Hive: Fast. Scalable. Powerful. The Blockchain for Web 3.0

Decentralized Hive Ecosystem
(Dated: September 28, 2020)

Hive is an innovative and forward-looking decentralized blockchain and ecosystem built on the Delegated Proof of Stake (DPoS) protocol. Since its inception, Hive has steadily grown as an ecosystem. Myriad dapps, APIs and front-ends contribute to a general and straightforward accessibility of data, transactions and records, so that this existing diversity and utility ensure that the ecosystem is welcoming to content creators, consumers, investors and builders. Hive is developed to store vast amounts of content and to make it available for time-based monetization. The performance of the blockchain is designed to scale with widespread adoption of the currency and platforms in mind. By combining the lightning fast processing times and fee-less transactions, Hive is positioned to become one of the leading blockchain technologies used by people around the world.

CONTENTS

I. INTRODUCTION

Hive is an innovative and forward-looking decentralized blockchain and ecosystem built on the Delegated Proof of Stake (DPoS) protocol [1]. It is the first highly-scalable DPoS blockchain independent of central authority that addresses the problems of mass adoption and versatility of use.

Hive allows the easy storage and retrieval of immutable strings of data and information. It sports three-second zero-fee transactions and is designed to store vast amounts of content and to make it available for time-based monetization. Hive recognizes that transaction fees are often one of the largest challenges to facilitating development and flexibility of use on a blockchain. Instead of requiring potentially costly and inconvenient transaction fees, Hive uses a novel stake-based Resource Credit mechanism to create a fee-less model.

Hive also aims to overcome mainstream adoption shortcomings in blockchain technology and content publishing by improving on their accessibility. It leverages the coined *Proof-of-Brain* (PoB) concept by distributing a portion of the inflation to content creators and consumers. To earn without financial investment, individuals partake in a wide range of activities. Those include blogging, participating in discussions, curating others, building and engaging with dapps, playing games and more; their limits are only constrained by their own imagination to further the decentralization of the system. All content is always readily-available on the blockchain and retains its original integrity.

Since its inception, Hive has steadily grown as an ecosystem. Myriad dapps, APIs and front-ends contribute to a general and straightforward accessibility of data, transactions and records, so that this existing diversity and utility ensure that the ecosystem is welcoming to content creators, consumers, investors and builders.

Hive was created as an independent and decentralized fork of the Steem blockchain [2]. As a community-driven fork, its intention is to continue the strong community values that have been established, while also freeing the ecosystem from the burden of Steemit Inc. and its disproportionate influence. While that influence had threatened Steem's decentralization since its inception in 2016, it was kept in check by the means of a social contract. Following the sale of Steemit Inc to Sun Yuchen of the Tron Foundation In February 2020, the exploitation of this influence and loss of confidence in the continued viability of Steem ultimately led to the creation of the Hive blockchain.

II. HIVE ASSETS

II.1. Assets

The Hive network comes with two classes of cryptocurrency assets named *HIVE* and *Hive Backed Dollars* (HBD). Moreover, HIVE exists both under a liquid form (simply called HIVE) and a staked form (called *Hive Power*). HIVE is the liquid currency of the Hive ecosystem. It may be traded, staked, bought, and sold. Hive Backed Dollars are intended to be pegged to the United States Dollar (USD) at a one to one rate.

Hive Power (HP), the staked form of HIVE, is vested during a process referred to as a "*power up*". Upon being powered up, Hive Power can then be entirely or partially un-staked at will, in a process referred to as a "*power down*". Staked HIVE then returns to its liquid form (*i.e.* HIVE) in equal amounts over 13 weeks period, with a segment delivered every 7 days.

II.2. Resource Credits

Instead of relying on transaction fees, Hive uses a fee-less system that leverages rechargeable Resource Credits (RC). In this framework, each account holds a given amount of credits related to its stake. Those credits are then consumed when transactions are executed on the blockchain and automatically recovered with time. The amount of Hive Power attached to a given account determines its level of stake and allows for the calculation of the associated bandwidth. The latter indicates how much a given account could transact within a specific period of time and originates from the available Resource Credits of the account, displayed as mana.

Resource Credits self-replenish at a rate of 20% per 24 hours. Such a replenishment rate acts as a self-limiter and requires the account to stake an amount of HIVE directly proportional to the account's purpose and intent of use. An account that projects a higher rate of use will need more Hive Power than an account that rarely transacts.

