HashStrat

Self-sovereign digital asset investments

Automated management of digital asset portfolios

On-chain strategies for long-term investors

Whitepaper v 1.0, draft, November 2022

https://hashstrat.com

Carlo Pascoli

carlo@hashstrat.com

TL;DR

HashStrat is a DeFi protocol to automate the construction and management of portfolios of digital assets.

In HashStrat, investors' portfolios hold a mix of stablecoins (USDC) and risk assets of choice (e.g. BTC, ETH) and use automated, on-chain strategies designed to capture volatility and manage risk.

Investors benefit from reduced volatility & drawdowns, when compared to just holding the assets, which help them be more successful, long-term investors.

Security and transparency have been a primary concern in the protocol design.
The protocol is fully self-custodial and trustless, all code is open source, holdings and trades are verifiable on-chain.

Embracing the ethos of DeFi, the protocol includes a DAO, the decentralized organization that allows users to propose changes and vote on protocol improvements.

The protocol generates its revenues by charging a small fee on profits withdrawn by users. These fees are collected into the DAO treasury and periodically re-distributed to DAO token holders as "dividends".

Content

Introduction

In this paper we introduce HashStrat, a DeFi protocol for self-sovereign investing.

HashStrat automates the construction and management of portfolios of digital assets without the need to entrust intermediaries, which is the case for traditional asset managers or crypto hedge funds.

Because of its trustless nature, the HashStrat protocol is also suitable to manage assets held in DAO treasuries and can be integrated into other DeFi protocols.

In the following, we show how the blockchain provides the best technology to manage digital assets and present the opportunity represented by digital asset management services that are native to the blockchain.

Decentralized Finance

The 2008 Global Financial Crisis, alongside the collapse of trust in financial insitutions, brought an unexpected positive outcome: the birth of the first digital asset, bitcoin.

Bitcoin represents a breakthrough in money technology being the first bearer instrument that can be acquired, owned and transferred digitally, without having to trust counterparties or intermediaries.

A few years later, the same technology that allowed bitcoin was generalized in the Ethereum blockchain.

Ethereum, and its Turing complete virtual machine, enabled the programing of money to go beyond what was possible in bitcoin and paved the way to a new industry called Decentralized Finance or, in short, DeFi.

On Ethereum we saw the launch of the biggest achievements in DeFi.
Protocols like Maker, Compound, Uniswap, AAVE, Curve, Balancer and others provided basic financial primitives that could be combined in novel ways, like financial LEGO bricks, into an ever growing suite of new financial services open and accessible to all.

Asset Management

In traditional finance, asset or investment management refers to the professional handling of clients' asset portfolios, with the aim to grow their value by acquiring and trading investments while, at the same time, mitigating downside risks.

In their 2020 report PwC valued Global Asset Management at $110 trillion in 2019, a market set to rise to $145.4 trillion by 2025.

The development of blockchain technology brought us a new class of assets, generally referred as crypto assets or digital assets. They include native blockchain tokens (e.g. BTC and ETH), utility tokens, non fungible tokens (NFT) and stable coins.

The combined value of these digital assets currently stands below $1 trillion, after reaching about $3 trillion at the end of 2021.

As of November 2022, about $40.46 billion is locked in DeFi (down from $180 billion in November 2021, but still up 3x from 1 year earlier), and DAO treasuries are holding about $9.0 billion worth of digital assets.

Despite the value of digital assets being a drop in the ocean when compared to traditional financial assets, their established status and growth trajectory justify the development of professional digital asset management solutions.

In 2021, for example, crypto hedge funds were estimated to have $4.1 billion in Assets Under Management (AUM).

Crypto hedge funds can provide investors with exposure to digital assets but they come with all the shortcomings of traditional finance, from asset rehypothecation to high management fees and limited accessibility.

But the biggest problem of all is that they rely on a fiduciary relationship between the investor and the asset managers. A fiduciary relationship based purely on trust.

A trust issue

The 2022 crypto bear market proved again how centralized entities don't deserve clients' trust. Crypto hedge funds and exchanges like Three Arrows Capital, Voyager Digital, Celsius, BlockFi, FTX (the list goes on) defaulted causing billions of dollars in losses to their clients.

