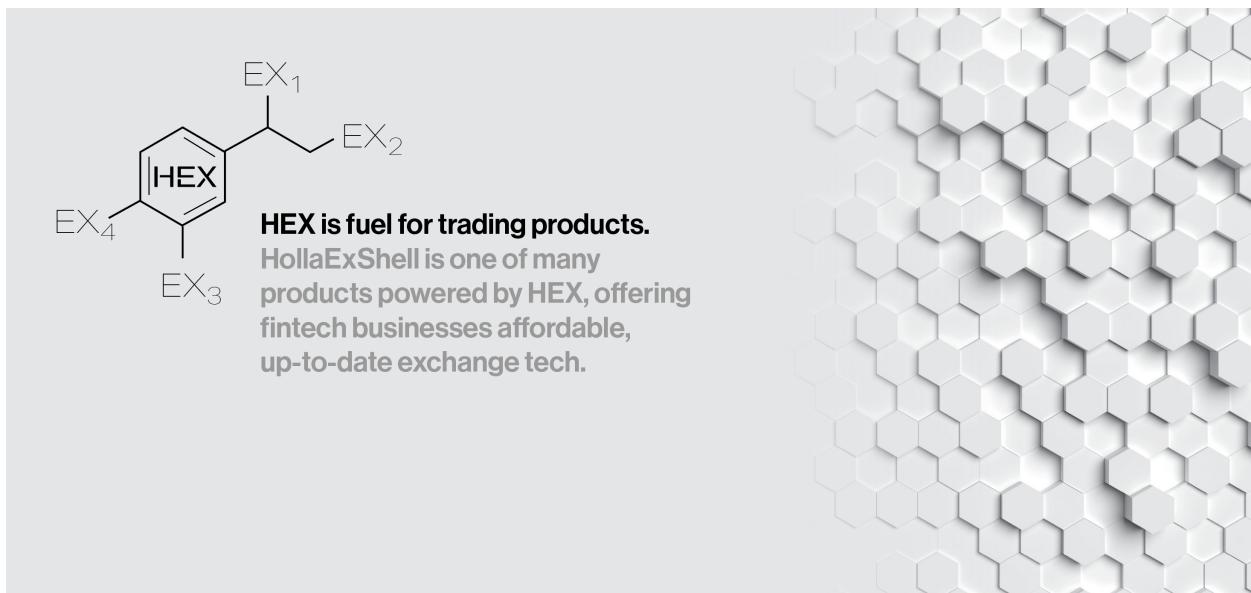


# HEX Whitepaper

## Distributed Exchange Network



**HEX is fuel for trading products.**  
HollaExShell is one of many  
products powered by HEX, offering  
fintech businesses affordable,  
up-to-date exchange tech.

## Abstract

With the emergence of crypto industry, we have seen a significant growth in open financial tools and services and primarily in exchanges. Exchanges are marketplaces that help us discover price in open supply and demand markets. As result exchanges create markets that are accessible to large number of participants whom can conduct transactions in a fair and efficient manner. Exchanges for a very long time have been multi billion dollar area accessible to few, however it's becoming more accessible today due to cryptocurrency and blockchain demand in the market. BitHolla Inc as a trading and exchange software technology provider introduced a new software package, **HollaExShell**, designed to enable businesses and individuals to launch and operate scalable exchange platforms on their own. This is achieved by creating a dynamic trading system with a flexible setup and configuration that can host infinite number of digital assets and cryptocurrencies. The solution provides a full trading platform including matching engine, APIs, real-time data feed and market data stream all available in a customizable trading terminal.

By utilizing blockchain technology based on Ethereum's smart contract, we created an exchange network known as **HEX Network** running on HEX fuel which creates an open ecosystem for businesses and individuals to operate and run a friction-less exchange. It would also create an opportunity for investors and other participants to allocate funds and share liquidity for exchanges through HEX in the distributed exchange network in an autonomous manner.

In this Whitepaper we go through the exchange history in the Background section and explain the motivation behind this ecosystem. We then describe the exchange and software specification of HollaExShell, its design and architecture as well as its components. Afterwards we discuss about the HEX Network and exchanges as participating nodes in the network and proceed with the token model and its distribution. Ultimately, future considerations, Roadmap and the conclusion to wrap up.

**PLEASE NOTE: THIS WHITEPAPER IS ONLY FOR EDUCATIONAL PURPOSE AND BEFORE ANY PURCHASE OF HEX TOKEN, YOU ARE REQUIRED TO READ AND ACCEPT THE TOKEN PURCHASE AGREEMENT OF HEX FOUNDATION IBC CO (NO 193571) REPUBLIC OF SEYCHELLES INCORPORATION.**

Copyright © 2019 bitHolla Inc.

Without permission, anyone may use, reproduce or distribute any material in this white paper for non-commercial and educational use (i.e., other than for a fee or for commercial purposes) provided that the original source and the applicable copyright notice are cited.

**DISCLAIMER:** This HEX Technical Whitepaper is for information purposes only. BitHolla does not guarantee the accuracy of or the conclusions reached in this whitepaper, and this whitepaper is provided "as is". BitHolla does not make and expressly disclaims all representations and warranties, express, implied, statutory or otherwise, whatsoever, including, but not limited to: (i) warranties of merchantability, fitness for a particular purpose, suitability, usage, title or noninfringement; (ii) that the contents of this whitepaper are free from error; and (iii) that such contents will not infringe third-party rights. BitHolla and its affiliates shall have no liability for damages of any kind arising out of the use, reference to, or reliance on this whitepaper or any of the content contained herein, even if advised of the possibility of such damages. In no event will BitHolla or its

affiliates be liable to any person or entity for any damages, losses, liabilities, costs or expenses of any kind, whether direct or indirect, consequential, compensatory, incidental, actual, exemplary, punitive or special for the use of, reference to, or reliance on this whitepaper or any of the content contained herein, including, without limitation, any loss of business, revenues, profits, data, use, goodwill or other intangible losses. The information in this document does not constitute a recommendation by any person to purchase HEX or any other cryptographic token or currency and BitHolla has not authorized any person to make any such recommendation. HEX tokens are speculative and involve a high degree of risk and uncertainty. The sale of HEX tokens is aimed solely at persons who have sufficient knowledge and understanding of blockchain and cryptographic tokens and other digital assets, smart contracts, storage mechanisms (such as digital or token wallets) blockchain-based software systems and blockchain or distributed ledger technology, to be able to evaluate the risks and merits of a purchase of HEX tokens and are able to bear the risks thereof, including loss of all amounts paid and loss of HEX tokens purchased. Potential purchasers must further make their own independent assessment, after making such investigations as they consider necessary, of the merits of, and their suitability for, purchasing any HEX and should consult their accounting, legal and tax representatives and advisers in order to evaluate the economic, legal and tax consequences of purchasing HEX tokens. Certain statements contained in this document may constitute forward-looking statements or speak to future events or plans. Such forward-looking statements or information involve known and unknown risks and uncertainties, which may cause actual events to differ materially. No reliance should be placed on any such forward-looking statements or information.

## Background

### First Phase: Institutionalization of Exchanges

The Italians created the basic concept of modern banking and stock markets, bringing the double entry book keeping into popular use. Before that exchanges were nothing more than gathering places for people to trade various goods and it wasn't until 1409 in the city of Bruges in Belgium where the concept of exchange was formalized and become an institution. The Exchange Bruges also known as

an inn 'Ter Buerse' became the first formalized exchange and because it was an inn many foreign merchants from across Europe began trading there. The word Bruges is a reference to the square and trading was not restricted to just the building but more a reference to the square as a whole where merchants gathered to trade outside. The word Bruges was then later corrupted into bourse and then the English popularized the word 'Royal Exchange' to what we simply use today as 'Exchange'.

This was the first phase, summarized as the institutionalization phase, where larger and larger concentration of wealth formed. It is important to note the direct trading on these exchanges were highly restricted and most of the public did not benefit directly from these markets. Instead connected brokers got between all trades —those nearest to the center of the exchange naturally profited the most.

As a side effect, exchanges have now grown into gigantic institutions that are ruthlessly protected by captured regulators. This protectionism has made it unthinkable for individuals to open an exchange due to the extreme costs and complexities in procedures of opening a new exchange.

## **Second Phase: Dematerialization of Assets and Trade**

The dematerialization phase was a significant phase, granting wider access to the exchange. Thanks to digitization, much of the world's assets now live on computers and since the 1970s assets have gone through mass dematerialization which involves a large scale shift away from paper certificates to digits on a screen. Some of these assets that have largely been digitized are:

- Stocks
- Currency
- Bonds
- Commodities such as gold, silver and oil ETFs

Still, one stubborn issue remained, the ownership and transfer of assets still relied on large number of middlemen. Heavy oversight and reliance on institutions to facilitate online trades despite being 'digital'. Although many of these assets can be turned into bearer instruments, meaning you can in some fashion claim physical ownership over the asset in the form of a paper certificate, it is costly and time consuming, rendering it unpractical for most to do so.