Resource Credits are used up by different forms of transactions at different rates. A transaction that involves the post of a paragraph of textual material will deplete more mana than a transaction consisting in an asset transfer. The amount of mana required to transact is also impacted by the number of transactions during the time of use. Transactions made on-peak consume more resources than those made during low usage periods.

No account is entirely prevented from issuing a transaction should it be created with no investment or provisioning through a delegation (see below). Accounts that have 0 HP Power may still issue limited transactions that vary as

per time of use and blockchain load. For example, an account with 0 HP may have enough Resource Credits to successfully issue 2 textual posts or about 17 transfers during a specific period of use. In this way, Hive removes one of the biggest entry barriers for users and developers.

II.3. Delegation

Hive Power may be temporarily lent to other accounts using a feature called "delegation". Delegated HP may be granted to other accounts for any length of time. The retraction of an existing delegation takes a total of five days to return to its origin wallet.

Delegated HP is not counted as deduced from the delegator's stake in respect to governance-level impact (see section III), but no longer counts towards their Resource Credit totals. In contrast, delegated HP raises the recipient account's Resource Credits for the duration of the delegation, but does not augment their own pre-existing stake in regards to governance-level impact. Ownership of the stake is retained by the delegator.

II.4. Allocation and Initial Supply, Inflation and End Supply

Hive started out with the replicated supply derived from a snapshot of Steem. Based on common Proof of Stake theory [3], stake that partook in the centralization attack on Steem was excluded from the initial distribution to protect the new chain from any potential future 51% attack[1]. All accounts, excepted those that explicitly influenced the DPoS security failure, received an initial supply of HIVE, HBD and HP directly mirroring their existing balances on Steem. The balance snapshot was taken at the time of the hardfork that created Hive.

Hive's decreasing inflation rate is one of its key monetary features and reducing minting over time. The inflation rate decreases by 0.01% with every 250,000 blocks, approximately 0.5% per year, until it reaches 0.95%.

Hive inflation is distributed in the following manner:

1. 65% is used to fill the reward pool (which is split in equal portions between content producers and curators);
2. 15% goes to HP stakeholders;
3. 10% goes to the witnesses for block signing;
4. 10% goes to the Decentralized Hive Fund (see the next subsection).

There is no pre-defined known value limit to Hive supply. The supply is dependent on the inflation rate.

II.5. Decentralized Hive Fund

The Decentralized Hive Fund (DHF) is a proposal-based DPoS financing alternative. The DHF places the consensus behind direct financing of development and other ecosystem-positive projects into the hands of the stakeholders. The distribution of the DHF is decentralized by design. Support for a proposal is calculated based on the total stake in support of that proposal. When a user opts to support a number of proposals, their stake influences the proposals equally. Support for a proposal may be granted or removed but the mechanism cannot be used to negate the sum of supporting stake with a negative vote. This prevents one single large stakeholder from doubling the impact of their stake and influencing the remuneration of numerous proposals, creating a level playing field.

Proposal funding is released when the total value of that supporting stake surpasses the stake behind a benchmark proposal. The benchmark proposal itself may vertically traverse the rankings as per the amount of its supporting stake. The payments are distributed on a hourly schedule over a set period of time as specified upon launch of each proposal. Proposals that surpass the benchmark proposal and unlock funding will receive the funding as remaining in the total ask of the proposal minus the time that had passed prior to funding. The total amount is only released where the proposal unlocks the funds prior to its scheduled duration.

---

[1] Interestingly, the creation of Hive was the first time in blockchain history that a full-scale migration was applied as a mitigation, speaking to the viability of Proof of Stake blockchains to recover from 51% attacks.

III. BLOCK PRODUCTION, SIGNING AND CONSENSUS

III.1. Delegated Proof of Stake

Delegated Proof of Stake (DPoS) is the consensus algorithm behind Hive. In a DPoS algorithm, the selection of block producers (called 'witnesses' on Hive) and all other consensus-based functions are decided based on the weight of staked funds supporting them. Stakeholders hold the highest prominence in DPoS. DPoS consensus is considered to be the most inclusive and the least centralized of all the blockchain protocols.[2] DPoS was first invented by Dan Larimer as a functional alternative to the Proof of Work system introduced with Bitcoin. Other prominent DPoS blockchains include BitShares and EOS; they are originally based on Larimer's Graphene framework.