Different protagonists were entrusted to operate their businesses as black boxes, and they failed to manage their clients' assets with integrity.

If that was due to cowboy-style risk management or pure fraud it's for the judiciary to decide, but these are fundamentally all failures of traditional finance models applied to crypto, something that, ironically, bitcoin and blockchain technology are meant to fix.

Digital Asset Management

As more of the world's digital economy transitions to the blockchain, the need will arise for asset management solutions that are native to the blockchain. Solutions that fully embrace the ethos of self-sovereignty, neutrality, openness, trustless execution and cryptographically provable truth that are at the core of Decentralized Finance. Solutions that prevent fraud and mismanagement that we witnessed in 2008 and 2022.

We are already starting to see the development of such solutions in the DeFi space with protocols like Enzyme, Set, Index Coop, Sommelier representing the first experiments in this new, exciting industry.

But with a combined AuM of about $150 million, these protocols are barely scratching the surface of the opportunity available for this new class of services.

In the following section, we introduce HashStrat, a new DeFi protocol for self-sovereign management of digital assets.

HashStrat Protocol

HashStrat is a DeFi protocol to automate the construction and management of portfolios of digital assets.

Investors' portfolios hold a mix of stablecoins (USDC) and risk assets (BTC, ETH) that are managed by transparent, immutable smart contracts, living on the blockchain. These smart contracts encode investment strategies with built-in risk management.

Investors select the assets they want to hold and their favorite management strategies. They deposit USDC tokens and their strategies will determine their initial portfolio allocation. The strategies decide when to spend USDC and buy more risk assets and when to sell them into USDC to offload some risk.

HashStrat strategies aim to produce returns that are competitive with the benchmark buy-and-hold strategy and ensure reduced portfolio volatility & drawdowns.

In the following sections, we describe the various components that comprise the protocol and how they operate.

Pools and Strategies

At the core of the HashStrat protocol is the concept of a Pool.

A Pool is like a digital vault that holds digital assets. A pool would typically hold one stable asset (USDC tokens) and a risk asset (wrapped BTC/ETH tokens).

A Pool is also configured with a Strategy, a set of rules, encoded into smart contracts, that defines how the assets in the Pool should be traded.
Strategies have the goal to increase the value held in the Pool over time while adequately managing risk.

Examples of strategies are:

- **Rebalancing**
  This strategy aims to capture volatility in the risk asset by rebalancing the Pool

whenever the value of either asset deviates significantly from the Pool's target allocation.

- **Mean Reversion**
  A strategy that would dollar-cost average in and out of the risk asset when its price deviates significantly from its long term trend.
- **Trend Following**
  A momentum strategy that would allocate to the risk asset when its price trend is up and de-risk into the stable asset when its price trend is down.

LP Tokens

When users deposit into a Pool they receive a certain amount of LP tokens back. These tokens represent their share of liquidity provided (LP) to the Pool, and are a receipt that has to to be returned back to the Pool in order to withdraw their funds. There are no lockup times, minimum investment requirements or other arbitrary constraints. Users are free to deposit as little as they like and withdraw at any time.

Staking

LP tokens can be “staked” into the HST Token Farm (more on that later).
Staking LP tokens means locking them up into a smart contract so they can earn (aka farm) DAO tokens HST as a reward.
This way, any user can become a member of the DAO and a stakeholder in the protocol.
At any time users can “unstake” and withdraw their liquidity from the Pools and keep the HST tokens accumulated so far.

Fees

The protocol generates its revenues by having the Pools charge a 1% fee on all profits withdrawn from the Pools. If no profits are made, no fees are due.

Fees stay in the Pools and are used to periodically reward users of the protocol and finance future developments in accordance with the DAO governance decisions.

Indexes

HashStrat Indexes are a concept built on top of regular Pools.
They represent baskets of Pools and allow you to easily get exposure to multiple assets and strategies.

When a user deposits funds into an Index, those funds are split among the Pools that comprise the Index, according to some predefined weights. The Index will receive LP tokens from its Pools and will return its own LP tokens back to the users to account for the share of the Index liquidity they provided.

Index LP tokens work exactly like Pool LP tokens and users will have to return them back to the Index to redeem their share of liquidity and withdraw their funds.

