the future.

Source: https://media.consensys.net/state-of-ethereum-protocol-2-the-beacon-chain-c6b6a9a69129

Phase 1 – Shard Chains (one year?)

According to news website Decrypt:

> *The current Ethereum set-up has a blockchain consisting of a single chain with consecutive blocks. This is secure, but very slow and not efficient. With the introduction of shard chains, this blockchain is split up, enabling transactions to be handled in parallel chains instead of consecutive ones. This speeds up the network, and can scale more easily.*

Shard chains are the key to future scalability as they allow parallel transaction throughput and there will be 64 in Phase 1 (more maybe added as hardware improves; but this is unclear at this moment in time). Each shard chain is like one copy of the current ETH1 chain operating in parallel. The shard chains use the Beacon Chain for coordination.

3 Types of Chains

Current Chain	Beacon Chain	Shard Chain
Proof of Work	**Proof of Work**	**TX & Data**
We will be transitioning to the beacon chain from here	Validators will reside here and link to the Shard Chains	Multiple shard chains - each holding a portion of transaction

Source: Ethereum Casper V2: Beacon Chain & Sharding Explained Simply (Mango Research)

In this phase there still are no smart contracts and no account balances.

> *It'll be like a trial run for the sharding structure rather than an attempt to use shards to scale.*

his means maximum TPS improvement over ETH1 is only around 64x at this time, however it's possible that more shards will be added in the future. The current Ethereum blockchain's capacity is about 15-30 TPS. An increase of 64x brings us to approximately 1000-2000 TPS. Using layer 2 scalability technologies like rollups combined with phase 1, some people are predicting a throughput of 100,000 TPS by the end of 2021, but it is not yet clear when this will be achieved.

Phase 1.5 – Integration with ETH1 ("estimated 2021", but could be 2022)

The existing Ethereum mainnet would be added to the Beacon Chain as a shard chain, transforming the network into a PoS consensus network from the current PoW consensus algorithm. At this point the existing PoW ETH1 miners will be forced to quit. This step is bigger than many people realize. About phase 1.5, Danny Ryan of the Ethereum Foundation says:

> *Phase 1.5 is huge. ETH2 is built for Ethereum and at this point, ETH2 becomes Ethereum. All of the applications we know and love become integrated in the upgraded eth2 consensus mechanism, retaining the feature-set we are used to while simultaneously opening up the vast new landscape of a secure proof-of-stake consensus with native access to a highly scalable data layer. This is the meat of the process in my opinion. This is the moment of grand success as we anchor Ethereum fully into its new reality.*

Phase 2 – State Execution (2-3 years)

Smart contracts and accounts will finally be supported and users can freely withdraw and transfer ETH2 tokens.

> **Special note: Alternate scenario involving rollups**
>
> *It is an open question when and how Ethereum 1.0 accounts and contracts will be migrated to Ethereum 2.0 (Possibilities) Also, it is possible that phase 2 might get canceled and replaced with a completely different strategy.*

In this scenario, Vitalk Buterin has written the following:

- Today, Ethereum has ~15 TPS.
- If everyone moves to rollups, we will soon have ~3000 TPS.
- Once phase 1 comes along and rollups move to eth2 sharded chains for their data storage, we go up to a theoretical max of ~100000 TPS.
- Eventually, phase 2 will come along, bringing eth2 sharded chains with native computations, which give us... ~1000-5000 TPS.
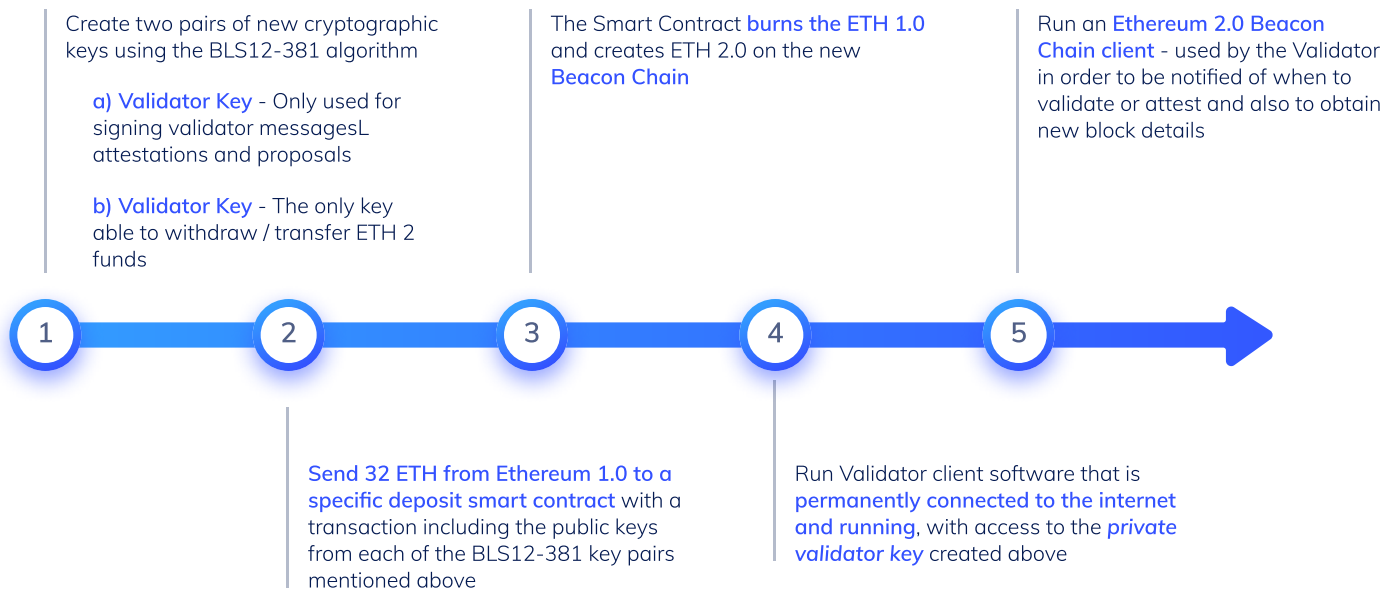
This implies a "phase 1.5 and done" approach to eth2, where the base layer retrenches and focuses on doing a few things well - namely, consensus and data availability.

