HYDRA CHAIN

Permissionless, Inflationary POS blockchain with fixed fiat transaction fees and a unique burning mechanism on generated transactional economy

1. Introduction

In the recent past, many misrepresented blockchain as something magical that automatically solves any problem. This whitepaper tells an interesting story of how a team that acquired extensive experience in building and growing a business in a not yet matured technological environment has used this unique knowledge in effectively iterating the business-oriented **Hydra blockchain**. A blockchain developer that had a unique practical usage perspective as a DaPP developer first. A perspective that has put the focus on critical economic limitations of existing chains and resulted in a unique blockchain economy.

1.1 The backstory

Back in 2018, the team behind LockTrip has published a document labeled "LockTrip Blockchain Manifest" which has become the fundamental design document of the Hydra Chain. The document was based on actual hurdles that were encountered as part of the development of the LockTrip DaPP.

As a strategy to come up with the best solution, the team has undertaken an evolutionary approach where it built Hydra on top of available open source technology, that has gone through the test of time — a successful strategy used by some of the current biggest blockchains (e.g Bitcoin Cash, Litecoin, Qtum and many more).

The philosophy behind Hydra is to implement critical economic features while utilizing proven technology for data transmission. Hydra is a permissionless, open-source, proof-of-stake blockchain built on top of open-source projects QTUM, Bitcoin, Ethereum and BlackCoin's PoV v3, designed by Pavel Vasin. In addition to a number of unique economic features, it has a relatively high inflation in order to stimulate stakers and market participants to contribute to its true decentralized architecture.

2. Specific problems Hydra Solves

2.1 Protection against inflation driven price degradation - enabling sustainable transactional economy deflation as a background process

At its core, a Fiat Price Oracle always updates the current FIAT value equivalent of HYDRA coin. Gas price is defined in fiat and then adjusted according to the USD exchange rate.

In addition, there is a unique feature that enables the whole chain to burn up to 50% of all transaction gas paid by users on the protocol level.

The combination of the **a) fiat fixed fees** + **b) ability to burn transactional gas** + **c) high inflation rate** creates a unique economic powerhouse, that safeguards security by providing high and at the same time predictable staking income to node infrastructure while offering significant protection against inflation price degradation due to the capacity to use the transactional economy as a way to stimulate deflation.

No other chain is solving this problem. Most blockchains usually apply a pre-determined “halving” in time-dependent events that are completely irrelevant from what the actual economy and usage of a particular chain are, and thus expose the whole network at risk. Uncontrolled inflation on the other hand poses the risk of degradation of price in time. Predicting when to change state and how exactly to do it is impossible, which is why HYDRA enables inflation to combat deflation as a background process and leave the market to determine it.

Two unique economic streams in a constant “battle” depending on the actual usage of the chain. At the launch, inflation will be dominating the chain and provide an attractive stimulus to staking nodes.

This on its end will grow the infrastructure as a combined network value. As the infrastructure value grows, adoption should follow that on its end will stimulate transactions.

As more transactions are generated, the burn rate will begin to cut supply.

Hydra stimulates infrastructure and community growth while offering protection against price degradation due to its ability to convert transaction gas into a permanent supply cut.

This also means that HYDRA solves one of the most difficult challenges with blockchains - **How** and **When** to switch a blockchain from an inflation state to a deflation. As an example, a halving type of sudden switch to deflation and complete stop on block rewards imply that there should be a transactional economy, powerful enough to sustain the same level of economic demand by the nodes infrastructure that had been built as network participants based on these same block rewards.

This is possible due to the ability of up to 50% on gas fees to be destroyed permanently on protocol level without affecting the staking economy. Think of it as a separate process.

On top of that, the fiat oracle empowers transaction Gas Burn specifically if HYDRA price starts to degrade. This comes as natural protection against severe price degradation.

Scenario 1)
For instance, if a standard HYDRA transfer costs $0.2 and HYDRA price is $0.5, that would mean that a transaction would cost 0.4 HYDRA. With a 50% burn setting, 0.2 HYDRA will be destroyed.

Scenario 2)
Imagine that HYDRA price drops to $0.1. The same $0.2 will now cost 2 HYDRA due to the lower HYDRA/USD rate. With a 50% burn setting, 1 HYDRA will be destroyed permanently.

The more HYDRA USD price falls, the higher the burning efficiency is.

[You can use the Staking Calculator to try out more advanced combinations]

With HYDRA total supply is no more a predetermined setting.

As it has been demonstrated with all successful blockchains, during the seed/inception phase, inflation dominates over transactions. This is normal as it takes time to grow the decentralized infrastructure and build a strong community. The weighted average is 4-5 years for accumulating a strong transactional economy which would follow afterwards.

If after 5 years HYDRA is to reach 5 transactions per second, which is around 15% of its bandwidth capacity (600 per block). Depending on the price of HYDRA, the network could **switch from a relatively neutral state to extreme deflation.**

To elaborate what this would look like:

- A $0.5 price would generate -33 HYDRA per block -> From that moment onward the monetary base will start to decline and potentially start to revert the supply that had been created as part of the initial seed/growth phase of the chain. A $0.5 price would translate to 19M market cap with a hypothetically projected 16.3M HYDRA burnt over a course of 12 months.

