Overview on Herdius

This document is a condensed version of the Herdius whitepaper. Let's get down to the nitty gritty of the core Herdius features, and then zoom out into hands-on use cases of the Herdius protocol.
The HER token usage and cryptoeconomics are described in another paper titled Herdius Tokenomics, however, this document is vital to the understanding of it. A good resource for further reading is our Medium - https://medium.com/herdius , please check it out if you are interested with taking a closer look at the following article: https://medium.com/herdius/what-is-herdius-3831a47cfb6 .

Herdius can be viewed as Layer-2 blockchain. It involves 3 core products: 1) a key management / identity solution specifically aimed at solving chain interoperability, 2) a decentralized exchange, 3) a more scalable blockchain. All of these three are in some way interconnected and form the single product that is Herdius. There are three different main value propositions, here they are and how we tackle them:

- For users we want to make it so that any dApp or service can be used through making a single transaction inside the Herdius chain. If you have Litecoin in your wallet and you want to use a prediction platform on NEO, we make it so that you can do the swap inside our DEX for that token, and send that token to another Herdius address thereby circumventing a lot of operations on other chains.

- For dApp developers, regardless of what platform they are running their app on, we want to make it so that all they need to do in order make their app accessible by the user base of Herdius is to open a single Herdius address. This address they would need to tie to their backend or main smart contract and from that point onward any Herdius address can send funds to that address and use the dApp just like a user of the native chain that app is running on.

- Exchanges can use our distributed virtual wallet network for their hot wallets. This way we can create a truly global liquidity pool. There is no technical overhead for exchanges as they can seamlessly match orders within their exchange with orders on Herdius. Other DEXs can also open a Herdius account and thereby gain access to the liquidity we have.

Current problem:

A common property of blockchains is the private / public keypair from which the private key a user has is the gateway to all data, assets stored on that particular private key's public counterpart. Lots of other platforms Aion, Polkadot, ICON, etc. use their own chains to store transactions and data and when going back to the main chain they have to utilize communication channels and or bridges. Problem is that each of these have to be set up separately and thereby are not a scalable and future resistant.

1) Key management, identity, interoperability:

Herdius interconnects blockchains on the private key level, that means it can securely generate a private / public key in a distributed way for any blockchain. This is possible through a combination of using hierarchical deterministic wallets (HD wallets), homomorphic encryption and Merkle trees. The private key that is generated is encrypted using a threshold scheme (BLS) and the different keys of that threshold are stored with individual nodes in the network. All you need is a single Herdius address, and all of the subsequent public and private addresses on any blockchain that you want to create an address on are automatically tied to this single address.

For the user there is no user experience overhead as once you would like to create an address on blockchain X, the respective key pair is generated in a distributed and decentralized way.

Example: Alice and Bob have a wallet that is compatible with the Herdius network (the wallet code will be open sourced and it is very easy to already existing wallet providers to adopt). Alice and Bob both have a Herdius public and private key, they use the private key to sign transactions / messages to both Herdius and non-Herdius users. The Herdius public key is used to receive payments in any currency inside the Herdius network.

Now Alice decides to open an Ethereum address while Bob decides to open a NEO address. The private key for both of those addresses is generated in a safe and distributed way through the participation of Herdius nodes. Neither Alice or Bob sees the private key that is being generated, however, in the backend though both of their Herdius keys have gained the “right” to reassemble that particular private key - works very similar to UTXOs in Bitcoin. Alice and Bob decide to swap their respective ETH and NEO on the Herdius DEX which happens in under 3s. After 3s they already have the respective tokens in their Herdius address, if they were to move the tokens to another address no private key is reassembled. On the other hand, if Alice wants to send her acquired NEO to a non-Herdius user, she just has to sign with her Herdius key and the funds are moved from Bob’s wallet.

Another example: Alice deposits 10 ETH to her Herdius address and proceed to send 0.1 ETH to 100 different Herdius users, she signs the transactions with her Herdius private key. If someone is to look at Etherscan at the original Ethereum address, no funds were moved. If, now 50 of those other users move the funds back to Ethereum that is when Alice’s private key is reassembled.

Advantages:

- Since we preserve the native key format of whatever chain we go back to, we do not need parachains, hybrid nodes, bridges, or communication channels. All we need to know is the curve parameters of chains to generate a key

- Also works with hardware wallets

- Above a simple swap / transaction was presented, but since keys are access to data and messages, that can come into play too

- It is blockchain agnostic and works & scales without us as a dev team having to lift a finger in the future.

- Anything that uses asymmetric keys for authentication can be hooked up to our distributed key generation. Form fingerprint sensors on phones to IOT devices. We can assign and generate any of these devices a wallet on any blockchain.

2) The Herdius DEX:

The Herdius DEX is built on top of the above architecture and it is blockchain as well as asset agnostic. That means any asset on Ethereum and future chains can be traded on it, including security tokens. It is truly decentralized in the sense that the Herdius team has no control over which asset is listed on the DEX, the masternodes do.

Our DEX offers under 3s order finality with lower fees than a regular DEX on Ethereum and a way better user experience since users trade from their wallet - imagine Shapeshift in a decentralized fashion from your wallet.

3) Scalability and new consensus mechanism

In current blockchain designs newly created blocks follow each other linearly which results in a capped transaction throughput. The Herdius chain is capable of "stretching" itself vertically through placing blocks on top each other, blocks-on-blocks (BoB), by having each of the blocks verified / mined by different subgroups of verifiers we can achieve parallel mining. Herdius Flow is our consensus algorithm to achieve such scalability. It makes use of averaged and weighted graphs / coordinates and AVL trees to make it possible for Herdius to easily scale to tens of thousands of transactions per second.

Presentation on our consensus mechanism can be found here:
https://www.slideshare.net/secret/aOQu4mddUtHZF6

Essentially we can create a byzantine fault tolerant system in which the masternodes who keep track of transactions do not need to communicate with one another which thereby reduces bandwidth overhead and transaction times. The only limitation to how much Herdius can scale is the number of validators at any given time.

Products of Herdius & vision for the future:

1) Decentralized exchange: The advantage of our DEX is that it is blockchain agnostic meaning that any issues, regardless of which chain it is issued on can be traded on the DEX seamlessly. Not only can other decentralized exchanges provide / share liquidity with our orderbook, but also other centralized exchanges can make their hot wallets compatible with the Herdius network and in the process match orders seamlessly with our chain.
2) The future will be many different chains converging to a single use case or use cases. Ecosystems will be even more split than currently. Herdius would act as an identity layer or highway to connect these split ecosystem. It would make it possible for a user of chain A to use applications in any other chains.
3) Single identity: Essentially what Herdius does is it gives the user a single Herdius keypair (public & private) with all identities on the other chains being derived from this key. If we were to KYC the Herdius address then it becomes possible to utilize a universal identity across chains. This would be an opt-in option to preserve the decentralized nature of the DEX, but at the same time it would introduce fiat to the system, making it tradeable against any asset on our DEX.
4) Custodian wallets: We can create a wallet architecture that solves the custody problem for bigger institutionals moving into the space. Since we have the private key sliced up in our system with different nodes, these nodes can provide insurance in exchange for securing the key. (This is a very early and exploratory discussion)