Most of the big assets trading today, such as gold ETFs have to go through a complex network of reliance to facilitate any trade, which the large exchanges have abstracted away at a high cost, hence why we still have high costs trading stocks internationally.

## **Third Phase: Deinstitutionalization of Exchanges**

Crypto has finally divorced the asset from the exchange and is marking the beginning of deinstitutionalization phase. Previously, all valuable assets such as stocks and gold ETFs required multiple establishments such as a bank, exchange and clearing house to grant 'real' ownership over any asset. But now with crypto the asset can stand on it's own without the need for an established financial institution.

As a result of these new digital bearer instruments such as Bitcoin, the exchange model and their role in society has shifted. Venues such as the NYSE and the NASDAQ whom up until now have enjoyed an almost complete monopoly on the worlds most valuable assets have for the first time been losing market share to small shop exchanges such as Binance and Coinbase. In effect the third chapter for exchanges is now in motion, and can be classified as the deinstitutionalization phase.

Acceleration of the deinstitutionalization phase is occurring largely due to increasing practice of tokenization of assets via open source protocols such as ERC20. Tokens provide the freedom to a wider gamut of investors to easily get involved in any project globally for fractions of the cost and right at the ground level.

No stock on a traditional exchange can be delivered in a peer-to-peer fashion, let alone globally. Because tokens are global and grant the holder real peer-to-peer transferability by default, future generations of investors will build a preference for digital assets and exchanges that offer them.

The paradigm shift in trade is creating a preference for exchange venues with assets that can actually be traded without the multiple parties oversight, including the exchange.

Digitally native assets such as bitcoin are not only separating state and money, bitcoin is separating investing from institutions. Allowing for unhindered peer-to-

peer exchange to occur, either on or off the exchange, a throw back to how trade was done 1000s of years ago.

## Motivation

We described how trade as an important element in commerce has grown to this date in the previous chapter. In the modern digital era and the emergence of digital tokenized assets, there is a significant demand for modern automated trading system. Exchange solutions are at the heart of this demand and they initially proved their significance in our societies during the dot-com era with examples such as NASDAQ and NYSE. With the growth of cryptocurrencies and the desire for open economies and markets, we believe that now more than ever, people need to have access to trading and exchange technologies globally. With all the asset tokenization including STOs and ICOs and freedom in trades, HEX with its exchange network and model is aimed to enable and create an economy to empower markets and boost trades all around the world.

## Exchange Specification (HollaExShell)

HollaExShell is an open exchange software toolkit system solution that comes in multiple components which are explained in this section in details.

While the HollaExShell as software solution is a standalone system, The exchange solution is considered as a node in an exchange network called HEX Network in which participants are exchange operators and it relies on HEX Token to run and function. HEX is considered as a fuel for the system to run and it has its own economic model described in later chapters.

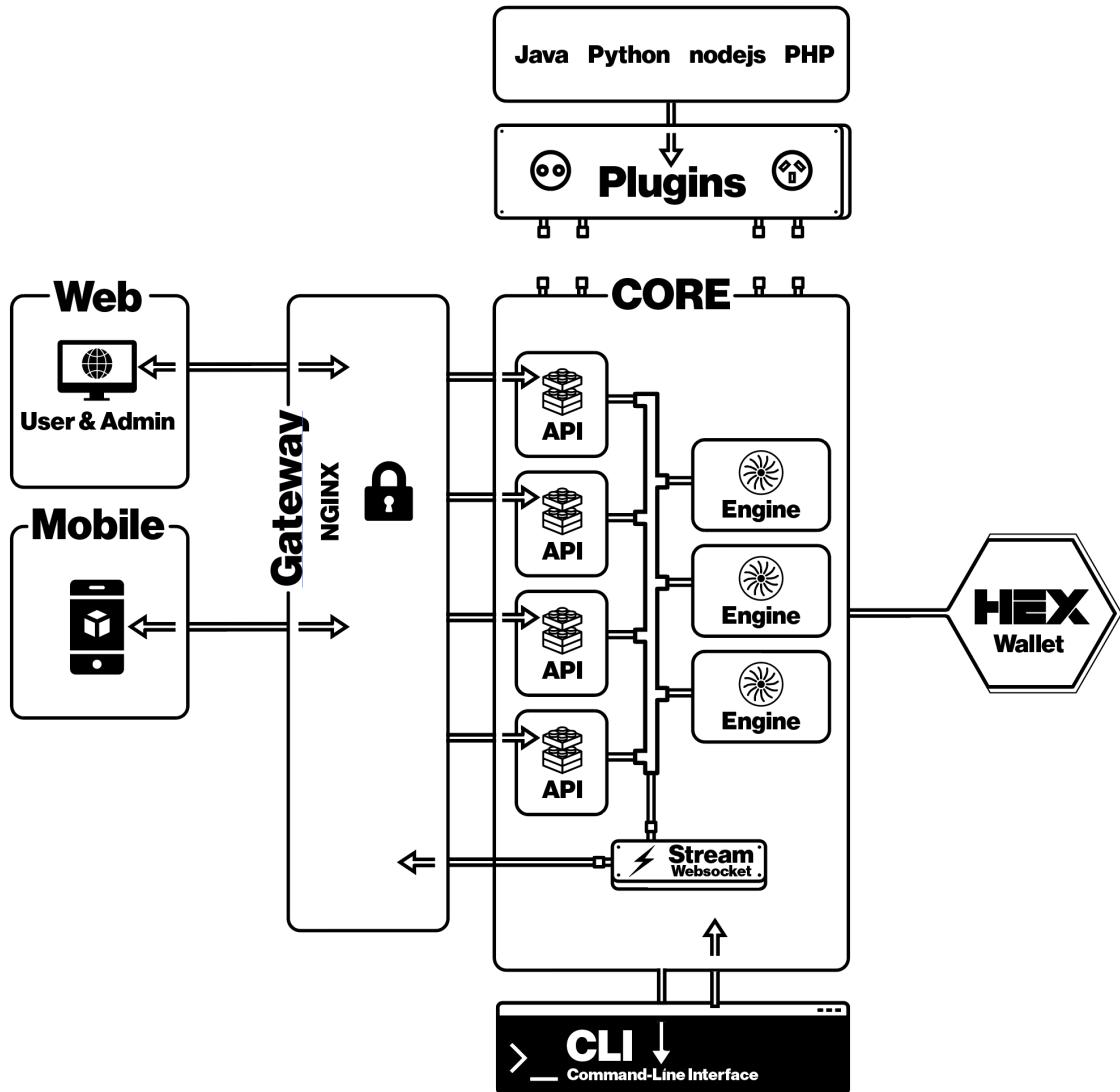
In this chapter we describe the exchange system specification and how the software in HollaExShell works.

*The software has been in production for more than 2 years and is used in numerous exchanges globally serviced by bitHolla.*

## Component

HollaExShell consists of 7 components:

1. **Core:** It refers to the main system that comes in binary and includes **API**, **Stream** and **Engine**.
2. **Gateway:** Entrance of the system as a system gateway. It connects external to internal network.
3. **Plugin:** Plugins are modules provided in an open market by developers which are built on top of core system.
4. **CLI:** Command Line Interface which helps communication with core and manages build, deployment and system activation through simple commands.
5. **Web:** Web application client provides a simple intuitive interface to exchange clients as a trading terminal as well as an admin dashboard with special access control. This component is considered as the system front-end. Admin Panel section is embedded in Web component and it is a dashboard for admin which comes with multiple roles and allows admin, support, supervisor to interact and support the back-bone of the system and its configurations.
6. **Mobile:** Mobile Application provides an interface to the exchange on Android and iOS.
7. **HEX Wallet:** HEX token is used by exchange operators to run and operate their exchange. Additionally it is also used as a means to obtain other financial software products such as bots and wallets. HEX wallet is embedded into the Shell system and manages the HEX wallet related operations of the exchange.



## HollaEx Core

Core is the main system technology back-end which empowers the exchange system. Core can be accessed and used through HollaEx CLI explained later in the whitepaper.

HollaEx Core contains three main modules: API, Stream and Engine. It is also flexible to adopt additional modules as a plugin attached to the system.

**API** is the main worker service in a microservice architecture that manages all the endpoints and requests to the system as a front gate. It's microservice architecture makes it a highly maintainable, testable and scalable service. All services are loosely coupled and are independently deployable. All the

communications outside the system use RESTful API endpoints and through JSON objects which are managed over Transport Layer Security (TLS) channels.

API module additionally manages user accounts, authentication scheme and serves as a primary gateway for all major APIs documented on HollaExShell.