HashStrat DAO

The DAO is the Decentralized Autonomous Organization governing the protocol.

All users have the ability to become members of the DAO and influence its evolution and receive a share of its revenues.

Members of the DAO can, for example, propose and vote on new strategies, how to spend the protocol revenues, what fees each Pool should charge, etc.

The DAO Token HST

Decisions and operations of the DAO are facilitated by the HashStrat DAO token (HST). This token is only issued to users of the protocol to reward them for being early adopters and supporters.

Users who deposit funds in any of the HashStrat Pools & Indexes can “stake” their LP tokens and then claim their HST tokens from the DAO Token Farm.

By earning HST tokens users are able to:

1. Participate in the governance process by making and voting on proposals that affect the future of the protocol.
2. Receive a share of the revenues generated by the protocol that get periodically distributed as “dividends” to HST token holders.

HST Token Farm

The HST token Farm is the component of the DAO responsible for distributing DAO tokens to users of the protocol who stake their LP tokens.

The Farm plays the key role of ensuring a fair distribution of the DAO tokens to those who are providing capital to the HashStrat strategies, and by doing so are helping with the bootstrap process of the protocol.

HST is a token with a supply limited to 1,000,000 units and no premine.
The Farm will distribute the entire token supply over the course of 10 years, according to this fixed schedule:

Year	Tokens Distributed	Circulating Supply	Total Supply
1	500,000	500,000	**1,000,000**
2	250,000	750,000	
3	125,000	875,000	
4	62,500	937,500	
5	31,250	968,750	
6	15,625	984,375	
7	7,813	984,375	
8	3,906	992,188	
9	1,953	998,047	
10	1,953	**1,000,000**	

DAO Governance

The protocol defines what changes and upgrades can be done to it.

These changes have to go through governance, which means DAO members have to submit and vote on proposals that, if successful, can be executed on-chain.

DAO token holders can also use their tokens to vote on polls on topics of interest when a decision can't be enforced on-chain.

In both cases, the weight of a vote is determined by the number of DAO tokens held in the user's wallet at the time when the proposal was submitted.

Here are some examples of changes that governance can decide on:

- Update the percentage of protocol revenues paid as dividends
- Update the Pools' fee percentage (from 0% to max 5%)
- Update the interval between dividend distributions
- Authorize a payment out of the Treasury
- Add/remove new Pools & Indexes
- Update the strategy used by a Pool

When a proposal for a protocol change is approved, before it can be executed on chain a predefined time period has to elapse. This interval, called timelock delay, exists to ensure that everybody has time to react to an undesired change.

Tokenomics

As discussed earlier, HST tokens allow their holders to participate in protocol governance and revenue sharing. They represent something akin to equities in the protocol and provide a claim on future protocol dividends.

Therefore, we can model the fundamental value of the HST token by discounting the value of future dividends expected per token.

From HST holders perspective, the value of dividends they can expect to receive depends on 2 factors:

1. Total protocol revenues (the total value of fees collected)
2. The percentage of HST tokens held (the user's share in the protocol)

