DEXHUNE

A GOLD PEGGED DX TOKEN ON AVALANCHE C-CHAIN

BY
ELIX EXO

Abstract

The following document briefly analyzes the design of existing stablecoins and proposes a new way to create price pegged assets. This system is called "Dexhune", and aims to bridge the divide between blockchains and real world assets in an easily replicable and affordable format.

Introduction

A "Stablecoin" is a type of asset on "cryptocurrency" networks that aims to have a specific price, the methods of pegging such prices vary, in the following segment explore two of the major types of stablecoins; algorithmic stablecoins and backed stablecoins (Rawal, 2020)

An Algorithmic stablecoin is one where the token can be minted or burnt rather than redeemed, this allows that asset-A can be burnt to mint more of asset-B and vice versa (Qureshi, 2021). In this situation if asset-A is the stablecoin trading on a CF/CP liquidity pool and its price goes down by 0.05%, a party can buy the stablecoin at the discounted price and burn it to mint asset-B. The conversion system uses a blockchain oracle to determine how much can be minted or burnt, a blockchain oracle is a mechanism for introducing external data into a blockchain, such as prices (Cedro Labs, 2023). Ideally so long as the oracle presents the correct price then all conversions will be accurate.

On the other end of the spectrum are backed stablecoins, the assumption behind these systems is that every token in circulation is fully backed and can be redeemed for the real asset or an asset of equal value, this requires that the issuer have full liquidity for redemptions (The Serenity Research, 2021).

Problem Statement

Stablecoins at their core are unstable, the vast majority of stablecoins use Constant function/product (CF/CP) liquidity pools (LPs) in order to trade on decentralized exchanges that make use of that trading structure, this come with a flaw, CF/CP LPs pair assets based on relative value of the two assets in the pool, if there were two assets ; Token-A and Token-B, with 1000/500 tokens each respectively, it can then be said that Token-B is twice as valuable as Token-A, each purchase of Token-B reduces its presence in the pool, thereby making it more scarce and therefore more valuable, each sale of Token-B into the pool makes it less scarce and less valuable, this applies both ways for each token (Berezon, 2020).

Regardless of if a token is backed or algorithmic they will find themselves at the mercy of such Liquidity pools.

On the other end of the spectrum are centralized exchanges which uses speculative orderbooks, a stablecoin on these exchanges is subject to the whims of "makers" and "takers", who make and take orders to buy or sell the token, but do so at free market rates, thereby allowing the token to be subject to market forces (Coinscapture, 2023).

The third matter of consideration are frontend applications used to interact with smart contracts, smart contracts are Turing complete or Turing incomplete instruction sets or apps that exist on either an EVM or a locking script or some similar setup (sCrypt, 2020 ; Oh, 2020). The frontend or "dapp" allows users to easily interact with the contract (Cardano Foundation, 2020). But this comes with the pitfall of convenience over decentralization, most dapps are not decentralized, they depend on privately controlled domain names which can change what is routed to, along with often centrally hosted software and lastly; API keys.

In order for a Dapp to interact with live data on the blockchain it needs to query it, but to do so requires an RPC connection (Kovacs, 2021). if one does not own the infrastructure needed to run an RPC then they have to use an RPC service and purchase API key subscriptions, if their subscription ends and they are unable to repay then any functionality that their dapp depends on API keys for; becomes unavailable.

Lastly are oracles; because blockchains are sandboxed environments; data cannot get in without a transaction and cannot get out without an API call, oracles use transaction data to push price updates required for redemptions or conversions of a stablecoin (Cedro Labs, 2023). However, if the oracle is compromised or is unable to push the transaction due to an insufficient balance, then the issuer's price will differ from the open market price, thereby opening an arbitrage opportunity that pushes the market price towards the incorrect issuer price, but the panic from such a scenario results in widespread sale of the token coupled with sudden liquidation of leveraged assets.

Proposal

Dexhune proposes a new type of pegged asset that negates the need for speculative orderbooks and CF/CP Liquidity pools. Dexhune proposes a new form of decentralized oracle that scales in difficulty to exploit.

The core of which is an exchange that allows anyone to create their own pegged asset using parity mechanisms and incentives that will be discussed in detail within this document.