- A $1 price would generate -1.15 HYDRA per block -> Again a slight deflation, while still yielding 51% income to stakers

Let's hypothetically assume that price degrades severely for some reasons and it falls down to $0.1.

That would immediately lead to a -289 HYDRA burn per single block with the same rate of 5 transactions per second. That burn rate will take out 392,603 HYDRA from circulation per day. Within one month, if the variables remain unchanged, 11.7M HYDRA will be destroyed permanently, reverting the inflation that took years to achieve.

In that same scenario, even if the network runs at 1 transaction per second, that would make a -33 HYDRA per block. Its strong design make it utilize even the most basic layer of transactional economy coming from transactions related to:

- basic wallet-to-wallet transfers
- exchange activity, daytrading, trading
- tokens, stabletokens
- community activity

The above types of transactions are usually inseparable from a coin economy and grow together with the popularity and market cap, reaching potentially tens of thousands per day.

Additionally, there's also the opportunity of products and specialized commercial dApp developers to build on top and supplement this economy.

HYDRA solves the fundamental problem of handling total supply on a completely different level.

Questions such as "When will the next halving take place?", "What will happen with price after the halving?", "Will the network collapse if block rewards disappear?" are no longer relevant, because total supply is the direct representation of the actual usage of the chain. This also gives a fair and transparent tool for all actors to properly interpret the total supply and its relation to transactions and price. It also eliminates speculation arising from communicating "total supply" - perhaps one of the most abused metrics in blockchain.

In HYDRA's design, total supply as a monetary base is entirely determined by the market with a leveraged impact in oversold states while still giving strong protection to the nodes. This makes the system extremely resilient to uncontrolled inflation and severe price drops as it is able to extremely effectively capture transactions and use them to counter balance the supply through the constant burn process.

- If the transactional economy is weak, inflation will dominate during the growth phase and subsidize the nodes until the moment transactions activity increases
- If the transactional economy is strong, deflation will dominate, and the supply will at some point decline potentially reverting the staking rewards that came through inflation in the seed growth phase of the chain. In the meantime nodes will always have a predictable income that will guarantee maximum security of users' funds.

2.2 The Balance between TPS and Decentralization

The premise of blockchain technology has always been its ability to be resistant against manipulation and censorship. The two most popular blockchains Bitcoin and Ethereum have strived exactly because of this revolutionary idea of not having to trust a single entity or rely on the decisions of a few selected individuals.

Yet, this powerful idea comes at a high cost. The more nodes participate in the validation of blocks, the more difficult it becomes to synchronize vast amounts of data across the entire network. This fundamental bottleneck has become the main trade-off debate in the industry and has resulted in many projects sacrificing decentralization for insanely high TPS (transactions per second) capacities. The problem is, that the moment a blockchain relies on a few selected nodes for its operation, it has given up the idea of censorship resistance. There are many such examples out there, which will not be further discussed in the context of this whitepaper.

The Hydra chain on the other hand holds true to the fundamental qualities a blockchain should offer and bases advancements on proven and 100% decentralized blockchain infrastructures. A special focus lies on improving the overall capacity to approximately 75 - 85 TPS without sacrificing decentralization, which puts the daily transaction limit at 6.5 - 7.3 Million transactions. For comparison, this represents a 6-fold improvement over the Ethereum network at the time of writing.

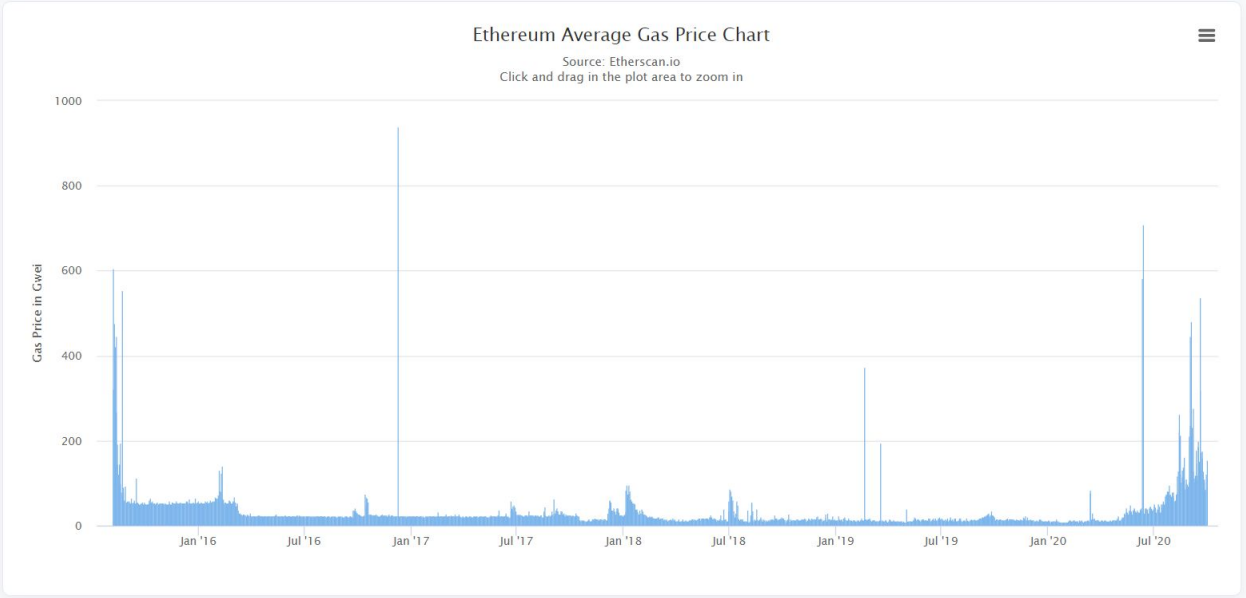
The Hydra chain in its core is based on the open-source production level Qtum blockchain, which on its own is a fork of Bitcoin Core with an Account Abstraction Layer that enables support for the Ethereum Virtual Machine (EVM). This hybrid blockchain solution utilizes the well-established UTXO transaction model and employs a true Proof-of-Stake consensus, which has been evolved from the BlackCoin project. We are undertaking the evolutionary strategy of combining the best of Bitcoin and Ethereum and building on top of it a proprietary blockchain that is capable of preserving decentralization, supporting Ethereum applications and at the same time reaching notable TPS performance.