Source: A rollup-centric Ethereum blueprint, by Vitalik Buterin (Oct. 2, 2020)

More info on phases from Ethereum researchers.

Step-by-Step - Launch of Phase 0

Becoming a Validator

1. Create two pairs of new cryptographic keys using the BLS12-381 algorithm

  a) Validator Key - Only used for signing validator messagesL attestations and proposals

  b) Validator Key - The only key able to withdraw / transfer ETH 2 funds

2. **Send 32 ETH from Ethereum 1.0 to a specific deposit smart contract** with a transaction including the public keys from each of the BLS12-381 key pairs mentioned above

3. The Smart Contract **burns the ETH 1.0** and creates ETH 2.0 on the new **Beacon Chain**

4. Run Validator client software that is **permanently connected to the internet and running**, with access to the *private validator key* created above

5. Run an **Ethereum 2.0 Beacon Chain client** - used by the Validator in order to be notified of when to validate or attest and also to obtain new block details

Source: https://consensys.net/blog/blockchain-explained/my-journey-to-becoming-a-validator-on-ethereum-2-0/

At the first week of November, the Ethereum foundation deployed the "launch contract", which is a smart contract on the existing Ethereum blockchain where validators must deposit their ETH in order to get the ETH2 required to start a validator. Almost immediately, as a show of support, the cryptocurrency's cofounder Vitalik Buterin sent 3200 ETH (worth approximately $1.4 million) to the deposit contract, enough for 100 validators.
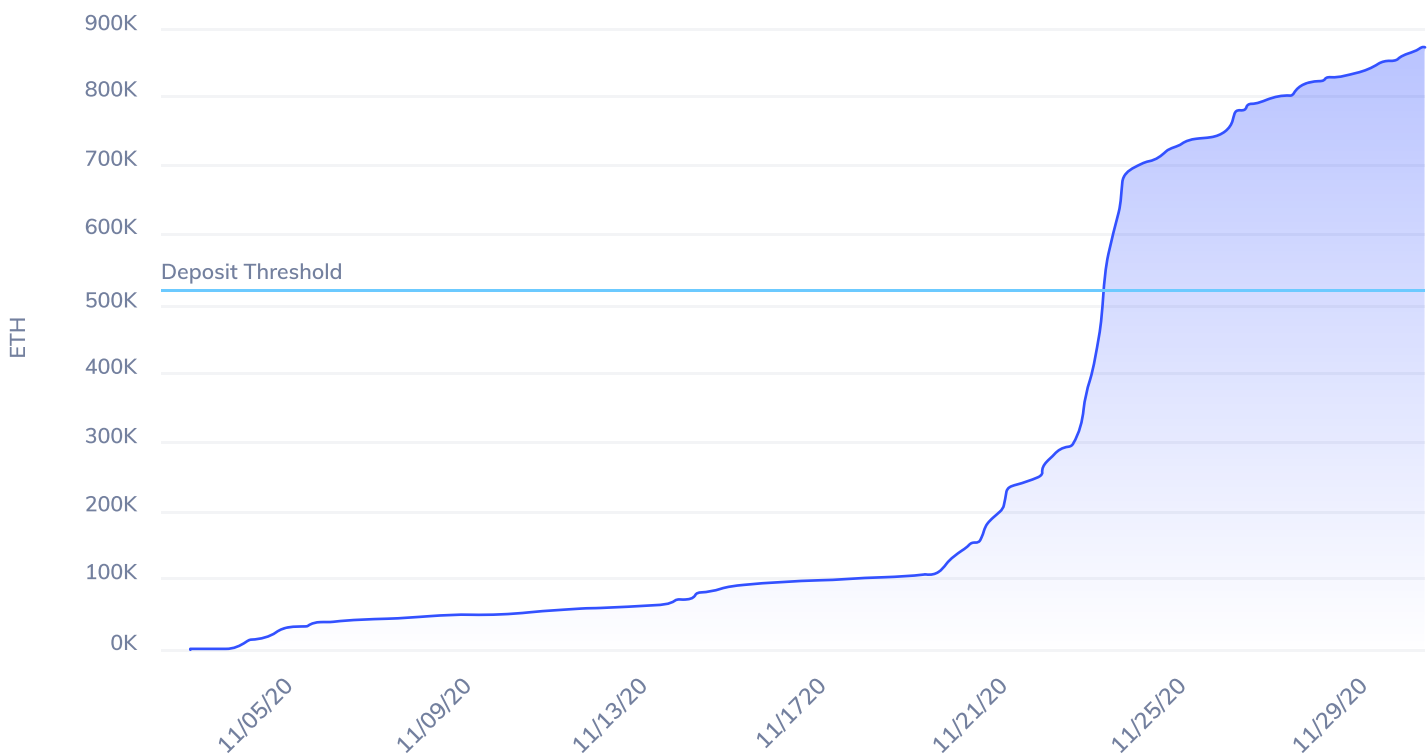
524,288 staked ETH was required to launch (16,384 validators). This number was calculated to make it economically difficult to attack the network. This amount was required to be staked by November 24, for the new network to launch on December 1. The amount staked started off growing very slowly and it looked like the deadline might be missed; as of 11/13/20, 64,320 ETH were staked (12%), and as of 11/20/20, only 107,360 ETH (20%) were staked. However, at the very end things rapidly picked up steam and by the deadline, 694,368 ETH (worth over $400 million) was sent to the contract. Roughly the last 25% of the ether needed to meet the threshold was deposited into the contract in less than a four-hour timespan.