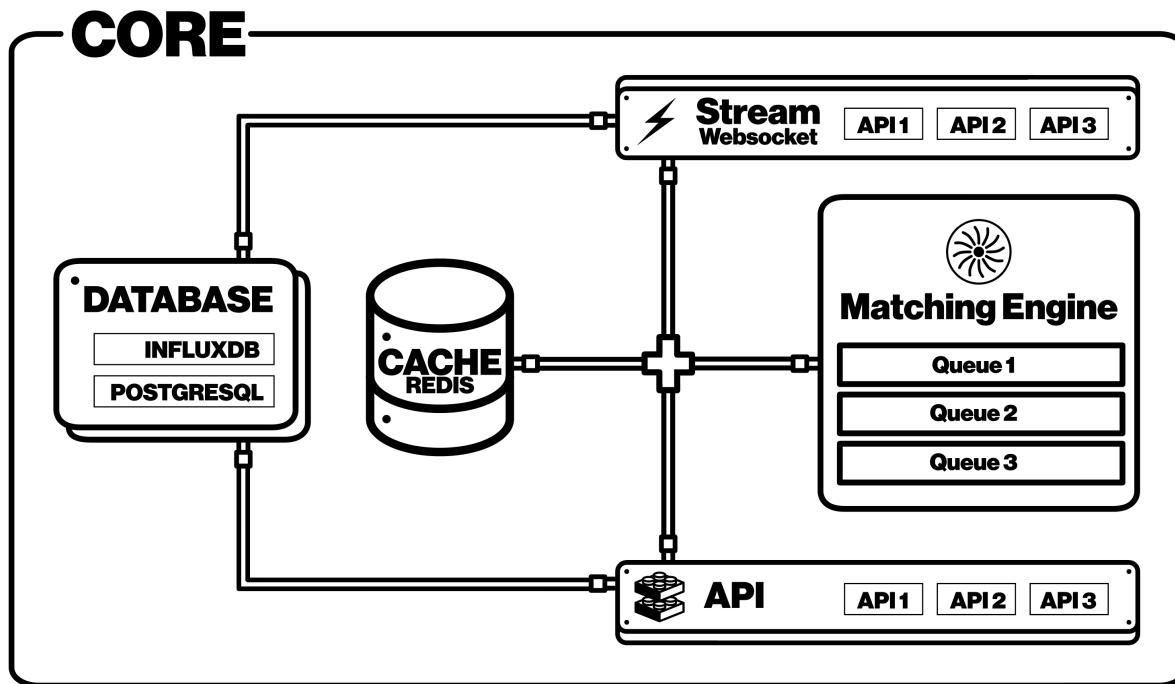
**Stream** handles real-time stream and datafeed and is the essential component which manages all websocket communication.

This [GitHub library](#) provides full abstraction of API and Stream channels for developers and the API documentation is available [here](#).

**Engine** is the core matching engine which takes care of the trading pairs, orderbooks, user orders and real-time trades.

Lets say the exchange is configured with three trading pairs ETH-BTC, BCH-BTC and XRP-BTC. Therefore we require 3 engines that are configured to each trading pair accordingly.

The full core is packaged through binaries in docker image provided by bitHolla which can be freely downloaded.



The Core details; dedicated trading engine with queue each created for each trading pair.

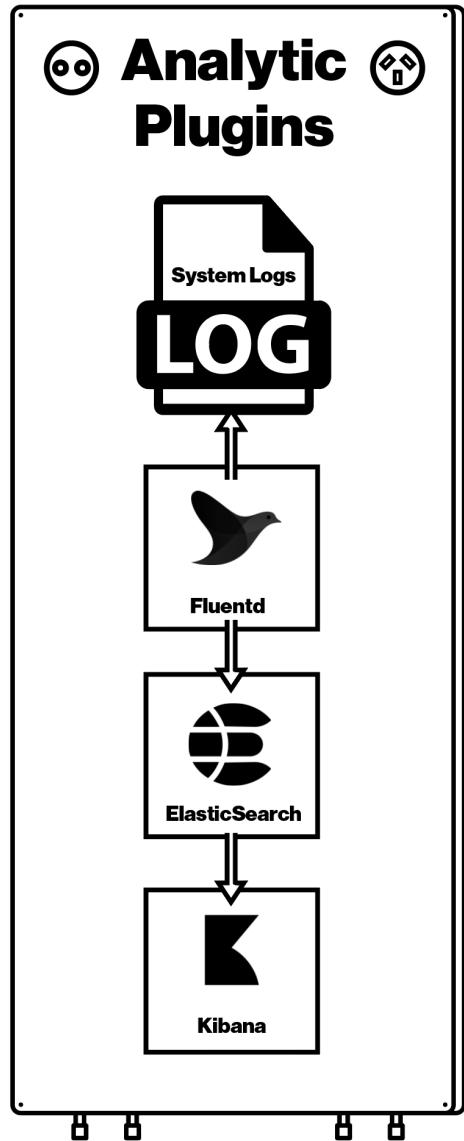
## **Gateway**

HollaEx Gateway is the secure entrance gate to the system. It is responsible for all the inbound and outbound traffic to the system. It protects the system against malicious activities as well as managing the security of the system.

The Gateway uses standard NGINX for handling SSL/TLS communication as well as traffic routing to different components. Gateway is configured as part of the HollaEx CLI and can be customized by the client if its required.

## **Plugin**

HollaEx Plugins are additional sidecars that can be attached to HollaEx Core. Plugins enable additional functionalities to the basic exchange core technology. Plugin can be added either as a binary file or a custom code. Custom code allows the exchange operator to make and run their own custom code on top of the system. There is a market place for plugins where developers can create and maintain for their clients.

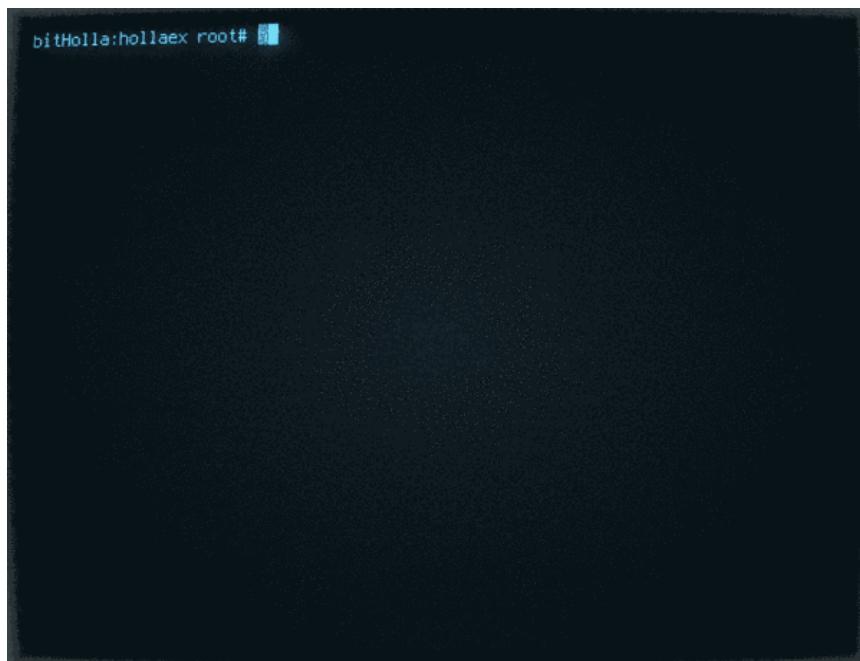


Example of analytics and logging plugin

Some plugins can be obtained directly from bitHolla such as Vault a crypto wallet system, Robolla an automated liquidity provider bot and XRayTrade exchange listing that increases the exchanges exposure to traders globally. Moreover there will be a marketplace where people can develop and provide plugins seamlessly. All plugins built by bitHolla are designed to plug seamlessly into the exchange solutions.

## HollaEx CLI

CLI (Command-Line Interface) is a command based tool, used to build, deploy and launch the exchange. CLI initializes an exchange with all settings and configurations, deployment setup using kubernetes helm charts and docker commands as well as the gateway nginx configuration. CLI contains all tools necessary for encoding/decoding and encrypting/decrypting system secrets and configuration. Video demo of the HollaEx CLI step-by-step process can be viewed here (*60 seconds*).



Demonstration of the deployment of the back-end exchange infrastructure through the 'hollaex run' command. More detailed step-by-step demo can be found on [youtube here](#).

HollaEx CLI is regarded as the main communication tool between the user and the core and takes care of all operations and configuration required for exchange operation. Below you can find an example of command for initializing HollaEx CLI:

```
hollaex init --name <NAME_OF_THE_EXCHANGE>
```

This command would initialize and create the required folders and files in your current directory including `settings`, `templates`, and empty folder for user-custom `plugins`.

User can easily maintain their own exchange's information on `settings` folder, such as exchange name or API endpoint URLs, able to see and modify generated templates on `templates` folder, such as `docker-compose.yaml`, based on their own requirements. For custom features specific to exchanges, custom plugins can be developed by the user agnostic to any programming language of user choice, and located in `plugins` folder. It would seamlessly be integrated with existing exchange system based on traffic routing coming from HTTP protocol to the gateway.

HollaEx CLI is built for different operating system and can be downloaded publicly. It can also be utilized and used as a docker image.