2.3 Unpredictable Transaction Fees

Business developers need to know the exact costs associated with the building parts of their businesses. Since blockchain is essentially a transaction based technology, not knowing how much a transaction will cost, practically means not knowing if the businesses built on it will be viable or not.

Ethereum and Bitcoin's current consensus mechanism is Proof-of-Work based (POW) and as such, the costs associated with the validation of each transaction are defined by the miners that process the underlying layer through an auction mechanism. This essentially means that the blockchain businesses, investors and users have no idea on how much the miners will require at any moment in future to support the network and validate the transactions.

The chart below showing the Ethereum gas price history for the past 4 years illustrates how dramatic changes can happen in a very short period of time. Over the course of a few weeks, the gas price has grown from 10 gwei to over 150 gwei - a 15x increase.



The intra-day volatility is even more radical. Throughout August and September 2020, Ethereum participants have experienced gas prices ranging from 30 to 700 gwei within the same day. This was mainly fueled by a strong upward trend in decentralized liquidity pools, which consume a lot of gas due to the involvement of multiple smart contracts in a single transaction.

The sudden changes resulted in smart-contract based transactions to reach fees of $200 and above. Perhaps the biggest problem with this is that there is no theoretical limit as to how high the fees can grow. Business developers have no guarantee that they won't be seeing an absurdly high level tomorrow. This lack of predictability represents a big obstacle to mainstream adoption and can turn otherwise healthy business unsustainable over time.

The Hydra chain achieves transactional gas cost predictability through a governed and stable gas price protocol. The gas price will be governed by the nodes through a voting mechanism and will be bound in fiat equivalent. The fiat rate will be governed by an Oracle that will monitor exchanges where the underlying HYDRA cryptocurrency will be traded on. The end result will be a blockchain that has a fixed price per transaction in USD equivalent, irrespective of the HYDRA rate, thus giving network participants the stability they need.

2.4 Capturing the Transactional Economy

The transactional economy is the lifeblood of the blockchain. It is what fuels the ecosystem, ensures the safety of the network and keeps a healthy balance between users and validators. At the time of writing, the transactional economy of Ethereum has reached $3.5M per day (excluding block rewards) and $1M per day for Bitcoin.

What this means is that a vast amount of value is being transferred out of the network to blockchain-agnostic mining companies. They usually keep a multi-chain operation where they quickly repurpose their computational power to the blockchain with the most profitable rewards and then sooner or later liquidate their earnings to re-invest into more computational power.

Although these rewards are rightfully earned for keeping the blockchain secure, it also means that the ecosystem is missing out on a significant part of its economy - block by block. The lifeblood, as described earlier, is flowing out of the body. The ultimate flaw in this model is that those who keep the chain secure are not tied to the actual chain in any way. The validating processors don't care about which blockchain they keep safe on that particular moment and their owners have no economic interest in the well-being of a particular chain, due to their ability to quickly repurpose their resources.

The Hydra chain solves this shortcoming by utilizing a Version 3 Proof of Stake mechanism developed by Pavel Vasin. Through this step, the Hydra chain is capturing 100% of the transactional economy and re-distributing it to those who not only work for the security of the network, but also own part of its supply. This effectively makes the chain self-sufficient and eliminates any external dependencies.

2.5 Environmental and Economic Sustainability

The Proof of Work (PoW) mechanism, which was first introduced with Bitcoin, has paved the way to decentralization. The value of BTC grew together with the overall network size, but so did the incentive to set up an ever increasing machinery of increasingly powerful and energy-consuming processors. On one side this was a very positive outcome and even needed for the health of the chain. Because the more processors are working to keep the chain secure, the more expensive it becomes to launch a 51% attack. The massive increase in energy consumption was built into the very system as an integral component.

The downside of this is the massive waste that results out of the competition to burn as much energy as possible by utilizing an ever renewing set of processing equipment. Needless to say, it is not a sustainable model for the environment. The above mentioned Proof of Stake consensus model removes the unnecessary calculations from the equation and reduces the work-load to a minimal computing power, which is orders of magnitudes

lower and can easily be managed by most computing devices available at retail stores. As a result, the impact on the environment is negligible.