Note

The current amount of ETH2 staked can be easily checked on the ETH2 Launchpad under "Network Status." According to the launchpad, as of December 14, 1,466,369 ETH was staked. The Twitter account "Eth2 Rewards Bot" also tweets out similar information and more. It says the current yield is 15.31% (which drops every week as more ETH is staked). Since only a fixed number of new validators can join every week, there is a waiting queue for new validators, 14 days as of December 14.
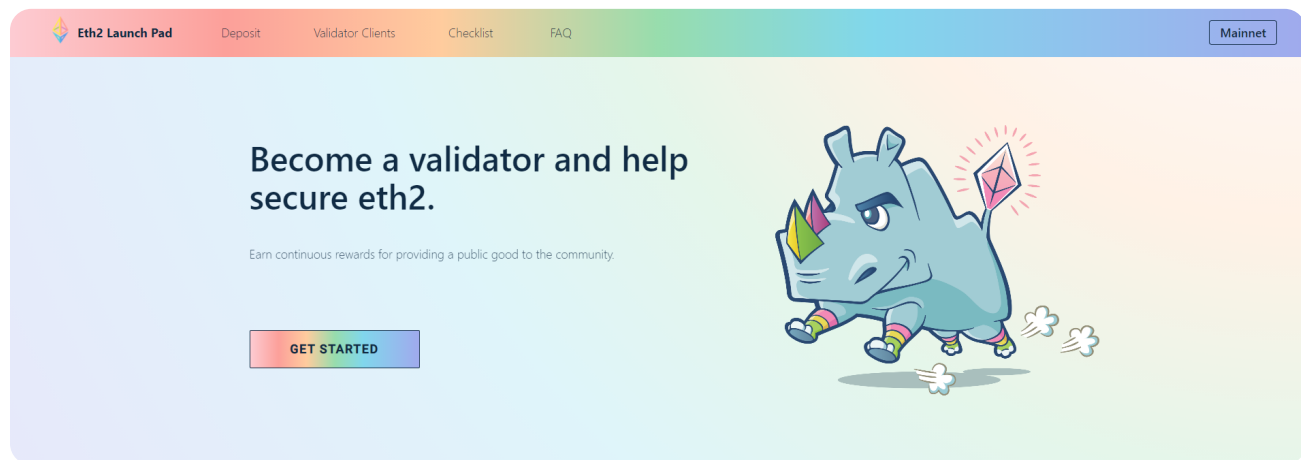
ETH2 Staked Over Time

Cumulative ETH Sent Over Time

Source: https://www.coindesk.com/valid-points-risks-rewards-staking-on-eth-2-0-validators

Getting Involved - Running a Validator

Source: Launchpad.ethereum.org

Many people are still struggling to understand what is required to run their own validator, or use a 3rd party validator. The blockchain software technology company ConsenSys is publishing a series of articles helping technical people set up their own validator. Bankless has also published a good tutorial on setting up a validator.