## HollaEx Web

HollaEx Web is a ReactJS web application works as a front-end user interface for the exchange clients. HollaEx Web uses ReactJS framework for view management along with Redux as a state manager of the client. All designs and UI elements are defined as SCSS files and compiled during application build and run-time. It uses `create-react-app` packaged and maintained by Facebook for development as well as optimized deployment setup. Communications with Core are done through REST API as well as websocket real-time streaming directly to the Gateway through SSL/TLS channels. Client supports full private websocket channels which can be used for real-time, user specific account updates such as orders being filled and incoming deposits etc. The Web contains two access control which is for user and administrators who can access the admin panel dashboard. Admin can setup different roles to administrate, monitor and manage the system. Admin Panel can support different access control and permissions for managing different access levels to the system.

HollaEx Admin has access to various system reports and allows fine grained reporting for overall system performance as well each user registered on the platform. Reports such as deposit/withdrawal list, list of users, logins and sessions as well as overall performance of the system with filtering are all available on the Admin Panel.

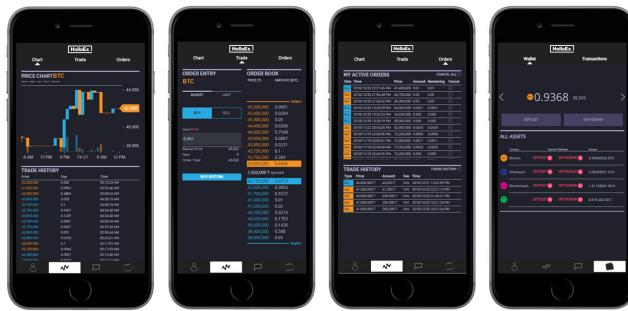
Admin can view and modify user data and it can also create roles with any predefined restrictions for accessing admin panel.

Additionally admin is capable of configuring the system. From trading fees to the coins that are available and their status, to customizing emails and messages can all be set on the admin panel.

HollaEx Web source code is made publicly available by bitHolla.

## HollaEx Mobile

HollaEx Mobile is the mobile app client version on HollaEx web built in React Native for both Android and iOS clients. HollaEx Mobile communication is all done through secure TLS channel with the server.



Authentication is done through tokens. These tokens are generated when user logs in and stored through `AsyncStorage`. On iOS, AsyncStorage is backed by native code that stores small values in a serialized dictionary and larger values in separate files. On Android, AsyncStorage will use either RocksDB or SQLite based on what is available.

## HEX Wallet

Shell has a built-in HEX Wallet that is used for managing HEX tokens and its operations. HEX Wallet supports all operations supported by HEX smart contract. These operations are activation, deactivation and standard token transfer. The wallet is embedded in the Shell and is automatically accessed by HollaEx Core.

HEX Wallet also can be used as a stand alone open source application which manages users HEX funds and operations for deposits withdrawals and all other features supported by the smart contract on the blockchain.

## Scaling

Each core worker can be replicated for horizontal scaling. More main workers result in scaling API endpoints. Additionally more stream workers help with the real-time data support to horizontally scale the system. Engine however is not capable of horizontal scaling due to the sequential nature of trading engines. Engine worker is a process that is required for each trading pair. As a result new trading pairs can be added without any downsides and the system only requires vertical scaling within the trading pair itself.

## Communication

Communications are divided into two different types of internal and external communications. All external communications are done through HTTPS and are passed through HollaEx Gateway. Internal communications are done through HollaEx CLI commands. Inside Core with API, Stream and Engine, the communications are managed by a BUS system that are managed using Redis PUB/SUB infrastructure.

## Data Storage

There are three main databases used primarily in HollaExShell:

- PostgreSQL: Persistent data such as user data, trade history etc
- Redis: Cached data and it is the Center of Communication BUS through
- InfluxDB: Real-time trade data and historic data processing and analysis.

## Coin & Digital Asset

Digital asset custody and coin management is regarded as the most sensitive area with any exchange. Due to the hacks and all the security flaws and issues which resulted in the loss of billions of dollars, we designed the system in a way that takes a special care of coin custody.

HollaEx Core is built in a flexible way that can manage different coins and list any digital asset. It can simply be configured to support any digital asset internally.

There are two wallet systems designed in the system: Internal and External. Internal wallet system refers to the user wallet and balance within the system which is designed as an internal ledger for internal purposes. This wallet is used

for all trades and internal transfer of assets. The external wallet refers to the custodial wallet which holds the actual crypto assets. Custodial wallet is out of the scope of HollaEx Core default coin management. Albeit, there are external custodial wallet management systems including bitHolla Vault or Bitgo which can be added as a plugin to the system. As a result the custody service is provided as a separated plugin that connects to a secure service environment that manages all the secure elements and private keys.

On a 100% backed system, internal and external wallet would have a 1 vs 1 ratio however this ratio would vary depending on the nature of the exchange and its operation as a fractional system.

## Trading Pairs

Unlimited number of trading pairs can be configured independently from each other. As explained in HollaEx Core, each trading pair is run on an Engine. These engines can be vertically scaled to manage higher traffic and better throughput on the trading engine. On a normal, retail level PC with 8 GB memory on quad core i5 cpu, according to bitHolla research benchmark, 100 trade activity per second can be managed on average. Trade activities are referred to adding and removing orders from orderbook as well as matching orders where trade occurs.

## Shared Liquidity

Exchanges can form a network in a mesh topography and communicate with each other in HEX liquidity pool at any time in order to share their liquidity. It is optional for the exchange operators to use this feature and allow others to re-market from the exchange while the exchange is also able to take the liquidity from other participants.

Exchange can opt in and opt out from the HEX liquidity pool at any time and by default are granted the default activation collateral HEX explained in the Token Model section of this paper. This functionality facilitates the communication between these participants and helps the growth of each exchange in the market.

HEX token is by default set on each exchange and all the share liquidity can be activated for exchanges that list the HEX trading pair.

# Security Design and Considerations

Security due to all the importance and sensitivity of exchanges and the financial aspect of it, plays an important role.

All external traffic to the system are done over TLS channels through the Gateway as a result all external communication channels are secured by TLS standards.

## Software Integrity

Exchange software integrity refers to the exchange doing what it is intended to do and preventing any malicious modifications into the system. The Core is provided in the form of executable binary with certain considerations to prevent external access to the code and changing the intention of the software. Any abnormal behavior is detected by the software and results in self lock of the system which would not allow any use of the exchange. All source code is obfuscated and significantly complex challenges are placed to prevent malicious access to the software. Additionally due to the term of service of HollaExShell any external malicious activity could result in legal action and consequences by bitHolla.

## Authentication

All private requests to the system are done through token authentication. There are two authentication mechanism used in this context:

- JSON Web Token (JWT)
- HMAC Signature

JWT is used in all private requests and validations on the system. It is attached in the header part of each request by the user sent over TLS. A request example is shown in the example below:

JWT is comprised of three sections, header, payload and signature. User information as well as token expiry is attached on the JWT payload. An example is:

```
{  
  "sub": {  
    "id": 1,  
    "email": "admin@bitholla.com"
```

```
},
"scopes": [
  "user"
],
"ip": "153.220.230.178",
"iss": "bitholla.com",
"expiry": 1552961148935,
"iat": 1552961148
}
```

User roles are specified within the scopes for access control. It's important to note that once the token expires, it cannot be used anymore and requires a new token.

For businesses and developers who seek to get a permanent token, the tokens have the scope specified as "**bot**" with no expiry date. Those tokens are stored in the database for validation.

It is also possible to apply IP enforcement to make sure that the IP user that sends the request matches with the IP that was initially used to create the token.

JWT is an efficient and fast mechanism for authentication, which improves the performance and scalability of the authentication within the system.

## HMAC Signature

HMAC signature is used for secure communication between third-party services. HMAC is a specific type of message authentication code (MAC) involving a cryptographic hash function and a secret cryptographic key. It may be used to simultaneously verify both the data integrity and authentication of a message, as with any MAC. The hashing algorithm we use is SHA256.

## Data validation

Open API, or Swagger, is used for managing all API requests and endpoint architecture. Open API has a full set of validations, from data type validation and required fields, which would prevent any sorts of unexpected input entering the system, such as SQL injection. As a result, we prevent all unwanted requests by filtering them through Swagger.

## OTP

In order to prevent keylogging, weak and stolen passwords, we use One time password based on its Time-based implementation (TOTP). Users can easily set that up using Google Authenticator and Authy and its mandatory for all sensitive actions, such as login and fund withdrawals.

TOTP is time-based and uses an initial seed created by the server to be scanned on the client's phone. Based on the initial seed and synced devices, client and server generate the same 6 digits code used for authentication.

## Email verification

In addition to OTP, for extra security, we also use email verification for highly sensitive actions such as withdrawal and account creation. The Email verification process means a user can only confirm an action by approving it through an email sent to them. Only then can a sensitive action, such as a withdrawal, be requested by the client through the link sent to the email.