III.1.1. Addressing 51% Attacks

A 51% attack may occur on a DPoS blockchain when a single stakeholder takes direct or indirect control of 51% or more of staked assets. Hive was originally created as a direct result of a 51% attack on the Steem blockchain committed by the founding company Steemit Inc. through unprecedented collusion. Due to its direct experience with the pattern, warning signs, capabilities and results of such attacks, the Hive decentralized community is regularly monitoring for any such attacks. Additionally, Hive has taken steps to deter and mitigate 51% attacks at the blockchain level through governance provisions, including delayed voting with any newly-staked HP.

III.2. Protocol Changes

Hardforks and key protocol changes are accepted by 17 out of 20 consensus witnesses. Witnesses accept protocol changes by updating their nodes or reject them by continuing to run the present version. Protocol changes will not be applied and take effect until consensus is reached. All protocol changes are proposed, developed, prepared for and implemented through a transparent and collaborative team-working environment. They are entirely open source from initiation to their final release.

III.3. Production Ordering

Blocks are produced at 3 second intervals and are signed by "Witnesses" selected based on the total weight of the Hive Power supporting them through individual approvals. There are 20 consensus witnesses that are granted block signing operations on a rotating schedule.

Every account may select up to 30 witnesses for approval, during which process it adds to the support each witness receives. The witnesses are ranked in priority based on the total amount of staked support they presently receive. While the 20 consensus witnesses have an equal opportunity to sign blocks, witnesses ranked 21 and further are treated as backup witnesses. The number of signing opportunities they receive is directly proportional to the staked support behind them.

Should a witness be unable to sign a block due to operating on a protocol version incompatible with the main chain or due to any other technical issue, the signing opportunity will be automatically granted to the next scheduled witness. The witness that failed to sign will be recorded on chain as have missed a block.

III.4. Price Feed Consensus

Hive witnesses are responsible for dependable and consistent price feeds.

The purpose of price feeds is to promote:

1. Exchange rate stability
2. Price accuracy
3. Dependable monetary policy

---

[2] Holbrook, J. (2020). Architecting Enterprise Blockchain Solutions (p.128). Sybex.

III.5. Node Types

There are several different types of nodes on Hive that are run by decentralized community members. These nodes are operated with different configurations and with the goal of optimizing resources and accessibility.

1. Witness Nodes: A witness node is used for signing blocks.

2. Seed Nodes: A seed node allows external peer-to-peer (P2P) connections.

3. API Nodes: An API node is any node that allows external remote procedure call (RPC) connections. It may have a selection of plugins.

III.6. Keys

There are private and public key pairs on Hive. All key pairs are directly derived from a password or passphrase, which in itself is not a key. Changing the password regenerates the key pairs. Public keys are openly available on the blockchain while their private counterparts are only granted to the account owner. Both pairs are required to validate a transaction.

III.6.1. Key Hierarchy

Hive uses a weighted hierarchy of keys:

1. Owner Key: Used for recovering accounts and regenerating other keys as well as setting a new password.

2. Active Key: Used to transfer and manage funds, vote for witnesses or approve DHF proposals.

3. Posting Key: Used to broadcast posting transactions.

4. Memo Key: Used for decrypting encrypted messages within the memo parameter of fund transfers.

Witnesses use their accounts to generate an additional key called a Signing Key. That key is used to indicate that a witness is available for block production and is unique to that witness. A default, static Signing Key may be broadcast by a witness account to disable itself as block signatory. This lets the blockchain know to not schedule that witness in the production order. To resume block signing, the witness must broadcast its unique Signing Key again.

III.6.2. Trustee System and Recovery

Where an account is compromised through phishing or a similar theft and its keys are changed without the owner's consent, it may be recovered by its Trustee Account. The default trustee of an account is the account that created it in the first place. Upon its creation, a new account may broadcast a transaction requesting a different Trustee. The trustee change takes 30 days to reach finality. Recovery is only possible where the period between the password change or owner key regeneration and the recovery itself is less than 30 days.

IV. DEVELOPMENT AND INTEGRATION WITH HIVE

Hive strives to be the perfect real-estate for existing and new dapps and ventures to build on. It is based on ChainBase, an evolution of Graphene. ChainBase is resilient against blockchain crashes and block corruption and is faster and more versatile than its predecessor. It permits snapshots to be created of its state and allows for parallel access to the database while handling a scaling amount of RPC requests easily without a significant increase in memory use. Hive is open to and can be readily utilized by all lines of business.