As pressing as the environmental component is, there is one component that is even more important to the success of any chain: its economical sustainability, which is directly linked to its security against external attacks. So far we have outlined a number of shortcomings of Bitcoin and other blockchains, but they all fade away compared to the significance of the systemic risk Bitcoin carries.

Regardless of whether a blockchain uses POW or POS to establish consensus, the security of it is directly correlated to the block rewards it offers as an incentive for security. For POW blockchains it establishes itself in the amount of computing power attackers need to compete. For POS blockchain it is the amount of coins being staked that present the safety barrier. In both cases the chain competes for these resources with alternative investment opportunities across the globe. The higher the market cap of the blockchain, the bigger the incentive for attackers. In contrast, the security correlates with the block rewards. This results in the following security factor for a given blockchain:

Security Factor = Resources Securing the Network / Market Capitalization

In the example of Bitcoin, the block rewards are being halved every 4 years. Since the rewards are distributed in BTC and the market capitalization is also directly correlated to BTC, the formula can be simplified to:

Security Factor = BTC Rewards Per Year / BTC Supply

As is public knowledge, the rewards keep halving every 4 years, while the supply of BTC is growing with every mined block. This means that the security factor is dropping by a tiny amount every block and additionally is being halved every 4 years. No one knows if and when this will translate to a 51% attack, but it is certainly possible that the experiment may have a very bad outcome one day.

The Hydra chain solves this by introducing inflation-based block rewards, which can be regularly voted on through the democratic governance protocol by coin holders. This not only incentivizes holders to stake their coins, but also allows for a high security factor to be maintained, making the chain sustainable.

2.6 Adaptation and Community Involvement

The world is constantly changing. Businesses, economies and technologies need to adapt to the new scenarios on a regular basis. This is even more true in the crypto environment, where innovations are being tested in rapid cycles and experiments are popping up everywhere. In contrast to this, most blockchains are highly static and inflexible. Even small changes can end up as huge challenges, both in terms of technical implementation and community support.

We have seen hard forks not working as intended and communities being disunited due to their different views on the proposed changes. Such events pose significant risks to the chain and can cause serious damage to the project.

To combat this risk, the Hydra chain inherits a decentralized governance protocol and is designed to adapt to many different scenarios in a harmless and constructive way. A number of blockchain settings are possible to be voted on by coin holders and can thus be changed “on the fly” as required. This gives the chain a very good flexibility and allows the community to steer it into the right direction in a peaceful process.

The settings that can be voted on are listed below:

- *Adding new admins (these can initiate a new voting)*
- *Removing admins*
- *Changing the Gas limit per KB (UTXO layer)*
- *Changing the Gas/Fiat rate (EVM Layer Gas)*
- *Changing the block size*
- *Modifying the transactional economy (reimbursement to token creators with range 0% - 50%)*
- *Modifying the protocol burn rate (range 0% - 50%)*
- *Modifying the protocol inflation rate (range 0% - 25%)*

Proposals can be pushed by elected admins within certain predefined limits. The voting process works by sending coins to the smart contract with the desired outcome. The smart contract with the higher coin amount at the end of the voting period will determine the outcome. All coins will be burnt thereafter, turning high-value disputes about certain proposals beneficial to the ecosystem.

In addition to the voting process, coin holders also have very easy access to the block validation mechanism and can earn passive income just by maintaining the network with the holdings. Contrary to the POW blockchain, the entry barrier on the Hydra chain is close to zero as no expensive equipment or minimum coin amount is required. This not only

increases the involvement of the community with the chain they are growing, but also allows for a much better decentralization as anyone can create an independent node and contribute to the network.

2.7 Establishing a Truly Shared Economy

Most people in the crypto industry experience the space as a gambling environment either in the role of traders, investors or simply by betting on random coins and tokens. The reasons for this are likely many, but one obvious reason is that most blockchains are not really sharing their economy at protocol level, which leaves price movements as the only option left. A good example was given in section 2.3, where the transactional economy is being funneled outside of the network. In contrast, the Hydra chain preserves it within the network and rewards network participants for their contributions. But this is not the only difference.

Chains that support smart contract functionality such as Ethereum do not incentivize developers for their contribution to the network. The only incentive for them is to build a profitable business around the chain, which is a strong limiting factor to the overall development of the ecosystem. There are many useful applications that do not necessarily allow for a profit to be applied.

The Hydra chain solves this important gap at protocol-level by enabling a reimbursement of transaction fees to token creators. The mechanism effectively rewards project owners based on the transactional economy they create, by getting a share of each transaction their token was involved with. Adjustments to the reimbursement rate can be made by voting on it with a range between 0% and 50%. Combined with the staking mechanism, this creates a truly shared environment, where network participants are rewarded on all levels for the value they add to the ecosystem.

3. Blockchain with an Economy like no other

3.1 Inflation Based Block Rewards

The inflation mechanism is a key component of the Hydra chain and shapes its economy fundamentally.