Email verification/confirmation achieves the following:

1. Ensuring that the email address is typed correctly (used for newly registered individuals)
2. Ensuring the emails that are sent to this address can be read and received
3. Ensuring the email address really belongs to the person trying to perform said action
4. Preventing some automated bots from creating accounts
5. Allowing exchange operators to contact the user about topics on security and/or important site issues and announcements.
6. Preventing unwarranted withdrawals in cases where the account is left open. Should somebody access the user's exchange account while they are still logged in, the impersonating party will not be able to withdraw funds since they do not have access to the user's email account to confirm a requested withdrawal.

The process of requiring an email confirmation action in order to approve sensitive procedures, such as fund withdrawal, is a common best practice when using cryptocurrencies

## **Captcha**

In order to prevent brute force attacks for certain important functions such as logins and signups, the login api endpoint requires a captcha provided by Google recaptch. Using this mechanism, an attacker is not able to send unwanted random login requests to the Shell and prevents these sorts of attacks.

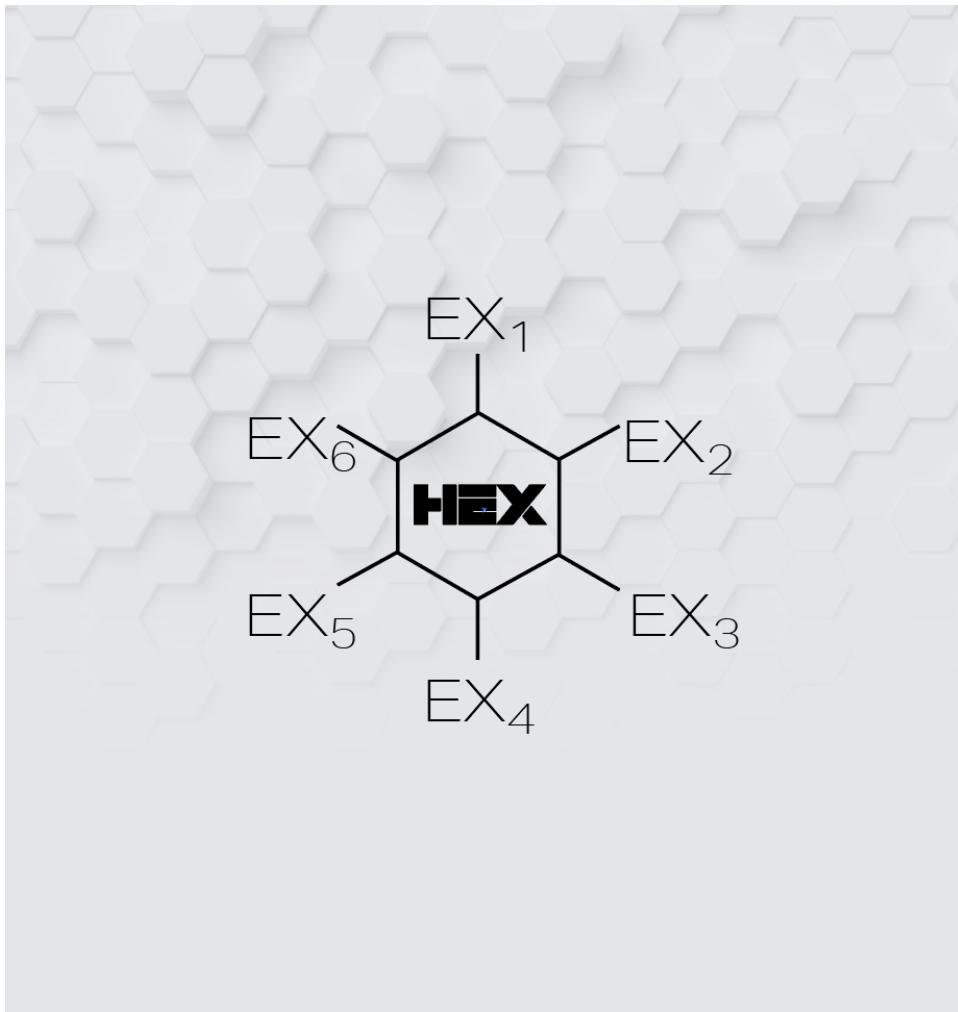
## **Insider attacks**

Insider attacks make up a significant portion of the hacks on cryptocurrency exchanges. Most attacks are exploited vulnerabilities from insiders who are ignorant or unaware of the security practices and policies in place. The system deployment and CICD through a strict policy would prevent these incidences from occurring. With the usage of HollaEx CLI, clients can easily create their own deployment pipelines and prevent rogue internal threats.

## **Updates and Maintenance**

HollaExShell is under constant research and development by bitHolla which would include future patches and updates. bitHolla according to the roadmap provided in this document has plans to continuously further improvements and upgrades to the system to the technology at the cutting edge in the trading ecosystem. Participants can expect patch updates and upgrades periodically.

## **Exchange Network**



HEX is an exchange network smart contract based on Ethereum's blockchain specification. HEX is the essence of each **HollaEx** exchange and is required as a digital fuel to launch and operate exchanges. It is used as Deposit within exchanges and allows participants to open exchange solution globally, share liquidity among the network, create credit lines and beyond.

HEX is the smallest unit of exchange and it supports up to 8 decimal points. It should be purchased before starting an exchange, deposited and locked to power the exchange upon its launch.



Distribution and the economic model of HEX is explained in details in the next chapter.

First of all lets answer these important questions to get a better understanding of HEX and the token model.

## **Why use a token?**

Token creates a fair economy and an open market for participants with transparency. As a front leader of open markets and exchanges, we believe in supply and demand as the best economic model. By tokenizing the product, we enable a market where people regardless of our involvement can freely trade and evaluate the product and its usage. Additionally it would give a fair opportunity to people to participate, use and contribute to the technology. This is a technology which may reshape the exchange and economic model and pricing the product as such. With all that said, our response would be why not use a token?

## **Why blockchain?**

A blockchain creates an automated and autonomous environment which would streamline some of the process without anyone's direct involvement and would create a fair and transparent environment for all participants. It sets the expectations clear which would result in transparent and clear process and achievements for all participants. We are aware of the high cost of running a blockchain and its inefficient data storage model for Bitcoin, Ethereum and other technologies. However for very minimal throughput that is required from the blockchain in HEX Network, HEX model fits very well on top of the existing solid blockchains such as Ethereum. HEX Network, uses smart contracts on Ethereum which would guarantee certain attributes in the system. First, it defines the number of tokens and the cap which prevents anyone from creating more tokens on the system. Secondly, all exchange operations for activation, deactivation and HEX transfers are done through the smart contracts. Lastly, it enables numerous functionalities in the distributed exchange network among participants such as opening credit lines, sharing liquidity and investment opportunities for new exchanges in a seamless manner.

## **Why the Ethereum blockchain?**

HEX Network requires a blockchain infrastructure with following considerations:

- Network stability

- Network security (Hash rate and consensus process)
- Global support (accessibility and its global network support)

Ethereum fulfills the requirements and provides the best platform for this cause.

## Launching Exchange

Launching an exchange and adding it to HEX Network is quite straight forward. Exchange operator is required to follow these steps:

- Download HollaEx CLI
- Initialize exchange through CLI
- Create a wallet
- Deposit the required amount in the wallet as a deposit.
- Activating HEX on the smart contract to lock your deposit. (The deposit can be unlocked by deactivating an exchange after 6 months from activation)
- Configuring the exchange settings
- Launching the exchange with CLI

Your exchange is then up and running and it automatically is added in the HEX Network.

## Activation

Activation of an exchange is a process in which the exchange operator locks the Deposit in HEX smart contract which would activate the HollaEx Shell software to run automatically. The Deposit amount is set based on the number of exchanges in the network and goes down as more exchanges participate in the network.

## Exchange Deposit

Exchange Deposit starts from 1,000,000 HEX for the first exchange activation and follows a geometric sequence with ration 0.99 which means that the cost goes down by 1% after every exchange going live.



The exchange cost will not reach below 1 HEX and that cost would be set as the minimum cost.

$$10^6 \cdot (0.99^{x-1})$$

### Exchange Deposit Amount Table

No Exchange	Cost (HEX)
1	1000000
2	990000
5	960596
10	913517
100	369729
1,000	44
10,000	1
100,000	1

The sum of exchange Deposit is calculated in eq1 as follows:

$$\sum_{i=1}^{i=n} 10^6 \times (0.99^n) = 10^6 \times \left( \frac{1 - (0.99)^n}{1 - 0.99} \right)$$

For the case when we have 1000 exchanges we would have almost 100m HEX locked.

$$10^6 \times \left( \frac{1 - (0.99)^{1000}}{1 - 0.99} \right) = 99,995,682 \simeq 100,000,000$$

The exact equation eq2 for calculating Deposit amount for any new exchange given numbered as  $x$ th exchange assuming  $\Omega$  is the total number of currently locked exchanges is as follows:

$$10^6 \cdot (0.99^{x-1}) + \frac{\left( \sum_{i=1}^{i=x} 10^6 (0.99^x) \right) - \Omega}{x}$$

The total number of tokens are set at 200,000,000 HEX which is a fixed amount and fixed permanently.