Besides the 32 ETH required to stake, operating a validator as specified costs $837 a year in cloud hosting fees. Running one's own validator is not something you can set up and walk away from. It requires a commitment to keeping the server up and running for 2 years. (As noted, it is possible to quit being a validator exactly once and without penalty, but the tokens will stay locked in that validator for another 1-2 years.) The operator will need to make sure the server is continuously up and running, apply security patches, and update all of the node software. This is a sizable commitment. However, 3rd parties are developing services to make this easier, as discussed below.

3rd Party Validators

At the time of writing, this information is rapidly changing and many products have been announced but not yet launched.

RocketPool

RocketPool was one of the first groups to announce their ETH2 staking service. They bill themselves as a "Decentralized ETH PoS Network", using smart contracts for custody of tokens. There was much hype around this announcement, however as of the start of December, the launch date is unclear, and other important details such as fees.

Stkr

Launched by ANKR on December 1, is a service that allows participants to stake with less than 32 ETH (min 0.5 ETH). Their architecture divides the work between fund providers, hardware providers, maintainers and ANKR stakers. They charge a **23% fee** and return a "new synthetic asset token" aETH (ERC-20) which is issued 1:1 to your ETH stake, so users can trade ETH locked up in STKR's staking. "aETH represents staked ETH2 plus earned final rewards." It will be interesting to see what aETH marketplace will be developed, its liquidity, and what price the market will value it at. Without enough liquidity, it might be meaningless.

STKR validator nodes can be run by ANKR corporation, run by 3rd party users using ANKR's cloud infrastructure, or run by 3rd party users on their own infrastructure. Node operators are paid ~10% (half of the fee). ANKR also provides simplified managed cloud services for those who want to set up their own validator, unrelated to the STKR service, so one could potentially pay for this service from ANKR then register as a STKR node operator and start collecting fees from other users.

Similar to aETH, **Coinbase** chief product officer Surojit Chatterjee announced yesterday the intention to create a market for staked ETH2 in a blog post. Coinbase has stated, in early 2021 they "will also enable trading between ETH2, ETH, and all other supported currencies providing liquidity for our customers."

Secondary markets for synthetic tokens like aETH or ETH2 might be able to address concerns around the lock-up period. It'll be interesting to see how liquid these markets become compared to other tokens, given the inherent counterparty risk associated with staking. A staked ether secondary market would probably be tied to the amount of ether held at a centralized exchange for staking. That could open up some exchanges to security concerns. This asset could be considered "staking derivatives or staking securities or securitized stake." Link

Codefi Staking API

ConsenSys is offering Codefi Staking API (staking "as a service") for institutions such as exchanges. First trials are with Binance, Crypto.com, DARMA Capital, Huobi Wallet, Matrixport and Trustology. We can expect that these companies will launch ETH2 staking products if they have not already.

Many exchanges are announcing plans to support ETH2 staking. It will be interesting to see how this plays out. For smaller retail investors, this may be the best option. Most likely, exchanges will charge high fees for this service. (For instance, Coinbase charges 25% fees for Tezos staking, where 5-10% is typical for 3rd party baking services.) However, they probably will provide some kind of alternate liquidity. Investors may be able to trade ETH2 tokens with other users on the exchange, but they would in essence be trading an IOU, and will not be able to take them off the exchange, as transfers are not supported. (See discussion of phases above.) **FTX** has announced it's considering trading a BETH IOU token as well.

Coin Metrics co-founder Jacob Franek spelled out in a tweet thread some thoughts about such IOU markets. He said a secondary market for staked ether tokens would only be as deep as the amount of ether locked in the deposit contract. Its trading quality would also be dependent on whether market makers began actively trading the theorized asset. The value of the token itself would be tied not only to the underlying inflation rewards stakers receive – between 8% and 15% annually – for depositing ether in the Beacon Chain, but also to the inherent risks from trading a product on top of the ever-under-construction Eth 2.0 blockchain. For example, penalties for failing to validate the new chain affect ether deposits. Those penalties would, at some point, affect how the staked ether token would trade.