IV.1. Integration

Cross-platform and application integration is inherently simple on Hive. Custom JSON (JavaScript Object Notation) operations may be declared on Hive and are frequently used by dapps to encode a range of text data onto the chain. JSON is a commonly used by the majority of modern applications and is compatible with virtually every programming language. This directly translates to the fact that almost any application may be connected with and make use of the Hive blockchain.

Custom JSON acts as a modifiable database which is customized to the explicit needs of the dapp. Any data that may be contained in a text string can be encoded at once. A dapp that requires its users to publish an additional identifier as part of a specific transaction may do so with custom JSON. That data can then be easily fetched either through a script that monitors the blockchain in real time or through various other mechanisms. Hive's flexibility with data storage and easy integration makes it possible to cover the needs and wishes of practically any requirement in the most user friendly of ways.

IV.2. Performance

To facilitate widespread and barrier-free integration, Hive currently utilizes and will continue to improve upon layered solutions. Hive is a scalable and flexible blockchain by design. It is equipped to support a larger database than any of its competitors. It allows for near real-time transactions that can be adapted for any application requiring speed and modularity. To support rapid scaling, non-consensus ledgers are implemented as plugins. A Hivemind (Python) database-driven 'consensus interpretation' layer acts as an API for the blockchain and eases both interaction and node requirements. The tiered layers are leveraged to allow Hive to scale at a manageable rate while it organically grows and expands. In addition to Hivemind, other key layers are projected for development as part of the deliverables roadmap.

IV.3. Endusers and Consumers

No initial investment is required on behalf of an account holder to participate in Hive and by extension to use any of the dapps connected to or built on Hive. Users may begin transacting immediately upon account creation. Non-investment stake growth is achieved by contributing textual content (publishing) and interacting through the curation of others. A dapp or venture has the option of introducing their product to existing userbase, onboarding its own clientele, or simply utilizing the blockchain as a data ledger for external consumers.

V. ECOSYSTEM GROWTH AND DISTRIBUTION

V.1. Onboarding and Accounts

Just like the rest of the Hive ecosystem, account creation is decentralized. Existing Hive accounts create new Hive accounts, which can then be provided to new users when they join Hive. The creating account then by default becomes the trustee of the created account and may take on additional roles such as account recovery in case of stolen password. This enables a positive and accessible onboarding and initial experience process for new users.

Multiple account creation services are in existence and are both diverse and offer free and paid options. The diversity in onboarding approaches and account creation options is ideal for providing a cryptoworld entry point for those who have never dabbled in cryptocurrencies or are unfamiliar with blockchain technology. New users are not required to manage complex wallets and register accounts with Exchanges prior to participating in Hive and interacting with their accounts.

A Hive wallet is also the account name; it is not a numbered wallet as on other blockchains. The username is the sole user identity in the Hive ecosystem. Hive does not leverage account hierarchy. Anyone may register any available username they wish. It may be of any composition as long as it is between 3 and 16 characters in length and adheres to minor special character constraints. New accounts may be instantly generated by an existing account for a small creation fee or a free 'claimed account token' where the claimer is an investor with an investment over a certain benchmark. All accounts cost the same upon registration irrespective of the account name. This promotes fairness and open opportunity for those entering the Hive ecosystem.

V.2. Censorship Resilience by Design

Hive is by design a decentralized blockchain that is sustained by geographically distributed servers and nodes. Every transaction is transparently and chronologically entered into blocks and signed onto the public ledger. All transactions entered onto the Hive blockchain have the element of finality and once confirmed in its three-second blocks, are irreversibly signed. Altering the content of recorded transactions and blocks is not possible as that would alter the state of the blockchain post-finality. Therefore, taking the default unalterability into account, no content on the Hive blockchain may be arbitrarily censored or altered in any way, shape or form.

Hive does not regulate its APIs or provide constraints on the type of endpoints that may be built on it. Individual front-ends and websites may present or not present segments of Hive content as they deem fit. This does not adversely impact the availability of the material stored on the Hive blockchain. With its censorship-resilient design, Hive is a dedicated proponent of free speech and transparency.

V.3. Communities

Communities are a topical way to organize and manage the frontend-facing collation and discoverability of user-generated content. They leverage the tag and follow features to sort, manage and thematically organize segments of content. A community is an account that is also set as a category for the content published in it. Upon its creation, a new account is generated and is then granted a modifiable label to display on the frontends. The community account itself may also opt to transact in the same way that any other account; it may post, cast votes, make transfers, and create other accounts.