The inflation of HYDRA is fixed as a percentage to the total supply. This is to incentivize members to take active part in staking and to ensure the income does not degrade over time. Halvings and the lack of predictability, combined with the volatile nature of gas fees

are critical economic features that Hydra solves without compromising permissionless decentralization.

The inflation formula works as follow:

[inflation rate%] x [total coin supply] / blocks per year

"inflation rate%" being the changeable parameter that can be casted with a community vote and will be limited within a 0% - 25% range.

This technically means that, with 18,585,933 HYDRA coins as a total initial supply and the default **128 second** block time (246,375 blocks per year), the calculation would look as follows: /based on a 0 gas fees for the particular sample blocks and a 20% inflation rate/

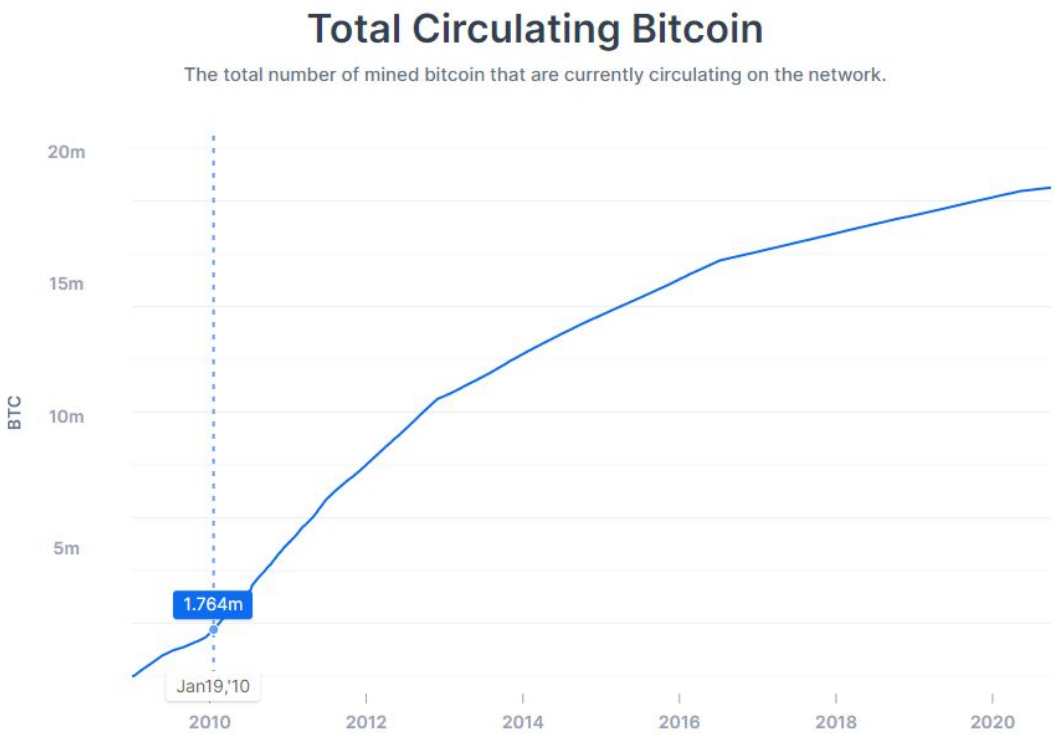
- **block 1** (0.2 x 18,585,933)/246,375 = 15.08751537290715 HYDRAs per block as a reward and a new total supply of 18,585,948.08751537
- **block 2** (0.2 x 18,585,948.08751537)/246,375 = 15.08752762050969 HYDRA block reward
  (and the cumulative increase continuing to grow)

3.2 Why high inflation is critical

Blockchains are essentially aiming for network neutrality, stability, and predictability. Without those three factors, it would be impossible to build sustainable and economically significant applications on top of them.

Bitcoin, in its initial phase, was actually a project in a hyper-inflation state. Giving enormous predictability to all actors through substantial mining rewards.

Over a period of just 12 months, the circulating Bitcoins increased from 50 to 1.7M. Needless to say that this translates to a massive inflation rate.