In an email to customers on December 3, 2020, Kraken announced that they will offer ETH2 staking as well as a market for trading "staked ETH for unstaked ETH." They note a few points, which are indicative of the issues everyone will face. Namely, they plan to launch a special trading pair between staked ETH and unstaked ETH to offer liquidity to investors who have locked up their ETH in staking. This market will not be offered to citizens of the US and Canada. Also, it is unknown the liquidity that will develop on this market, and if the liquidity turns out to be poor, the market may not survive until later phases of ETH2.
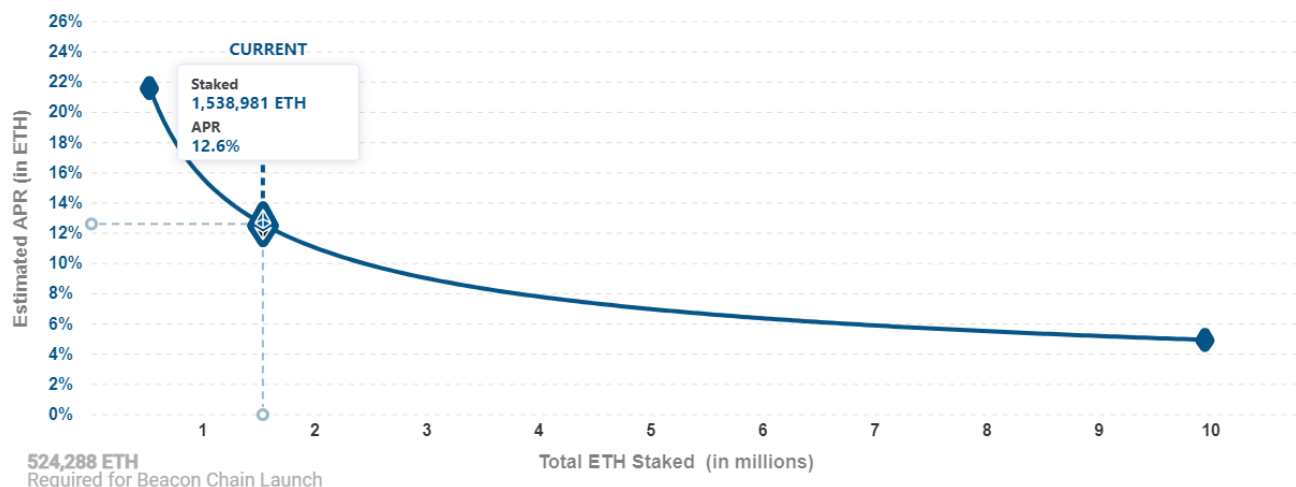
Several companies, including **Darma Capital**, are planning to offer intermediated staking that would allow users to continue accessing their capital. Through its LiquidStake initiative, both retail and institutional stakers can delegate their capital and maintain the ability to use it as collateral to receive USD Coin (USDC) loans. Unlike other staking derivative proposals, LiquidStake will not create new tokens to represent the bonded Ether (ETH).

> ***Remember, all 3rd party validators entail security risk, as delegation is not supported by the base protocol.*** *Staked tokens could be compromised by a malicious actor, as they do not remain in one's wallet.*

The Investment Case and ROI - How much can one earn?

First, let's discuss precise yields. "Rewards will be highly variable in ETH2 by design and are best observed through a probabilistic simulation. As a result, you will only know exactly what your reward is once it is received." (Quote from official ETH2 calculator sheet).

ETH2 staking rewards range from the following. For comparison, a snapshot of DeFi yields from more trusted projects shows yields sitting around 5%–7%, according to DeFi Rate.

Source: ETH2 Launchpad Interactive rewards graph ("Staking and Rewards" heading). The highlighted data point shows the state of the network as of December 14.

21.6%	4.9%	2.16%	1.53%
at minimum 524k (~0.47%) of the network staking	at 10M (~9%) staking	at 55M (~50%) staking	at 110M (~100%) staking

These figures are given in APY, such that if one stakes one validator, 32 ETH, with a 10% APY, one would earn 3.2 ETH after one year. **It is worth nothing that staking rewards do not compound** (link).

Each 32 ETH validator gets the same reward every time. After transferring ETH2 tokens is enabled (2+ years), after accumulating 32 ETH in staking rewards, one could start a new validator. In this way, partial compounding is possible, but is complicated. Rewards are calculated and paid per epoch (a period of time during which transactions are proposed and validated by token deposits).

On December 2, one day after launch, Coindesk reported that active validators are, on average, earning 0.00403 ETH/day, or $2.36/day at time of writing. This amount will certainly decrease as the number of validators increases.

Developers are only expecting that 20-40% of the network will stake. Compare this to Tezos, which has 80% of the network staking (at a ~6% yield), but minimal DeFi use cases at this time. (Tezos was one of the first major blockchains to launch with delegated PoS).

See also official calculators: ETH2 calculator worksheet and Interactive rewards graph ("Staking and Rewards" heading). **Beware, not all 3rd party calculators are accurate!** Especially with assumptions such as what percentage of the network will stake.

Investors must balance all of the above factors.

What are the Risks - Downside

Let's summarize some of the downside risks. Remember, funds are locked for a long time. Transfers between validators are disabled until at least phase 1 (one year), but even this does not allow free withdrawals. Validators will have to wait until phase 2 (around two years) to be able to withdraw funds at will. As mentioned, ETH2 can not be converted back to ETH1. With transfers disabled until at least phase 1, there's no way for a validator to voluntarily exit and then restart later. **This means validators need to be in it for the long haul**. They must keep their server up and running for 1-2 years, updating and monitoring frequently.

Then there are early adopter risks, such as potential for software bugs. These bugs may result in slashing penalties. Already, bugs were found in one of the ETH2 client's software from Prysmatic Labs which caused everyone using it to miss the first week's worth of rewards. Also,let's not forget the relatively low APY, which is about ~5% APY with 10% of network staking, and can drop to a low of <2%.

Conclusion

ETH2 Myths - True or False?