Protocol revenues

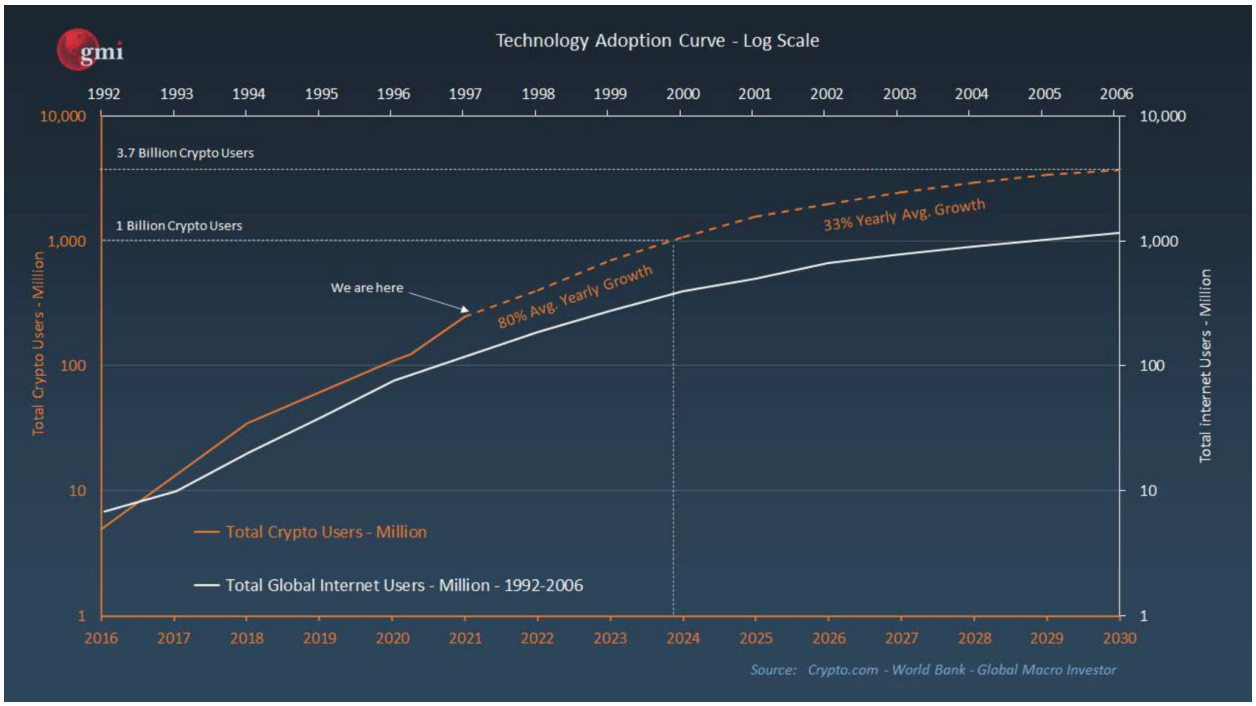
To estimate (1) we have to model the growth of the value of the assets managed by the protocol.

This is a function of net user deposits and the growth of the crypto markets, where the latter produces the appreciation of the assets that will determine the protocol fees (aka revenues) when those gains will eventually be withdrawn.

To estimate the future growth of the crypto markets, we observe how bitcoin & crypto adoption is moving on an exponential curve akin to that of the internet.
In 2022 bitcoin & crypto adoption reached 300m+ people, 4% of the world population, and stands where internet adoption was in 1998.

This trend suggests hitting 1 billion users by 2025 and approaching 4 billion by 2030, a 33% annualized average growth rate.

Because asset prices are strongly correlated to adoption, if the current trend continues future protocol revenues are essentially determined by the amount of liquidity attracted.



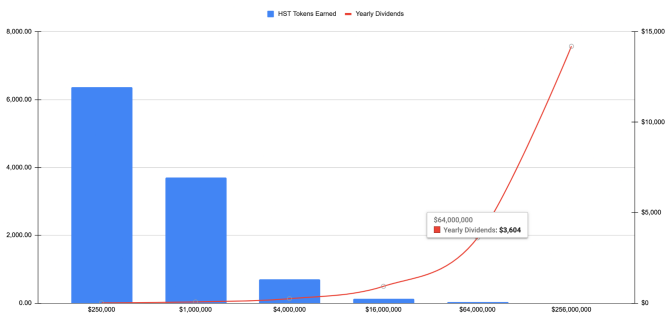
HST distribution

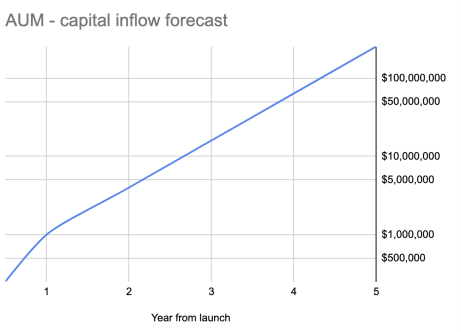
To estimate (2) we need to model the amount of HST token received by users for the liquidity they provided. This is a function of the HST distribution rate and the total liquidity “staked” in the protocol.

The HST distribution rate is known, but it’s worth noting how its halving schedule represents a big incentive to provide liquidity early, when the amount of HST tokens distributed is higher and the liquidity competing to receive those tokens is lower.

This dynamic is designed to bootstrap the protocol and to compensate early adopters for the higher risks they take in investing into a new protocol.