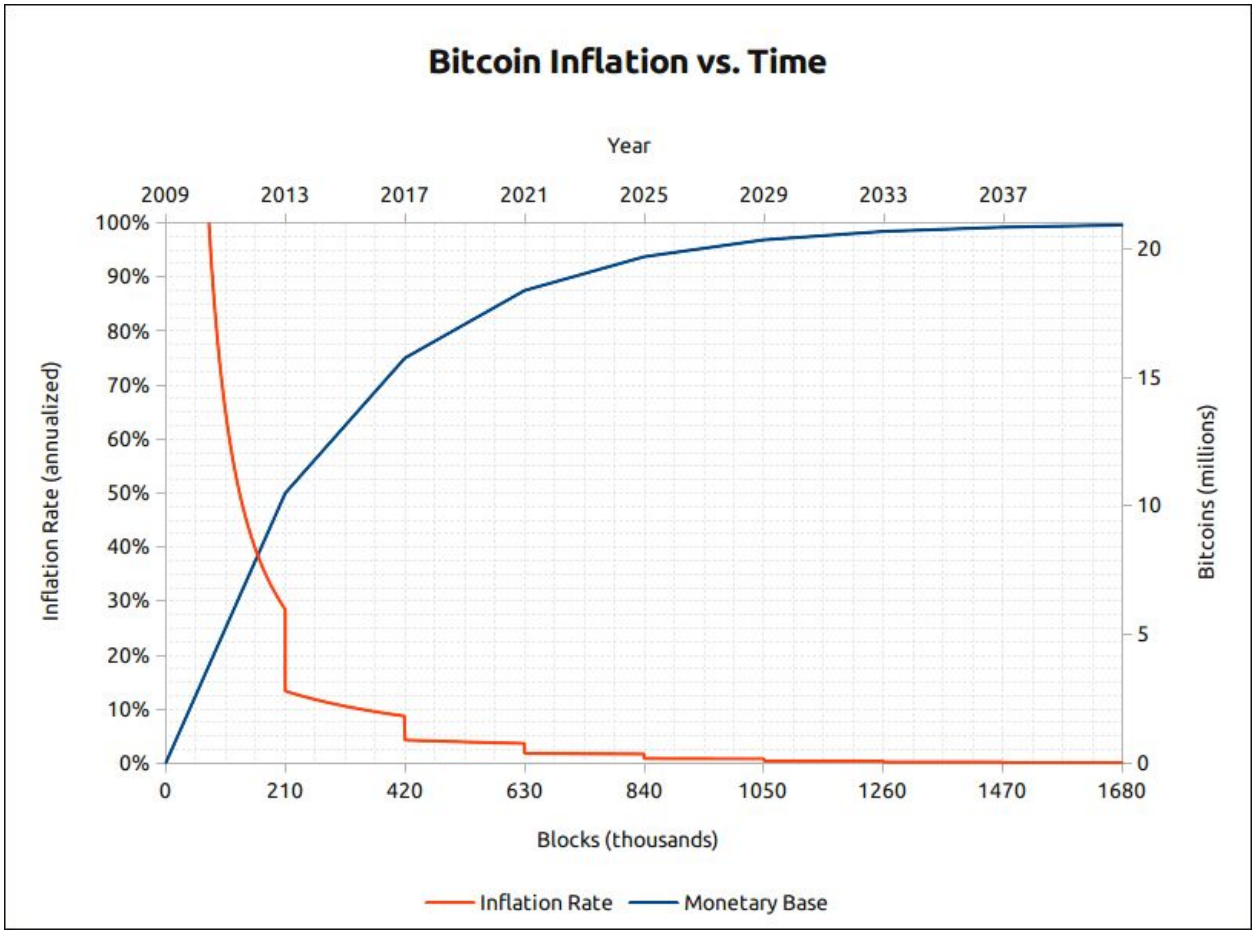


The irony is that almost every Bitcoin holder purchases BTC with the perspective of buying a deflationary asset, while at the same time not realizing that the current state is quite the opposite as BTC is still in high inflation mode. To further emphasize this paradox, few BTC owners realize that the current economy behind bitcoin is unsustainable in the context of a complete switch to deflation.

Simple math can prove this:
Block reward 6.25 BTC every 10 minutes = translates to an approximate $80,000 value per block created through inflation / $11.5M in 24 hour timespan.

At the same time, the current average 24h transaction count is in the 310,000 range. A $0.5 per transaction would imply a $157,500 transactional economy.

The transactional economy amounts to 1.3% of the total economy. A theoretical complete switch from Inflation to deflation at this point would lead to a 98.7% collapse of infrastructure security.



While Hydra is not aiming to reach such high inflation rates, depending on the proportion of the stakers, rates could rise significantly nevertheless.

This is why we believe that for an underlying blockchain platform, a predictable and high inflation rate is the best economic driver as it safeguards the network security, while tokens built on top should be deflationary. This is specifically the case with HYDRA, as it is complemented by LOC as a fixed supply deflationary HRC20 token.

Staking Rewards

Coin holders, who are planning to keep their coins for the long term have the opportunity to grow the amount of coins they own by staking them. As a mechanism this rewards the core community most and strengthens the security of the chain.

The inflation rate can be **voted** on as part of the Distributed Governance Protocol (DGP) by holders within the range of 0% and 25%. The voting will be held in regular intervals, giving the network enough flexibility to adapt to external and internal factors.

Due to the fact that not everyone will stake, the APR could end up being significantly higher than the inflation setting.

Example 1:

- Inflation rate set at 10%
- 40% of total supply being staked

→ APR = 10% / 0.4 = **25%**

Example 2:

- Inflation rate set at 15%
- 20% of total supply being staked

→ APR = 15% / 0.2 = **75%**

APR = *Annual Percentage Return*

The calculations above are based on inflation based block rewards only. On top of these, there will also be income arising from the fixed fees on a transaction basis, which will be voted on through the governance protocol and distributed with each block individually.

3.2 Flexibility to change between Inflationary and Deflationary State

Even though the Hydra Chain can be set at high inflation, there is also the functionality to turn it into a deflationary economy, if needed. For this to happen, the following two settings need to be enabled through votings:

1. The Inflation rate must be voted to 0%

2. The Burn rate must be voted to a value above 0%

This combination will effectively decrease the supply of coins over time, as a share of each transaction fee will be removed at protocol level. On the flipside, this will result in a significantly lower APR for stakers, as they will rely on the transactional economy solely.