Once a community is created, it may be labeled as desired and operated by its owner. Users may join communities, submit content to them, manage communities where they are set by the owner as administrators, hide undesirable submissions by muting them, give them descriptions and perform many other interactive actions with the ultimate goal of building an active and cohesive community.

With the majority of the community infrastructure based upon a layered approach and creative utilization of core blockchain features, communities are designed to be both flexible and functional. The naming of communities is not exclusive and multiple communities may have the same or similar names; their base account is set by a *hive-000000* name-number naming convention. This prevents name squatting and allows any user to form a community on any topic. Where numerous similar communities are in competition, the one with the highest rate of user engagement will become the main community on its chosen topic but without disabling or otherwise harming its competition. It is important to note that communities do not generate monetary rewards for their owners and organizers by default; their value is a purely qualitative improvement to the user experience. However, frontends may augment community features with additional revenue generation capabilities.

V.4. Qualitative Content-based Inputs

Hive has two streams of designed monetization: quantitative and qualitative proof-of-brain work. Quantitative work refers to automated processes with predetermined compensation mechanisms such as operating a witness node. Qualitative work refers to the creation and provisioning of consumer-focused content such as articles, linked or embedded videos and images, apps, games, curation, community organization, and work funded through the proposal system. Out of that scope of work, the two mainstay contribution options are the addition of content and the service of content discovery.

V.5. Content Monetization

Hive is by design intended to store vast amounts of content and to make it available for time-based monetization. Content may be submitted in the form of a 'post' (parent post) or 'comment' (child post). Once submitted, a piece of content will be monetizable for a period of 7 days. During that time it may be curated upwards or downwards through upvotes and downvotes until its final value is determined at the end of the 7 day timer. Where a front-end or website displays the value approximation prior to the completion of the 7 day timer, that approximation is variable and has not yet reached finality. Posts and comments are subject to the same monetization timer.

All qualitative actions carried out on Hive are by default solely leveraging individual users' organic stake. When content is submitted and the monetization period starts, that content is evaluated through curation in a proportional

manner that is influenced by its discoverability, its quality, the reputation and popularity of the presenter, its originality, and its subjective value to the ecosystem. This interaction is reminiscent of both social media networks and traditional economies. When large waves of content contributors use Hive at the same time, discoverability naturally goes down and competition goes up. Simultaneously, content consumption rises as the many contributors are also consumers, while others only consume without contributing. When such a surge occurs, the potential value of individual content pieces fluctuates due to the increase in competition (which in some popular niches may also equate with market saturation) and the gap between the top and bottom monetized content expands.

V.6. Distributing Rewards

The reward pool is used to distribute funds to those who actively participate in creation and/or curation of content. The funding for the reward pool is composed out of 65% of the inflation.

When a user submits a post it initiates a 7 day curation window during which it may be upvoted or downvoted until its final evaluation is reached at the end of 7 days. Upon reaching final evaluation, 50% of the earned rewards are granted to the creator and 50% are proportionally split between the curators who have voted for the post with a positive value. Voting with a negative value does not generate curation rewards.

Distribution is carried out in a manner that automates partial staking. A modifiable percentage of each distribution is granted as HP. The remainder is granted as either HIVE or HBD, depending on the market value of HIVE to HBD.

VI. CONCLUSION

Hive is a constantly evolving and innovative ecosystem that aims to fuel mass adoption of blockchain technology and cryptocurrencies. It makes available and possible opportunities to both its userbase and to the general public. Since its inception, it has steadily grown as an ecosystem, with a diverse family of communities, dapps, content creators, investors and consumers. The performance of the blockchain is designed to scale with widespread adoption of the currency and platforms in mind. By combining the lightning fast processing times and fee-less transactions, Hive is positioned to become one of the leading blockchain technologies used by people around the world.

[1] F. Schuh and D. Larimer, "Bitshares 2.0: general overview," *accessed June-2017.[Online]. Available: http://docs. bitshares. org/downloads/bitshares-general. pdf* (2017) .

[2] D. Larimer, N. Scott, V. Zavgorodnev, B. Johnson, J. Calfee, and M. Vandeberg, "Steem: An incentivized, blockchain-based social media platform," *March. Self-published* **4** (2016) .

[3] V. Buterin and V. Griffith, "Casper the friendly finality gadget," *arXiv preprint arXiv:1710.09437* (2017) .