DragonX

Whitepaper v1.0

Dan S

January 7, 2024

Abstract

DragonX is a cryptocurrency with extreme privacy features with influence from projects like Monero and Zcash. Its roots can be traced directly back to **Bitcoin**[1] and continues the original goal of a peer-to-peer electronic cash system. With a custom implementation of the official **RandomX**[2] proof of work algorithm, DragonX is meant to be mined from regular computers rather than machines that have no other uses. It has privacy features at every layer of the system that very few other blockchains have.

Contents

1. Introduction

DragonX is the first zk-SNARKs cryptocurrency with a RandomX proof of work algorithm as well as Hush's first "Hush Arrakis Chain". Its emission schedule is exactly the same as Bitcoin, albeit with faster blocktimes. The Genesis block was mined on November 5th, 2022.

DragonX was announced one month in advance with no pre-mine, fast-mine, founder's reward, or any other gimmick. The main goal of DragonX is to showcase the power of **Hush Arrakis Chains**[4] and help contribute to the development of **Hush**[3].

Chain Specification

Algorithm	RandomX
Blocktime	36 seconds
Block Reward	3 DRGX
Reward Halving	Every 3.5M Blocks (4 Years)
Total Supply	21,000,000 DRGX
Premine	0 DRGX
P2P Port	21768
RPC Port	21769
Blocksize	4MB

2. Hush Arrakis Chains

A Hush Arrakis Chain allows someone to easily launch a coin in a similar way to Side-Chains on Ethereum with a single command (or none if a service provider is used) with full control over the chain parameters while staying completely independent of the Hush blockchain. Arrakis chains can be quickly and easily launched for a variety of use cases, whether it's between two individuals wanting secure communication, small events, or communities that want a secure and private form of currency.

One of the most notable features in Arrakis chains is the choice of Proof of Work algorithm. Currently users have a choice between Equihash or RandomX. These choices can be helpful in building a chain that is more accessible to the target audience. For instance, a blockchain with the intent to be used primarily on mobile would benefit from RandomX, allowing users to efficiently run a full node from a low power device such as a smartphone.

Hush uses a version of the official RandomX implementation that has been customised so that should an ASIC be developed for another RandomX coin such as Monero, it will be incompatible with DragonX's implementation of RandomX.

3. Privacy

As an Arrakis Chain, DragonX utilises all of the extreme privacy technology implemented in the Hush blockchain.

Privacy by default:
All regular transactions have the full privacy of **z2z**[5] transactions, meaning only shielded addresses called **z-addresses**[5] can be used as senders and receivers in a transaction. A z address hides the sender and recipient addresses as well as the amount being sent, and hence give drastically more on-chain privacy than transparent addresses.

zk-SNARKSs:
Because DragonX has the Zcash protocol embedded inside, it uses **zk-SNARKs**[6] AKA, *Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge. This "Zero Knowledge" functionality allows a transaction to be verified without revealing any information about the transaction itself other than the fact that it is a valid transaction.*

Encrypted peer-to-peer networking:
Connections between DragonX nodes are encrypted with **TLS**[7] 1.3, a protocol designed for private communication over the internet. It is used for securing different services such as websites, voice calls, emails, and messaging. It's important that connections between nodes are encrypted so as to reveal as little information about each node and their interactions between other nodes as possible. In a transparent chain such as Bitcoin, this information can easily be used to link transactions to ip addresses. Most other coins do not implement this.

Sietch:
Sietch[8] is another layer of security implemented over the Zcash Protocol. It prevents metadata leakage of how many recipients a transaction has by hiding that information. With Sietch, DragonX and any other Arrakis Chain have increased protection against linkability analysis, metadata leakage from normal blockchain operations, total increased privacy of all funds, and a drastically increased difficulty in blockchain analysis.

4. Accessibility

Full Node Wallet:
DragonX is a build option in the full node GUI wallet called **SilentDragon**[9] (SilentDragonX when built for DragonX). The SilentDragonX wallet has all the functionality of the original but with an added "1 click" mining button. This allows less technically inclined users to easily start mining without the barrier

of learning to use a command line as well as slightly decrease the power of mining pools.

Light Wallet:

The light wallet, **SilentDragonLite**[10] is currently in progress of being implemented for DragonX by the Hush team. Along with faster syncing, this will allow users the option to easily access the [HushChat] feature. Making it much easier to send messages.

HushChat:

HushChat[11] is essentially a decentralised **signal protocol**[12] which does not require any centralised servers and uses Zaddrs instead of phone numbers.
It is compatible with any Zcash protocol chain, which means any Arrakis Chain can use their own version of Hush Chat. In DragonX's case, "FireChat".

Despite being a messenger built atop a blockchain, Hush Chat will have the capability for "instant" messaging by reading transactions in the mempool before they are confirmed.

Android Wallet:

The android wallet is a fork of the hush android wallet which is based on the Zcash android SDK. It was implemented by the Hush team.

5. References

1 Bitcoin Whitepaper. https://bitcoin.org/bitcoin.pdf (visited on 2024-01-06) (↑p1).

2 RandomX design. https://github.com/tevador/RandomX/blob/master/doc/design.md (visited on 2024-01-04) (↑p1).

3 Hush Is Privacy. hush.is/privacy (visited on 2024-01-06) (↑p1).
Hush Whitepaper. https://git.hush.is/hush/hush-v3-whitepaper/src/branch/master/hush-v3.pdf (visited on 2024-01-06) (↑p1).

4 Hush Arrakis Chains - The z2z Platform. https://git.hush.is/hush/hush-arrakis-chains (visited on 2024-01-04) (↑p2-3).
Hush Arrakis Chain Creator. hush.is/hac-creator

5 ZADDR. https://git.hush.is/hush/terminology (visited on 2024-01-05) (↑p3).

6 WHAT ARE ZK-SNARKS?. https://z.cash/learn/what-are-zk-snarks/ (visited on 2024-01-01) (↑p3).

7 What is TLS (Transport Layer Security)? https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/ (visited on 2024-01-06) (↑p3).

P2P https://git.hush.is/hush/hush3/src/branch/dev/doc/overview.md#p2p (visited on 2024-01-64) (↑p3).

8 What is Sietch?. https://git.hush.is/hush/sietch (visited on 2024-01-01) (↑p3).

9 SilentDragon. https://git.hush.is/hush/SilentDragon (visited on 2024-01-01) (↑p3).

10 SilentDragonLite. https://git.hush.is/hush/SilentDragonLite (visited on 2024-01-01) (↑p3).

11 HushChat - Signal-like Protocol on Hush. https://git.hush.is/hush/hushchat (visited on 2024-01-01) (↑p4).

12 Hacker Lexicon: What Is the Signal Encryption Protocol? https://www.wired.com/story/signal-encryption-protocol-hacker-lexicon/ (visited on 2024-01-05) (↑p4).

Remember Remember the 5th November for freedom of speech is not free!!