Price DAO

The price DAO is the first and most vital piece of Dexhune, it is a decentralized oracle making use of NFTs in a DAO format where holders propose price updates then vote to accept or reject them.

The price DAO presents exchange rates of DXH to AVAX and vice versa. The 'Price DAO' accepts "proposals" from NFT holders, these proposals are numerical values concerning the "Rate" data on the smart contract, proposals need "votes" from NFT holders to either pass or be rejected, these votes decide to either accept or reject a price update. Additionally, each vote is equally counted and yields 12DXH to the proposer from the contract's balance, this reward is only paid if the proposal passes. All voting sessions last for 15 transaction blocks (30 seconds). The NFT collection used for this price DAO is 'Peng'.

When considering security it must be noted that if someone were to gain majority vote and decided to set the price to something incorrect, such as; 1000AVAX to 1DXH, that would deteriorate trust in the exchange and drain the contract's liquidity. But as the project progresses it becomes more expensive to acquire a 'Peng' NFT, which reduces the potential for such attacks.

But continued growth in value is required as more tokens are issued to the DAO over time, therefore the reward rate will increase by 13.5% every year for 40 years . After 40 years the contract maintains the last stated rate.

The equation for the price is; XAU / 10000 = 0.0001XAU to ##USD.

##USD / Price-AVAX = AVAX to DXH

Price-AVAX / ##USD = DXH to AVAX

So if 1XAU is $1980, 1DXH would be worth $0.198, if AVAX price is $12.710, then AVAX to DXH would be : 0.0140AVAX to 1DXH

and DXH to AVAX would be : 66.890DXH to 1AVAX.

Price updates will fill two fields; AVAX to DXH and DXH to AVAX.

The voter submits the values as;

0.0140 : 1 ; 66.890 : 1

It is to be noted that the price field can accept arbitrary data such as "three dollars and fifty cents" which is a string completely unusable by any contract that depends on the DAO.

However, because votes happen so often the 'Price DAO' would need to be used alongside an automated system, a prototype of which will be created alongside the DAO.

Once fully developed it can be projected that the ideal price for a 'Peng' is; (Estimated value from exploitation / 1000). And this scales as the project grows because to capture a Peng is to capture 1/1000th the potential to drain the Liquidity.

Moreover, much like Byzantine fault tolerance, the system incentivizes participants to behave in the best interests of the network. If a party could make comfy profits from voting in addition to dividends for supporting the Price DAO, whereas attempting to exploit the system could result in major losses if the cost of Peng is far greater than the amount gotten from the exploit they would be more inclined to behave.

The rarity of Pengs is integral to their security, and over time as 'Pengs' get lost or confiscated they will become even more expensive due to scarcity.

Lastly; all value from mint is used as liquidity in the Dexhune exchange contract, thus serving a dual function.

DXH Token

The second smart contract is the DXH token, a time based dividend token.

Parameters

Name : Dexhune

Ticker : DXH

Price : 0.0001XAU (Gold)

Decimals : 0

The DXH token is an ERC-20 which at certain intervals will mint a fixed amount of tokens distributed to holders based on how much they own, the amount distributed is always 0.12% of existing supply. For this to happen the 'Mint' function has to be called, whoever calls the functions receives 5DXH alongside the other minted allocations.

The contract sends a second fund to the 'Exchange contract' worth 0.12% of existing supply. Then lastly a third fund to the 'Price DAO' worth 0.12% of existing supply. In addition to the first fund, this totals ~0.36% expansion every 4 days or 32.85% per year.

The dividend rate is; 10.95% APY with compounding value per mint.

It is to be noted that the token has no decimals, this makes it impossible to peg against other assets on CF/CP LPs or orderbooks.

However, dividends will cease after 40 years (630720000 blocks or after being called 3650 times). Each mint interval in blocks is; 172,800 blocks.

Notwithstanding, after 40 years; 'Exchange Contract' rewards and DAO rewards persist but at a fixed amount of 6,387,851,520DXH to each contract every 4 days. This translates to a

diminishing rate of expansion which overtime becomes negligible to the overall supply.

When the DXH contract is created a total of 10,000,000DXH is minted to the deployer, 90% of this will be deposited into the 'Price DAO' at launch to make up its functional balance, whereas 10% will be sent to the 'Exchange Contract'.