These HEX tokens are required for exchange activation and operation. The Deposit amount in HEX is required to be locked in order to run an exchange. The HEX tokens in the wallet can have 2 different modes:

- Default: The normal mode for the tokens. The tokens can be transferred and traded in default mode.
- Locked: Locked within an exchange. It is required for exchange activation and is used as collateral deposit to power the exchange.

## Deactivation

Any activated exchange can be deactivated at anytime by the exchange operator through sending the message along with the signature to the HEX Network smart contract. However it would only be approved by the network and unlocks the tokens if and only if the period passed from activation is more than 6 months. This feature prevents people from quickly activating and deactivating exchanges and pretending that they are running an exchange in order to manipulate and reduce the Deposit for running an exchange.

Once an exchange is deactivated, it stops functioning and can no longer be used by the operator. It would also affect the Deposit cost to increase according to eq2.

## Launch

Once an exchange is activated, it needs to be initialized and launched. The initialization process requires configurations and certain settings for the exchange the operator needs to set depending on his exchange through HollaEx CLI. The exchange initially checks the blockchain for its status upon initialization during the launch process.

## Destruction

Exchange can be destructed in one of these events:

- Manually deactivation of the exchange.

- Internal malicious activity detection. This could trigger if anyone tries to break into the Core and manipulate the network environment.

HEX smart contract supports the functions below:

```
// Used for activating an exchange which would result in the lock of the amount
activate(amount)

// Used for deactivating an exchange which would result in unlocking the amount
deactivate()

// HEX token transfer
transfer(address, amount)
```

*All other ERC20 specifications are supported in HEX specification.*

The functions are all supported through HollaEx CLI using the HEX built in Wallet. The communication is done with HEX DAPP on Ethereum's blockchain.

Once an exchange is activated it joins HEX Network as a node. HEX exchanges create an interconnected network of exchanges checking for each others availability and liquidity sharing. Since exchange is an online business and requires to be open on internet for its clients to use, HEX network uses internet as a relay network for communication between the nodes. Each node is referred to an exchange and corresponds with other nodes through TCP/IP http requests. Exchanges ping each other to check for their status regularly. This network is used to build reputation and credit score in the system. Its used as one of the factors for lending across exchanges and sharing liquidity.



This is an initial design of the smart contract and there might be additional function and feature to support new features in the network such as exchange group activation, time locked liquidity sharing etc.

## Token Model

HEX is a smart contract token based on Ethereum's blockchain as explained in the previous chapter. These token fuels are used by exchange operators to run exchanges. Since HEX Deposit for each exchange is locked, it is also used as an

exchange default liquidity among exchanges as well as a measure for an exchange reputation in the network. In this chapter we explore HEX token model and how it functions based on its use cases for different actors.

## Participants

HEX economy has 3 main actors:

- Exchange Operators
- Investors
- bitHolla

It is important that all participants in the system are incentivized and as such we are required to go through all participants and their incentive model in the system.

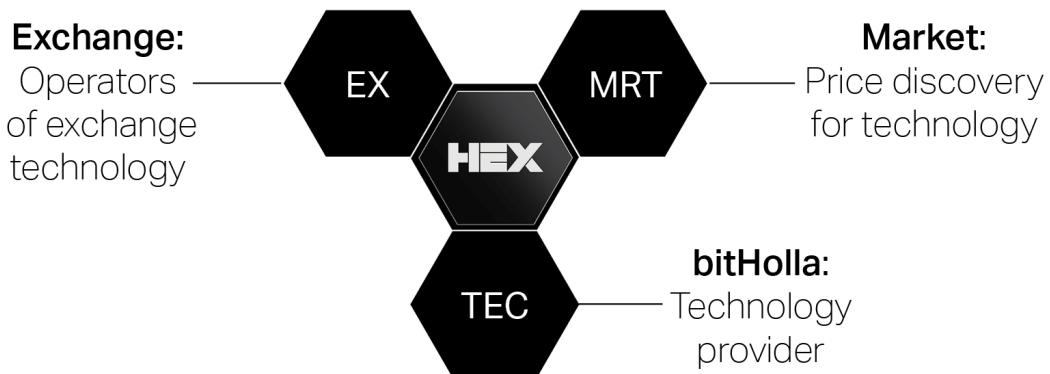
HEX economy is quite lucrative for exchange operators since it reduces the entry barrier and risk of starting the lucrative business model of running an exchange. The only requirement for Participants is the Deposit which upon deactivation can be sold in the market. This means an exchange operator does not have to pay anything to run an exchange in this model other than a deposit. This would help businesses to test out and run the exchange prototypes in an affordable manner.

Investors whom believe and understand the technology can participate over the finite scarce HEX tokens that represent the limitless exchange economy and contribute to the democratization of our trades and exchanges powered by HEX. Investors can expect the economy to grow as more exchange operators participate infinitely which would result in the increase of HEX token price. It is expected to increase on the assumption that as more exchange operators come online they be required to lock up HEX and in effect taking out supply and thus increasing scarcity of the HEX token. As the growth of the network increases so too should the price of the HEX token.

BitHolla as the technology service provider benefits from the freely traded HEX open market through the large participation and exploration of the usefulness our BitHolla's exchange software and its potential globally. The exchanges software have significant potential, and besides crypto have not been fully explored in other industries not related to crypto. As a result BitHolla believes that it may

open up brand new opportunities in other sector that can create their own new and exotic market places with an affordable and open exchange software.

Throughout this setup, BitHolla benefits from its token market share as well as continuous fees and value added services and plugins.

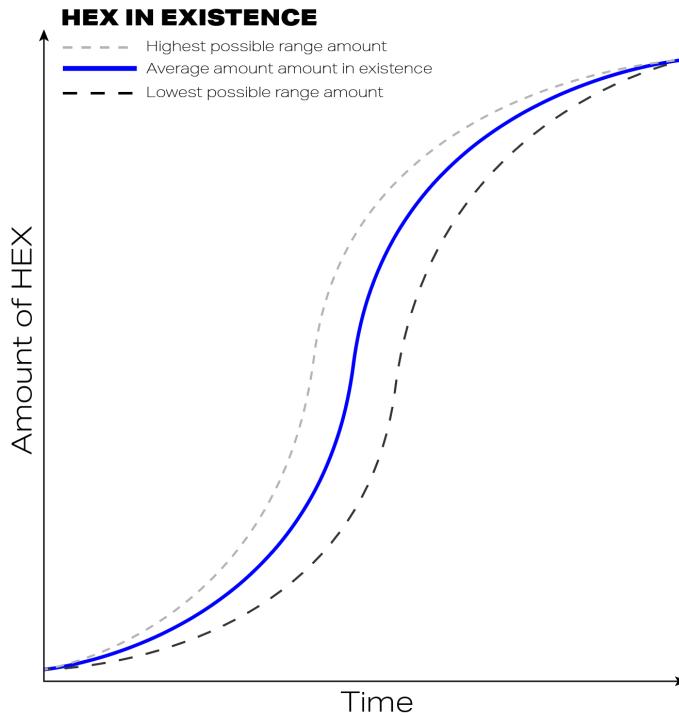


**HEX Economical Triangle:** HEX acts as a bonding agent between all parties while being utilized as fuel that efficiently powers the exchange network.

## Distribution

Total maximum cap of the HEX tokens are 200,000,000. These tokens are distributed initially through a private sale for early investors and exchange operators (including current bitHolla exchange clients), followed by a public sale in an innovative process which is patent pending known as a **Wave Auction**.

### The Wave Auction — Public HEX Sale



The wave auction is designed to give enough time for investors and exchange operators time to evaluate HEX and the exchange technology. In the middle of the timeline will be the peak distribution. Some randomness taken from Ethereum blockchain is added to the amounts distributed within a range to reward early obtainers of HEX whom take the initiative.

Public Sale commences on [hex.bitholla.com](http://hex.bitholla.com) with innovative distribution model called a Wave Auction.

The Wave Auction is a creative model for token distribution in which HEX tokens are distributed daily through distribution waves that occur automatically and are purchased and obtained by the top bidders. Buyers must place limit buy orders on the HEX orderbook every day and upon random times in a day a wave of HEX tokens with a random amount sold to the top bidders.

For the Wave auction a floor price is set initially at \$0.2, and that is the initial public sale price. Strictly in the wave auction, the price can not drop below the floor, meaning bidders can not place bids below the stated floor.

The wave is a market sell with one condition that if the whole wave is not purchased by the bidders from the orderbook and the market sell order reaches the floor price, the leftover amount is burnt from the wave.