In the chart below, we can see how, for a $10k model investment, the amount of HST tokens earned (blue bars) decreases exponentially with time, whereas the amount of expected yearly dividends (red line) grows exponentially.





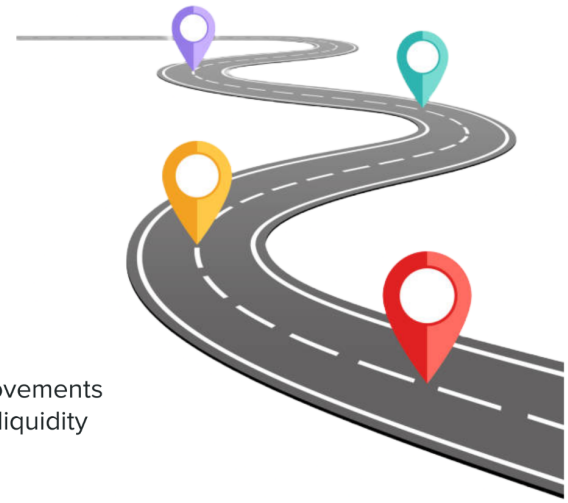
This model assumes a sustained capital inflow into the protocol as per second chart, and a continuation in the adoption trend of the bitcoin and crypto ecosystems for the rest of the decade.

Roadmap

After the soft-launch of the MVP and DAO in 2022, the goal for 2023 is to prove the product-market fit by acquiring an initial user base and reach the first million dollars of assets managed by the protocol.

To achieve this milestone, we will pursue a pre-seed round of investments.

The funds raised will allow us to invest in security audits, UI/UX improvements, new strategies and some targeted marketing.



2022 (Q2/Q3)

- MVP Development
- MVP soft-launch
- Beta testing

2022 (Q4)

- MVP validation
- DAO development
- Grants applications

2023

- Pre-seed round
- Security Audits
- Strategies R&D
- UX & design improvements
- Initial user base & liquidity

2024

- Seed round
- UX/Design overhaul
- Marketing
- More liquidity & users
- Fiat on-ramp solutions

Having proved the product-market fit and achieved initial revenues, in 2024 we should be in a position to pursue a seed investment round and scale up the protocol.

These funds will be allocated to attract more users and liquidity through sophisticated strategies, broader marketing outreach and an improved user experience that could also include a fiat onramp.

Conclusions

In this paper we presented HashStrat, a DeFi protocol for self-sovereign digital asset management.

We started by acknowledging how bitcoin represents the breakthrough that allowed the advent of a new class of assets and a new market that sits on an exponential growth trajectory, akin to that of the internet 25 years ago.

We remembered the failures of asset management services offered by centralized, trusted entities, and presented the opportunity to address these failures through blockchain technology because of the cryptographically verifiable guarantees that only blockchain technology provides.

Finally, we introduced HashStat, a DeFi protocol designed to automate the management of digital asset portfolios that is trustless, open and transparent.

We described its tokenomics and functionality, including the ability to manage future improvements through a DAO, the decentralized organization of its users.

Resources

https://www.bitcoin.com/bitcoin.pdf

https://www.pwc.com/gx/en/industries/financial-services/assets/wealth-management-2-0-data-tool/pwc_awm_revolution_2020.pdf

https://www.pwc.com/gx/en/financial-services/pdf/4th-annual-global-crypto-hedge-fund-report-june-2022.pdf

https://assets.ctfassets.net/hfgyig42jimx/5i8TeN1QYJDjn82pSuZB5S/85c7c9393f3ee67e456ec780f9bf11e3/Cryptodotcom_Crypto_Market_Sizing_Jan2022.pdf

https://www.swfinstitute.org/fund-manager-rankings/crypto-fund-manager

https://phemex.com/blogs/crypto-bitcoin-s-curve-adoption-curve

https://blockchain.news/analysis/crypto-users-stand-at-300m-representing-nearly-3.7-percent-the-global-population

https://www.washingtonpost.com/business/2022/06/27/three-arrows-capital-default-crypto-voyager-digital/

https://twitter.com/woonomic/status/1580258490953580544

https://deepdao.io/organizations

https://defillama.com/