But given the compounding rate of expansion the supply of DXH would expand as follows;

In 30 days: 10,273,553 DXH

In 365 days: 13,886,781 DXH

In 10 Years: 266,695,545 DXH

In 40 years: 5,058,981,004,125 DXH

It is to be noted that these rates expand exponentially, meaning with each mint a new supply level is achieved and then compounded upon at the subsequent mint, ensuring a non-diminishing rate of returns.

Dexhune Exchange

The third smart contract is the Dexhune Exchange, which allows two modes of trading; 'peer trading' and 'Mass Settlement' at either fixed prices or at "parity".

Peer Trading

Peer trading is one of two ways the Dexhune exchange contract settles orders, this allows that users create "buy" or "sell" orders at a predetermined price, these orders are then taken voluntarily by addresses known as "takers", they accept these offers in order to gain rewards in a minted token, this ensures low slippage and no fees.

Trades occur as follows; "makers" deposit their token into the 'Exchange Contract' pending a trade, this encodes 1 of 100,000 writeable NFTs with the details of the trade.

takers can then accept certain trades, thereby sending their token for swap into the 'Exchange contract', this causes the contract to settle both parties and reset the encoded NFT for that particular order.

To ensure that takers are incentivized to trade, each taker is rewarded 2DXH per trade up to a maximum limit of the amount of DXH in the Exchange contract's Balance.

Using this method, trades are completed once the taker's end is fulfilled, the settlement and

reward are done in the same transaction.

NFT Encoding

This is a process of attaching simple identifying data to individual items of a set of 100,000 NFTs owned by the exchange contract, the details written to each item are as follows; the particular token name and contract for the order, the amount for trade, maker address and lastly the block height. Each individual token is encoded separately for each trade and then once the trade is complete the data is erased, there will be a total of 100,000 of these NFTs.

When NFTs are encoded they are sent to an 'Active trades' Wallet, this is just a contract controlled by the exchange contract where the NFTs are easier to differentiate from non-active trades. Only the Exchange contract has the power to transfer the NFTs, thus it can recall them when the trade is settled.

Pricing

The Price for each trade is gotten by checking the 'Price DAO', this shows the exchange rate of AVAX to DXH and vice versa.

The price for DXH is enforced on all trades, all tokens listed are either at a price relative to DXH or at parity. Parity means the contract checks how much DXH there is in the token's stated parity address and determines the token's price relative to DXH and enforces that for trades of the target token within the Exchange contract. Parity can be used in conjuncture with any number of systems to control the amount in the listed token's 'Parity contract', thereby controlling the price, each purchase or sale of the token does not interact with this address therefore does not affect the price. Dexhune's Parity mechanism could allow the emulation of any data set, such as real estate, commodities, and securities. In addition to this; non-financial data sets can be monetized, this includes birthrates in a certain locality, weather, Precipitation rates in a region, etc.

Nonetheless, the value received from each trade is determined when the trade is initiated, this means the exact amount for trade will not change regardless of what happens to the price of either token.

Listing

The default token is AVAX and [DXH].

Although, additional tokens can be added, Adding a token creates an encoded NFT specifically for it, stating its contract address and parity address(if applicable). There will be a total of 1,000,000 list NFTs, making them somewhat scarce.

To address the issue of limited listing space, each listing will cost an increasing amount of DXH,

each time a new token is listed the cost increases by 0.5%, with a starting price of 100DXH and maximum price of 1,000,000DXH. All DXH from listing fees are held within the contract and are eventually used to reward traders or issue 'mass settlement'.

But it must be noted; tokens with decimals cannot be listed, this is meant to prevent listing tokens that exist on CF/CP liquidity pools or orderbooks.

Parity

Each token listed at parity needs a special smart contract that allows the exchange contract to check balances of both DXH and the listed token, then calculate their relative value based on how much of either token is present.

Mass settlement

Mass settlement is a trading structure exclusive to DXH trades, this allows that funds for all trades from or to DXH are automatically settled using the contract's balance. This ensures that DXH has a dual liquidity mechanism, each new token listed helps in growing the liquidity for DXH but listed tokens themselves cannot tap into this same liquidity for mass settlements, lest create an attack surface.

This means all trades *to* a certain token from AVAX are automatically settled if enough of the token is owned by the exchange contract, however trades *from* the token *to* AVAX can only use 'Peer Trading'.