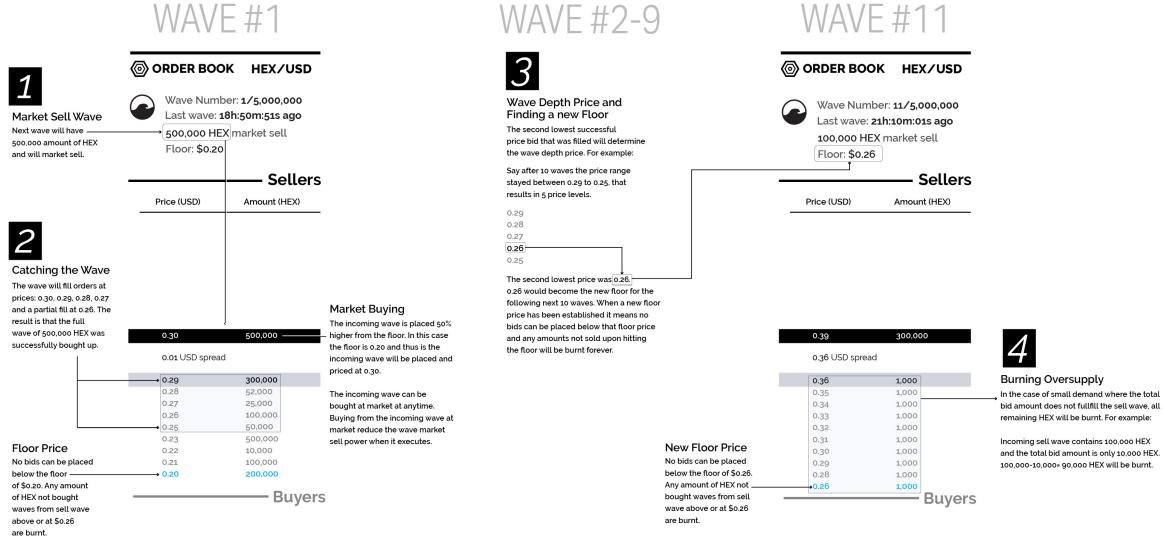
The floor price is recalculated after 10 waves and will be set to the second lowest price. Therefore it could either be set equal to the current floor or goes up conservatively.

With the sorted set of depth prices of the last 10 waves represented below, Floor  $F$  is calculated in eq3 as follows:

$$prices = \{p_1, p_2, p_3, \dots, p_{10}\}$$

$$F = p_2$$

# Wave Auction Example



## Distribution Amount

Waves distribution follows S curve distribution model and distributes 100,000,000 HEX within almost 500 days from the initial public sale. The distribution amount follows Gaussian curve as follows:

$$\frac{10^8}{\alpha\sqrt{2\pi}} e^{-\frac{1}{2}(\frac{x-\mu}{\alpha})^2}$$

Where  $\mu$  is median which is 250 meaning on the 250th day will have the highest amount of tokens distributed.

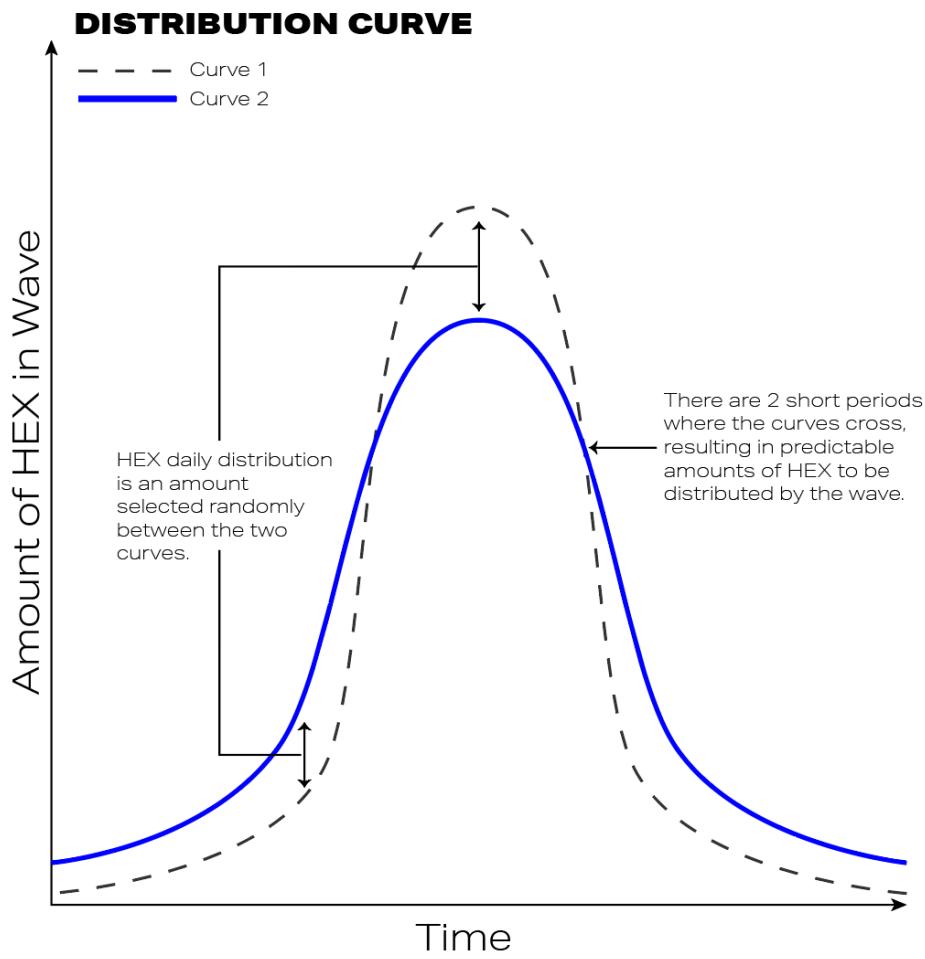
Where  $\alpha$  is the standard deviation in the bell curve equal to 70 for the first curve and 80 in the second curve. This would create two curves in which the daily random amount to be distributed is selected between the two curves randomly.

Curve 1 (eq4) is:

$$\frac{10^8}{70\sqrt{2\pi}} e^{-\frac{1}{2}(\frac{x-250}{70})^2}$$

Curve 2 (eq5) is::

$$\frac{10^8}{80\sqrt{2\pi}} e^{-\frac{1}{2}(\frac{x-250}{80})^2}$$



The graph illustrates the possible variance in the amount of HEX distributed over time. There are times of extreme variance in the middle and periods of predictability on amount of HEX distributed in the wave per day.

This table illustrates the number of HEX distributed every day based on the two curves.

Day	Curve 1	Curve 2
<u>1 (first day)</u>	1019	3928
<u>10</u>	1597	5540
<u>30 (one month)</u>	4083	11367
<u>60</u>	14322	29715

Day	Curve 1	Curve 2
<u>90</u>	41815	67489
<u>120</u>	101596	133173
<u>180 (6 months)</u>	345672	340069
<u>250</u>	569918	498678
<u>300</u>	441593	410201
<u>365</u>	147820	177462
<u>400</u>	57372	85982
<u>500 (last day).</u>	968	3777



The actual number of HEX distributed everyday is a random number between the two curves. It is impossible to know the numbers since they are selected randomly prior to the wave.

As it can be seen initially for the first and last 2 month and the last month the waves are a tides with small amounts to be distributed.

Tides are followed by normal waves and eventually by 9 months for 3 month it generates bigger waves known as Tsunamis. This follows the adoption curve and assumes the market reaches maturity as tokens are distributed.

## Wave Time

Waves initiate randomly by taking Ethereum's blockchain hash as a random element required for the random trigger of the wave. The specification of it is as follows:

Assuming Ethereum blocks are generated every 13 seconds on average, we would have in eq6:

$$n = \frac{60 \times 60 \times 24}{13} \simeq 6646$$

Each newly created block generates a random number  $R$ . We then calculate eq7:

$$hit = R \mod n$$

Once `hit` is equal to `0` the wave automatically starts.