⑦ Is it secure?

> 💬 The ETH2 development team is exceptionally talented and are making every effort to ensure security of the protocol. They even formally verified the bytecode of the ETH1 deposit contract. However, like any new software, there may be bugs in the different implementations of ETH2 that may result in part of the 32 ETH deposit being slashed (lost). Even if the network is secure, the lack of support of delegated staking means that if you are not running your own validator node, or you have less than 32 ETH, you must transfer ownership of your tokens to a 3rd party, and you may never get those tokens back. Third party stalking services are using smart contracts to prevent staked tokens from being stolen by hackers, but the smart contracts might have their own security vulnerabilities.

⑦ High rewards?

> 💬 With the bare minimum of token holders staking (0.47% of the network), ETH2 offers a very tantalizing APY of 21.6%. However, this drops rapidly, to 4.9% at 9% staking, and a low of 1.53%. Also, because there is no delegation mechanism in the protocol, 3rd party staking providers have to do a lot of work and as such charge high fees, much higher than for layer 1 blockchains that have native support for delegated staking.
>
> *Staking will need to compete with DeFi and other sources of yield*. Certainly there are many other ways to use one's ETH tokens instead of converting them to ETH2. ETH2 staking will have to compete with these other use cases, such as interest paid by DeFi projects. Some people think this may yield a conflict of interest, where if DeFi yields are too good, not enough people will stake their tokens to secure the network. Time will tell.
>
> Rewards do not [easily] compound. You have to save up 32 ETH of rewards then launch another validator. This is non-trivial and it takes time to accumulate this much reward. Exchanges with big reserves will be able to achieve closest to continuous compounding here. (This isn't even possible until transfers are enabled, at phase 1 or later)

⍰ Is it liquid?

💬 Funds staked are illiquid for a significant time. The exact time will depend on the future development schedule of ETH2. Different sources estimate this time from 1 to 3 years. Realistically it is likely at least 2 years.

Exchanges are trying to offer liquidity, but are essentially trading IOUs which cannot be taken off the exchange.

⍰ Will it allow Ethereum to massively scale?

💬 Sharding (scheduled for deployment at phase 1, at least a year away) with 64 shards in itself may only increase TPS by 64x (64 shards), and many existing applications will need to be updated. (Increasing shards requires increasing hardware requirements, so it is not likely to happen right away.) However, layer 2 scaling solutions such as rollups are being proposed to further increase the TPS. If smart contract support can be achieved with rollups, phase 2 may become unnecessary, and performance may reach 100,000 TPS, but this is uncertain and much development is still required. Some people are expecting rollups to be integrated before phase 1. We need to keep watching this.

Final Thoughts: Is Ethereum staying in the lead?

There may be no single company that has done more to promote and foster real world use of Ethereum than ConsenSys, the venture studio founded by Joe Lubin, one of the co-founders of Ethereum. ConsenSys' mission statement refers to Ethereum as a "world computer" that will "enable a new class of frictionless, global commerce with inclusion for all." This was a mighty vision when it was penned, but it turned out Ethereum 1.0 was too slow and expensive, making it unfit for many otherwise good use cases. ETH2 is finally on a path to making that vision a reality. Furthermore, ETH2 has been designed with an emphasis on decentralization, truly giving it a chance of becoming the "world computer."

Ethereum thus far has undeniably been a tremendous success. The Ethereum community has attracted some of the brightest minds, including app developers as well as developers of the core protocol. The upgrade of the core protocol is an extremely ambitious task which has been planned and executed very carefully to date.

However, many parts of the roadmap from here are a little fuzzy. Will rollups arrive on time? Will their functionality be as expected? (A lot of layer 2 scaling technologies have not lived up to their hype.) Will ETH1 apps and accounts be smoothly migrated to ETH2?

We believe that the upgrade will ultimately be successful and bring many improvements to the protocol. Despite all the problems Ethereum is currently facing, few projects have jumped ship to other blockchains. The community behind Ethereum is arguably the largest in the industry. The core protocol team will not stop until details like rollups and migration are finished; the only question is, how long will it take? Other, newer blockchains are slowly chipping away at some of Ethereum's use cases, but the blockchain market as a whole is growing significantly such that this is not a zero sum game. In further testament to the power and success of Ethereum, many of these new blockchains are developing interoperability solutions to Ethereum. It is clear that Ethereum is not going to fade into insignificance any time soon.

Should YOU Participate in Staking ETH2?

Let's return to the investment case for staking. Overall, since ETH2 cannot be converted back to ETH1, the opportunity cost of ETH2 staking is quite high. Staked ETH2 is locked for a long time, with potentially not that greater rewards (relative to other current DeFi and PoS blockchain opportunities). Meanwhile ETH1 tokens can be used in DeFi and dApps. Furthermore, delegating tokens to be staked by someone else is not supported by the protocol, and requires a 3rd party delegation mechanism with potentially high fees and security risks. Exchanges will offer markets to trade locked staked ETH2 (which cannot be taken off the exchange), but these markets may not be available in the US, may not have good liquidity or pricing, and require leaving coins on the exchange. It will be interesting to watch exchanges launching staking, and groups issuing staking security tokens, and how liquid and at what prices they will be traded at.