In this process, the contract will attempt to settle up to 10 orders each time mass settlement is triggered. But in conjuncture with mass settlement, takers can still voluntarily complete trades to gain rewards.

Though it is to be noted, because the exchange contract holds a great deal of DXH (from daily mints), this means all trades *to* DXH will be instantly settled with no counterparty, this accumulates AVAX in the contract.

Lastly; any AVAX sent to the contract for whatever reason becomes part of the DXH liquidity pool. This eventuality can be used to add liquidity to DXH.

Frontend

The Dexhune frontend will be somewhat opaque compared to contemporary Dapps, this is because it will make use of a "Blind" design, this means it will not query the blockchain for address information or smart contract states, rather each transaction is built using preset bytecode and user input, then presented to the user's wallet to sign and broadcast. This means if the user inputs incorrect data; the transaction can fail.

This "Blind" design is considered to eliminate a critical security hole in purchasing, renewing and

owning API keys.

The second unique feature of the frontend is the hosting, the frontend will be immutably hosted using IPFS, however, this document proposes 'SSHS' or "Star Side Hosting Service', in simple terms; it allows the disclosure of IP addresses associated with IPFS hosts of a certain item, this IP in conjuncture with a wallet public key are stored with the SSHS client once installed, the public key is provided by the hosting party, thereby they can be identified and tipped for their service.

The third matter of consideration is the domain name renewal contract, which is discussed as follows;

Renewal Contract

This system will use Avvy Domains. The Avvy name for Dexhune will be held by a 'Renewal Contract', which is an NFT collection called 'Marker Fragments' with 100,000 items, they have an initial cost of ~$5 worth of AVAX. But each time 'Fragments' are minted; the cost of mint increases 10%, with a max price of 100AVAX, all AVAX is stored within the contract.

The contract uses the stored AVAX to renew the domain name. Approximately every 6 months any user will be eligible to call the 'renew' function, which prompts the contract to renew the Avvy name for 6 years, as a reward fo calling the 'renew' function, the contract grants 1% of any AVAX it holds to the address that called the function.

Conclusion

In the above document, issues regarding existing stablecoins were discussed, and a potential solution was proposed. Dexhune aims to open up the pathway for innovators to create any sort of price pegged asset and create a more harmonious de-fi environment.

References

Cardano Foundation, (2020) "An Introduction to Decentralized Applications" https://medium.com/cardanorss/an-introduction-to-decentralized-applications-d0fb4f961647

Cedro Labs, (2023) "How do Oracles Work?" https://medium.com/cedro-finance/how-do-oracles-work-12ddff3d41bc

Coinscapture, (2023) "Crypto Orderbooks: How do they work?" https://medium.com/@coinscapture/crypto-order-books-how-do-they-work-7f72d27d3104

Dmitriy Berezon, (2020) "Constant Function Market Makers: DeFi's "Zero to One" Innovation" https://medium.com/bollinger-investment-group/constant-function-market-makers-defis-zero-to-one-innovation-968f77022159

Franciska Kovacs, (2021) "Why Are RPCs So Important In Blockchain Development? 5 Use Cases" https://medium.com/ankr-network/why-are-rpcs-so-important-in-blockchain-development-5-use-cases-60a16a02c143

Haseeb Qureshi, (2021) "A Visual Explanation of Algorithmic Stablecoins" https://medium.com/dragonfly-research/a-visual-explanation-of-algorithmic-stablecoins-9a0c1f0f51a0

SCrypt, 2020 "Introduction to Bitcoin Smart Contracts" https://medium.com/@xiaohuiliu/introduction-to-bitcoin-smart-contracts-9c0ea37dc757

Se Jin Oh, 2020 "What is a Smart Contract? A Beginner's Guide to Blockchain" https://medium.com/haechi-audit/what-is-a-smart-contract-5fa0d32939af

The Serenity Research, 2021 "Overview of Asset Backed Stablecoins" https://medium.com/coinmonks/market-info-overview-of-asset-backed-stablecoin-7e111488e4af

Yogesh Rawal, 2020 "Complete guide to Stablecoins" https://medium.com/akeo-tech/complete-guide-to-stablecoins-in-2020-1f37b7e11d9d