The probability `P` of such event is calculated in eq8 as follows:

$$P(n) = \frac{1}{n} \simeq 0.000150466$$

With the assumption that Ethereum's blockchain has a block generation rate of 13 seconds per block we have our probability distribution as a binomial probability distribution while the mean and standard deviation of our probability distribution for 24hours hit event specified in our target are as follows:

$$\mu_x = n \times P = 1$$

$$\sigma_x = \sqrt{n \times P \times (1 - P)}$$

We can simply calculate binomial distribution of a wave hit based on the number of hits `x` in eq9 as follows:

$$b(x; n, P) = \binom{n}{x} \times P^x \times (1 - P)^{n-x}$$

The cumulative binomial distribution of one wave happening within 24 hours is calculated in eq10 as follows:

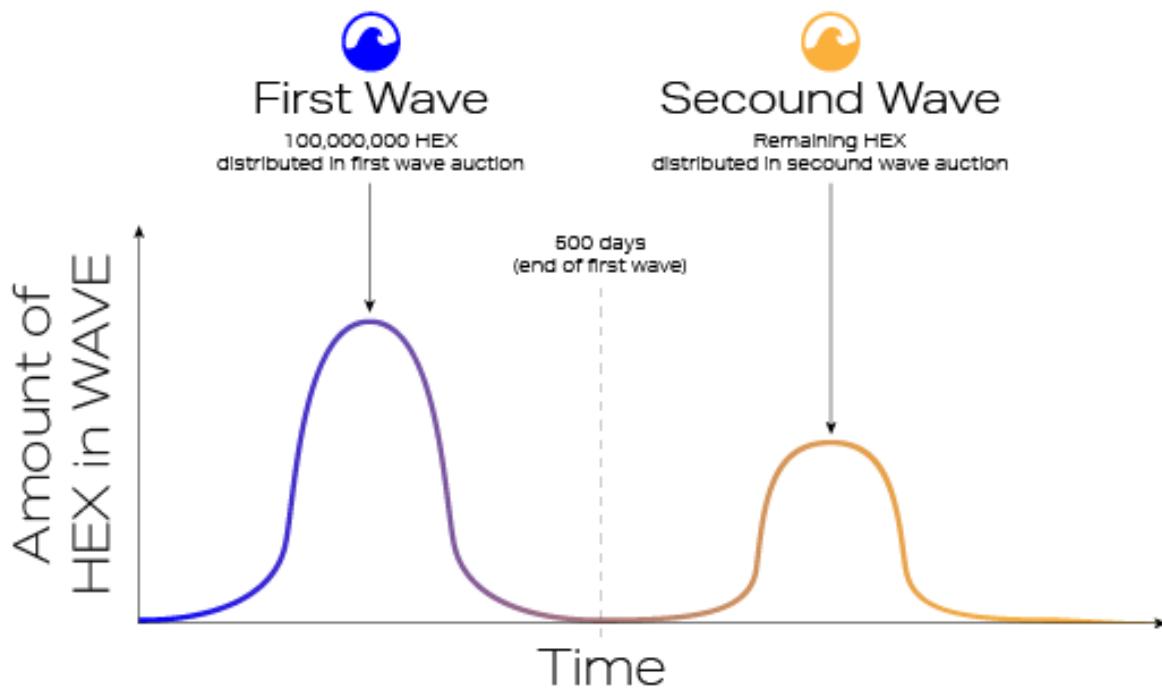
$$b(x \geq n, P) = \sum_{x=1}^n \binom{n}{x} \times P^x \times (1 - P)^{n-x}$$

This would result in the probability of roughly `63` percent to find a block within a day. The distribution graph below indicates the cumulative binomial distribution:

In part, the wave auction is designed to create healthy early market anticipation and awareness of the wave, and rewards individuals that pay close attention to wave activity. HEX Foundation will provide some early automated notification on incoming tidal waves (waves with large amounts of HEX) and historical wave data

such as last wave depth (amount) and intervals and averages will be built to help guide and reward talented market analyzers.

According to the Wave Auction the total amount of 100,000,000 HEX are distributed in 500 days. This is followed by the second auction where the remaining 50,000,000 HEX is sold similarly. The distribution is illustrated in the diagram below:



The Second Wave Auction (orange) will distribute half of the amount of HEX compared to the First Wave Auction (blue) depending on how much HEX was sold in the private sale.

Second wave curve 1 (eq11) is:

$$\frac{\frac{1}{2}10^8}{70\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{x-250}{70}\right)^2}$$

Second wave curve 2 (eq12) is:

$$\frac{\frac{1}{2}10^8}{80\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{x-250}{80}\right)^2}$$

# Future Considerations

## Hardware Exchange

In order to protect and safeguard the exchanges, research and development in hardware needs to be done. bitHolla as an IBM partner will allocate certain resources towards hardware exchange solution. HollaExShell could then be placed inside a hardware which then runs a trusted secure environment with HSM for additional built in security. This would not only increase the security but it would also provide optimized Shell system for specific hardware design which would increase the performance and efficiency of an exchange.

## DEX

BitHolla has done extensive research into the development of DEX and are looking forward to future technologies and their development where we can process transactions through DEX using HEX token model. The Decentralized Exchange model, in their current form are not efficient and practical models today. While the current HEX distributed exchange network model is the more practical solution, we constantly work on improvements in R&D towards improving the technology.

## Lending and Derivatives

Another area of interest in future research and development is lending market and support of future contracts and more complex derivative products on the exchange. Derivative products such as future contracts, options, forwards etc work the same way with the matching engine. However they require certain risk calculator for managing user's risk and their collateral which is in the roadmap and are a consideration for bitHolla's future development.

## Roadmap

# HEX ROADMAP

## Origin

The bitHolla company first created the HollaEx white-label exchange software to contribute to the trading and adoption of cryptocurrencies.

## HollaEx®

Q4 2017 v 0.1.0 Testnet release

2017

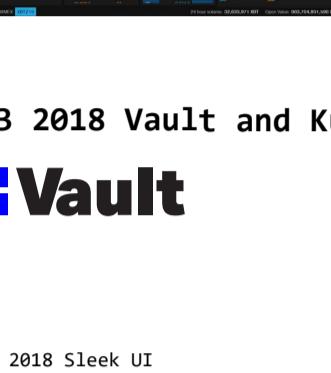
## Automation

Development of automated and smart deployment of HollaEx, Vault and bots.

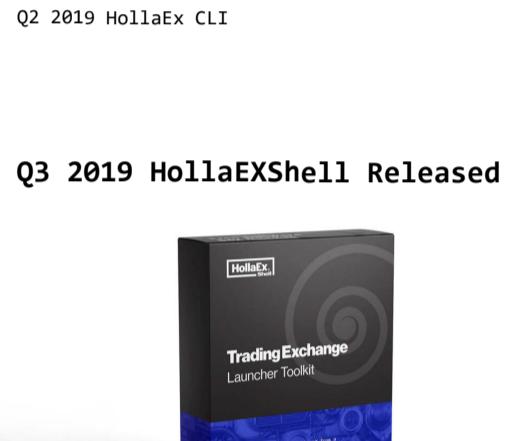
Q1 2018 v1 Production release

2018

## Q2 2018 HollaEx cloud packages



## Q2 2018 XRayTrade pro Terminal and UI



## Q3 2018 Vault and Kubernetes deployment

## Vault

Q4 2018 Sleek UI

2019

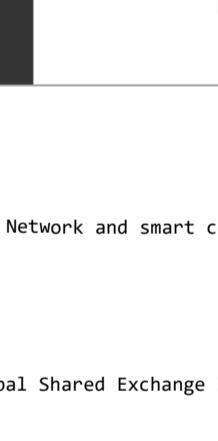
## Digital Fuel

Formulations of the power source for bitHolla trading products with HEX fuel.

Q1 2019 Package and modularization

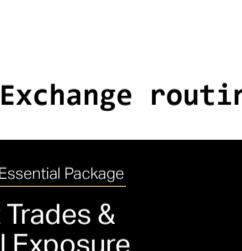
Q2 2019 HollaEx CLI

## Q3 2019 HollaEXShell Released



Q4 2019: Mobile App

Q4 2019 HEX Token Distribution



2020

## Exchange Connection

Connecting all exchanges using the XRayTrade platform and provide and increase trading activity and product exposure.

Q1 2020 HEX Official Launch

## Q1 2020: Admin 2.0 dashboard



Q1 2020: HEX Network and smart contract - Launch of the community Exchange

Q2 2020: Global Shared Exchange Investment (Exchange DAO)

Q2 2020 Plugin marketplace

## Q3 2020 Robolla shared liquidity



Q4 2020 Exchange routing and listing with XRayTrade



## Q4 2020: HollaExShell 2.0



2021

## Continuous Upgrades

Continues upgrades of the bitHolla products range

and a move towards autonomization.

Q1 2021 +1000 active exchange

Q1 2021: HEX Network trustless lending and credit system

## Q2 2022: HEXA (HEX Autonomous) Autonomous Exchange without operator.



## **Conclusion**

HEX is an open exchange economy, empowering the future of open and online marketplaces. It is used as a type of digital fuel which allows exchange operators to freely run and operate exchange systems.

The technology is already built and is in production globally and we seek to expand and open up the technology to the world through the HEX Network and model. It helps increasing the transparency, accessibility and the global penetration of one of the most innovative creation o humanity, exchanges.

HEX forms an exchange network where participants can share and re-route their liquidity and credit lines and investors have the opportunity to boost launching new exchanges and create new venues for trading globally.

HEX is distributed in the most transparent way following market adoption curve pattern and is distributed through Wave Auction on [hex.bitholla.com](http://hex.bitholla.com) where investors and exchange operators can participate to purchase these tokens.

If you would like to participate and contribute to the future of free and open markets, this is the opportunity.

***"Creating opportunity via open marketplaces"***

A handwritten signature in black ink that reads "bitHolla". The "b" and "H" are connected, and "Holla" is written in a cursive script.