Most investors will probably rely on an exchange to do staking. If you do not mind leaving your coins on an exchange, and not being able to withdraw for a couple of years (potentially trading IOUs or taking out loans against your staked coins in the meantime, for an additional fee), then staking your ETH is maybe a good idea. Or if you are truly a long term HODLer and Ethereum believer, you probably want to stake some or all of your portfolio. Perhaps you don't trust other DeFi interest generating protocols? Staking coins for yield is likely safer than lending your coins to a DeFi protocol.

However, if you are simply looking for investment yield from staking, there may be better options. We suggest checking some of the other PoS blockchains referenced earlier in this report. This may be the subject of future reports from Wave Financial.
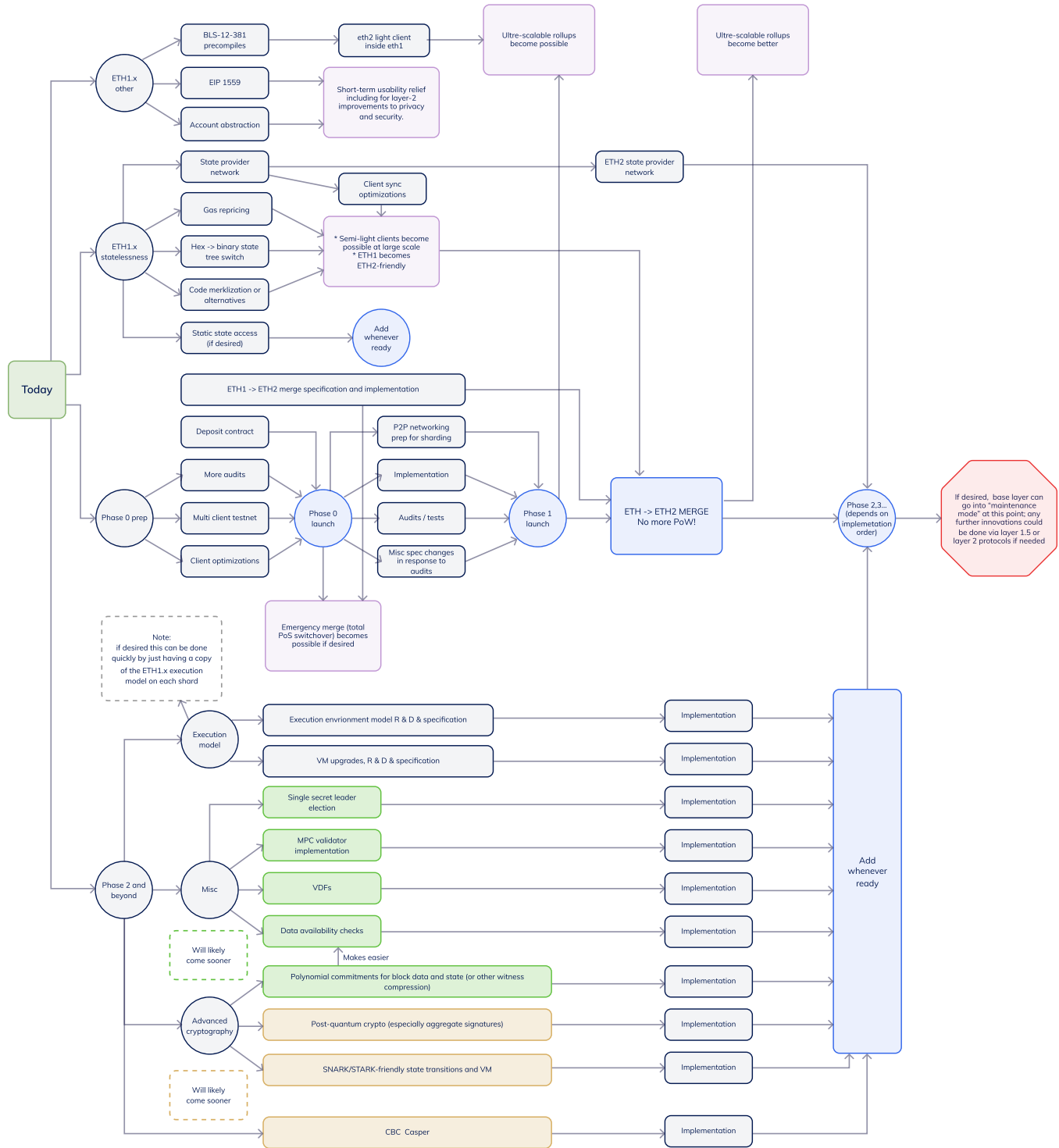
Additional Info

ETH2 staking overview (Ethereum Foundation) - An overview of Ethereum staking: the risks, rewards, and requirements for doing it.