Other Paths to Deflation

Although the above approach will certainly lead to deflation, there are also paths to deflation with inflation switched on. As outlined in Chapter 2, the only criteria for this is a strong transactional economy.

If there is enough activity on chain, the transactional economy can dwarf the staking rewards coming from inflation and thus coins can be burnt at a faster rate than they are created. We have created a highly functional staking calculator to explore this behavior (see section 3 of the calculator). You can access it from the link below.

Staking Calculator

4. Unique democratic governance that monetizes differences

Hydra offers a significantly enhanced governance protocol that provides the tools to its community to debate, vote and adjust the chain based on the preference of the majority. Without such tools, as history has proven, community differences can escalate and lead to forks that dilute the value of a chain. In addition to that, Hydra also effectively monetizes these differences.

A user friendly simple voting, embedded within the Hydra wallet, enables every single community member the ability to cast his/her vote by sending HYDRA to the vote smart contract. A system that accumulates HYDRA in favor of a “yes” and “no” with the side that has the biggest balance automatically being enforced from a certain block in the future.

Example

Vote for change of the Burn Rate on protocol level

Yes: 1,048 HYDRA
No: 958 HYDRA

Final outcome “Yes” wins. 2,006 HYDRA **burnt** as part of the process. A system that is protected against abuse and manipulation as each vote consumes the economy.

The more votes and the stronger the disagreement, the higher the economic benefit for all HYDRA owners as the higher the probability for more votes to be casted

Hydra goes on to the extent of enabling automated voting for critical features that other projects don’t modify.

Block size and Block time being perhaps the most difficult ones.

5. Technical Specifications of the network

The Hydra Chain in its core is based on the open-source production level Qtum blockchain, which on its own is a fork of Bitcoin Core with an Account Abstraction Layer that enables support for the Ethereum Virtual Machine (EVM).

This hybrid blockchain utilizes the well-established UTXO transaction model and employs a true Proof-of-Stake consensus, which has been evolved from the BlackCoin project. We are undertaking the evolutionary strategy of combining the best of Bitcoin and Ethereum and building on top of it, unique economic features, while preserving decentralization, supporting Ethereum applications and at the same time reaching notable TPS performance.

EVM offers full support of ERC20 as well as all other Ethereum compatible smart contracts. Full migration compatibility from Ethereum (or any other EVM supporting blockchain) to Hydra.

5.1 Proof-of-Stake consensus

Hydra utilizes “PoS V3”. Designed by Pavel Vasin - technology that has been proven as safe and effective by projects BlackCoin and Qtum

A brief history about the development of the technology:
(*Some extracts of this section have been sourced from technical blog post made on Earzl.net to which we have applied small adaptations*)

PoSv1 - Originally implemented in project Peercoin. It relied heavily on the notion of "coin age", or how long a UTXO has not been spent on the blockchain. It's implementation would basically make it so that the higher the coin age, the more the difficulty is reduced. This

had the bad side-effect however of encouraging people to only open their wallet every month or longer for staking. Assuming the coins were all relatively old, they would almost instantaneously produce new staking blocks. This however made double-spend attacks easy to execute. Peercoin itself is not affected by this because it is a hybrid PoW and PoS blockchain, so the PoW blocks mitigated this effect.

PoSv2 - This version removed coin age completely from consensus, as well as using a completely different stake modifier mechanism from v1. The number of technical modifications are significant. All of this was done to remove coin age from consensus and make it a safe consensus mechanism without requiring a PoW/PoS hybrid blockchain to mitigate various attacks.

PoSv3 - PoSv3 is really more of an incremental improvement over PoSv2. In PoSv2 the stake modifier also included the previous block time. This was removed to prevent a "short-range" attack where it was possible to iteratively mine an alternative blockchain by iterating through previous block times. PoSv2 used block and transaction times to determine the age of a UTXO; this is not the same as coin age, but rather is the "minimum confirmations required" before a UTXO can be used for staking. This was changed to a much simpler mechanism where the age of a UTXO is determined by it's depth in the blockchain. This thus doesn't incentivize inaccurate timestamps to be used on the blockchain, and is also more immune to "timewarp" attacks. PoSv3 also added support for OP_RETURN coinstake transactions which allows for a vout to contain the public key for signing the block without requiring a full pay-to-pubkey script.

Proof of Stake's Protocol Structures and Rule

- Impossible to counterfeit a block
- Big players do not get disproportionally bigger rewards
- More computing power is not useful for creating blocks
- No one member of the network can control the entire blockchain

The kernel hash is composed of several pieces of data that are not readily modifiable in the current block. And so, because the miners do not have an easy way to modify the kernel hash, they can not simply iterate through a large amount of hashes like in PoW.