ETH2 staking launchpad (Ethereum Foundation) - This was created for those who intend to start staking, guiding them through the process to convert their ETH1 and make keys, but just *clicking through all the warnings at the beginning is very educational.*

The State of ETH2, June 2020 (Danny Ryan, Ethereum Foundation) - A broader perspective on the current and future phases of ETH2 from Danny Ryan, one of the core developers.

Appendix

ETH1.x other
- BLS-12-381 precompiles → eth2 light client inside eth1 → Ultre-scalable rollups become possible
- EIP 1559 → Short-term usability relief including for layer-2 improvements to privacy and security.
- Account abstraction

ETH1.x statelessness
- State provider network → Client sync optimizations → ETH2 state provider network → Ultre-scalable rollups become better
- Gas repricing
- Hex -> binary state tree switch → * Semi-light clients become possible at large scale * ETH1 becomes ETH2-friendly
- Code merklization or alternatives
- Static state access (if desired) → Add whenever ready

Today

ETH1 -> ETH2 merge specification and implementation

Phase 0 prep
- Deposit contract → P2P networking prep for sharding
- More audits → Implementation
- Multi client testnet → Phase 0 launch → Audits / tests → Phase 1 launch
- Client optimizations → Misc spec changes in response to audits

ETH -> ETH2 MERGE No more PoW!

Phase 2,3... (depends on implemetation order)

If desired, base layer can go into "maintenance mode" at this point; any further innovations could be done via layer 1.5 or layer 2 protocols if needed

Emergency merge (total PoS switchover) becomes possible if desired

Note:
if desired this can be done quickly by just having a copy of the ETH1.x execution model on each shard

Execution model
- Execution envrionment model R & D & specification → Implementation
- VM upgrades, R & D & specification → Implementation

Phase 2 and beyond

Misc
- Single secret leader election → Implementation
- MPC validator implementation → Implementation
- VDFs → Implementation
- Data availability checks → Implementation

Will likely come sooner

Makes easier

Advanced cryptography
- Polynomial commitments for block data and state (or other witness compression) → Implementation
- Post-quantum crypto (especially aggregate signatures) → Implementation
- SNARK/STARK-friendly state transitions and VM → Implementation
- CBC Casper → Implementation

Will likely come sooner

Add whenever ready

Source: https://twitter.com/VitalikButerin/status/1240365047421054976?s=20

Research Note Authors

Jim Maricondo
Director at Wave Financial

jim@wavegp.com

🐦 @upandbeyond

Originally a software engineer, Jim enjoys evangelizing blockchain technology and its efficiency and fairness. Formerly in charge of opening the Tokyo ConsenSys office, he also helps projects enter Japan.

Constantin Kogan
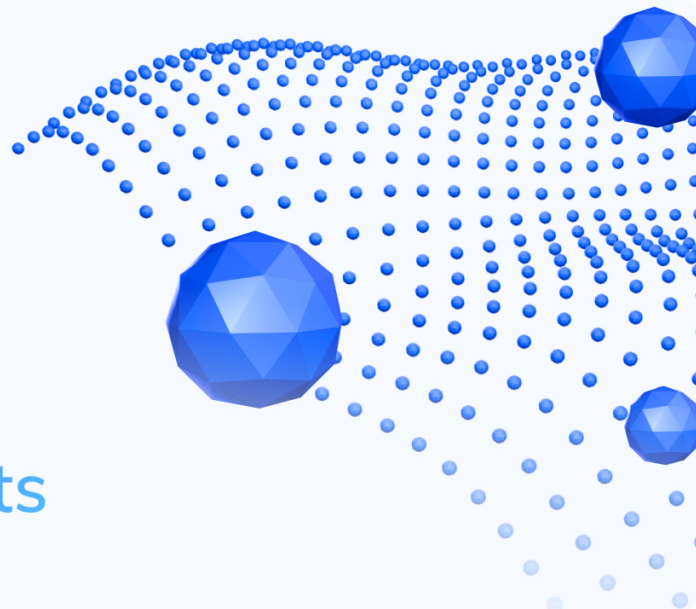**Managing Director at Wave Financial**

constantin@wavegp.com

🐦 @constkogan

He has been a cryptocurrency investor since 2012. He has over 10 years of experience in corporate leadership, technology and finance. He contributes to the digital asset space as well as the sharing and value economies.

Wave Financial LLC (Wave) is a Los Angeles and London based investment management company that provides institutional digital asset fund products. Led by a team of highly experienced financial services professionals, Wave provides investable funds via their diverse investment strategies applied to digital assets and tokenized real assets. Wave also offers managed accounts for HNWIs and family offices seeking tailored digital asset exposure, bespoke treasury management services, and early-stage venture capital and strategic consultation to the digital asset ecosystem. Wave is regulated as a California Registered Investment Advisor (CRD#: 305726).

Contact Us

Twitter

LinkedIn

www.wavegp.com

info@wavegp.com

Facebook

Medium

YouTube