Proof of Stake blocks add many additional consensus rules in order to realize it's goals. First, unlike in PoW, the coinbase transaction (the first transaction in the block) must be empty and reward 0 tokens. Instead, to reward stakers, there is a special "stake

transaction" which must be the 2nd transaction in the block. A stake transaction is defined as any transaction that:

Has at least 1 valid vin
It's first vout must be an empty script
It's second vout must not be empty
Furthermore, staking transactions must abide by these rules to be valid in a block:

The second vout must be either a pubkey (not pubkeyhash!) script, or an OP_RETURN script that is unspendable (data-only) but stores data for a public key
The timestamp in the transaction must be equal to the block timestamp
the total output value of a stake transaction must be less than or equal to the total inputs plus the PoS block reward plus the block's total transaction fees. output <= (input + block_reward + tx_fees)

The first spent vin's output must be confirmed by at least 500 blocks (in other words, the coins being spent must be at least 500 blocks old)

Though more vins can be used and spent in a staking transaction, the first vin is the only one used for consensus parameters.

These rules ensure that the stake transaction is easy to identify, and ensures that it gives enough info to the blockchain to validate the block. The empty vout method is not the only way staking transactions could have been identified, but this was the original design from Sunny King and has worked well enough.

Rules for PoS blocks:

- Must have exactly 1 staking transaction
- The staking transaction must be the second transaction in the block
- The coinbase transaction must have 0 output value and a single empty vout
- The block timestamp must have it's bottom 4 bits set to 0 (referred to as a "mask" in the source code). This effectively means the blocktime can only be represented in 16 second intervals, decreasing it's granularity
- The version of the block must be 7
- A block's "kernel hash" must meet the weighted difficulty for PoS
- The block hash must be signed by the public key in the staking transaction's second vout. The signature data is placed in the block (but is not included in the formal block hash)

- The signature stored in the block must be "LowS", which means consisting only of a single piece of data and must be as compressed as possible (no extra leading 0s in the data, or other opcodes)

Some Key features/characteristics of Hydra

- A true Proof-of-Stake consensus that enables every single user to stake without any requirement for a minimum amount of coins
- Total output of 75 - 85 TPS / 6.5M - 7.3M transactions per day (approximately 6 times the capacity of the current Ethereum network)
- One-click installers for running a node on an average household computer (after you install the node, you will be able to stake your coins)
- Ethereum VM support in order to have full compatibility and easy migration of Ethereum DAPPS and Ethereum smart contracts
- Coin owners are able to stake their coins to get a piece of the transactional economy from the LockTrip booking app as well as from all other DAPPS and tokens
- Revenue from the transactional economy shared with the ERC20, ERC223, ERC721 smart contracts – they will be accredited on a protocol level **with 50% of the fees they are able to generate through their transactions**. This technically means that Hydra is the first blockchain, which utilizes a true shared economy that sustainably incentivizes dAPP developers. The people who contribute to its adoption will benefit from the transactions they generate, regardless of their business model. **A unique opportunity for Defi** due to the enormous amount of transaction gas consummation and high transaction count.
- Easy installation of nodes for average users

Github Repository: https://github.com/LockTrip/Blockchain

6. Coin Distribution Event

Since Hydra chain has been financed and developed by the LockTrip team and community, the distribution of the HYDRA coins will happen to LOC holders **proportionally** to the amount they hold, over a gradual 12-month process. The launch of the blockchain is planned in three stages, of which each is described briefly below.

Stage 1 - Cold Launch

Stage 1 initiates with the launch of mainnet. The blockchain will initially be supported with nodes maintained by Hydra Foundation and thus will start off as a decentralized and permissionless network, which due to the consolidated amount of HYDRA, wil be characterized with relatively centralized staking power. This will be for a period of 3 months. During this time period, the external infrastructure will be set in place, such as exchange integrations, wallet integrations and the swapping mechanism will be installed, to be used by current LOC token holders on the Ethereum network.

As soon as these are in place, swapping will be launched for LOC holders and the migration will be officially commenced. LOC tokens on the Ethereum chain will be swapped for LOC tokens on the Hydra chain at a 1:1 swapping ratio, meaning that 1 old LOC (ERC20) token will be swapped for 1 new LOC (HRC20) token. This keeps the total supply of LOC unchanged.

In order to support on-chain transactions, a small supply of HYDRA coins will be available on exchanges for purchase immediately after the main-net has been launched.

Stage 2 - Airdrop to community

Stage 2 represents the main phase in terms of HYDRA coin distribution and gearing up the transactional activity on-chain. Over a period of 50 weeks, HYDRA coins will be airdropped to LOC holders on a weekly basis (2% per week), with a new snapshot being made each week.

For example, a user owning 10,000 LOC tokens at the time of the weekly snapshot, will receive 10,000 HYDRA x 0.02 = 200 HYDRA for that particular week. And the process will be repeated until 100% of HYDRA's total 18,585,933 supply is distributed entirely.

In order to incentivize HYDRA coin owners to stake their coins, the inflation rate will be set to 10% throughout the airdrop phase. The staking power of the community will grow gradually as the airdrop progresses and the staking weight of the company nodes will be reduced to allow for the community to slowly take over.

The transition towards complete decentralization will happen during this stage.

Stage 3 - Full Operation

The final stage marks the completion of the migration process. With the airdrop of HYDRA coins being finalized, both the transactional economy as well as the staking weight of community nodes will reach its natural trajectory.

The first voting round regarding the inflation rate will be held, allowing HYDRA coin owners for the first time to decide on the settings of the chain in a fully decentralized self-governing mechanism.