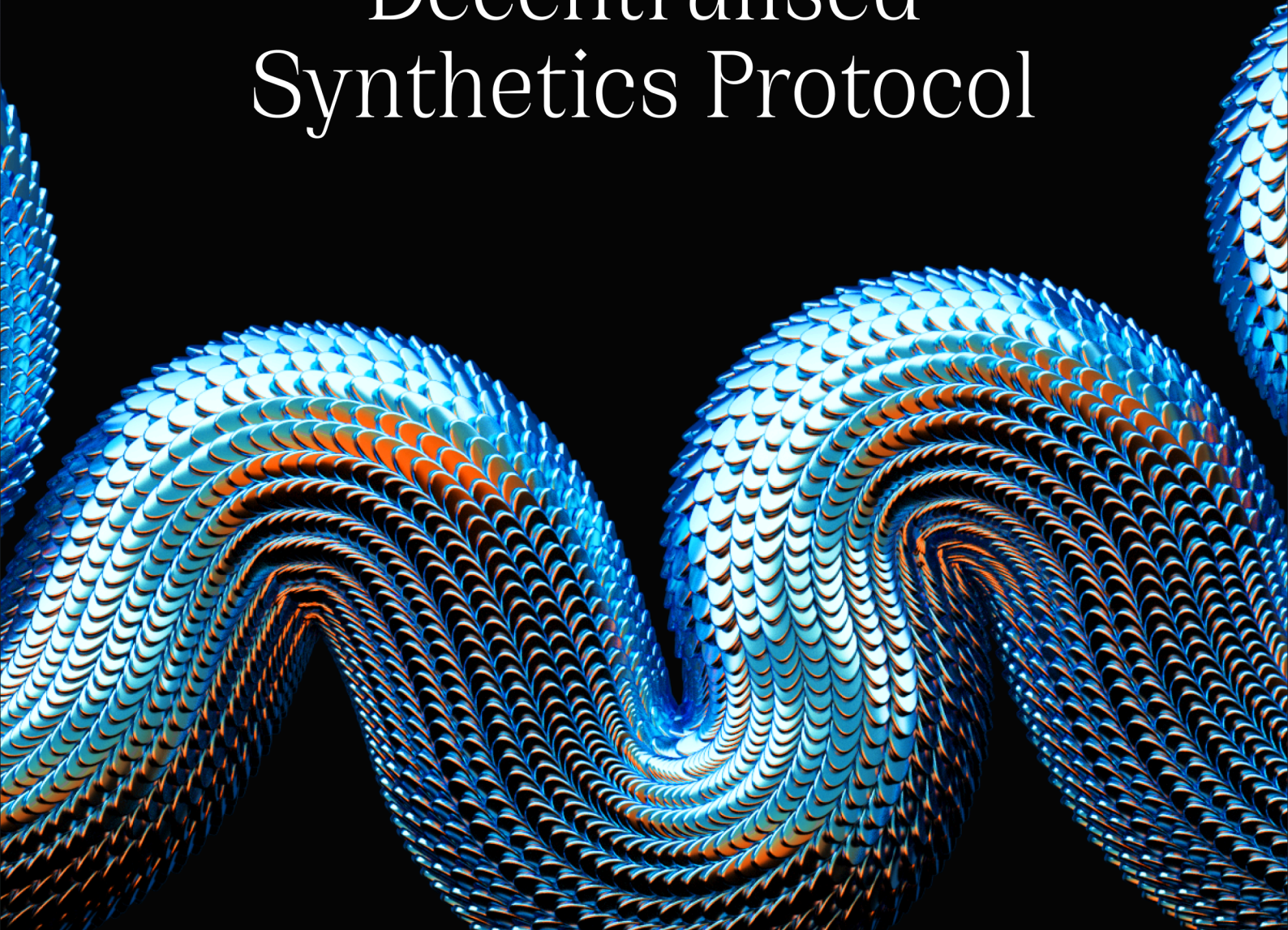




BUTANE

VERSION 1.2

Designing a Secure,
Decentralised
Synthetics Protocol



This page intentionally left blank



BUTANE

An advanced synthetics platform for the Cardano
blockchain.

Micah Kendall
micah@butane.dev

Jay Taylor
jay@butane.dev

03 September, 2024

v1.1

This page intentionally left blank

Abstract

The landscape of decentralised finance (DeFi) is constrained by limited liquidity and inefficient market mechanisms. We introduce **BUTANE**, a groundbreaking approach in the realm of synthetic assets, designed to optimise liquidity and boast immense scalability. Diverse collateral options, efficient liquidation processes, and secure governance mechanisms lie at the core of the protocol. Prioritising robust security and exploring innovative price feed solutions, the protocol seeks to establish new industry standards for economic reliability. This paper serves as a comprehensive guide to the architecture, functionalities, and transformative potential of **BUTANE**.

1 Disclaimer

The content of this white paper is subject to future alterations, may involve unforeseen risks, and could give rise to new discoveries that necessitate reevaluating our initial assumptions. The team reserves the right to modify the white paper & project specification for any reason.

This white paper is intended to accompany the code that **BUTANE** will be deploying. It is crucial to emphasise that the definitive source of accuracy and reliability is always the code itself. A more technical specification of **BUTANE** may be found in the protocol's [yellow paper](#) .

The technical details presented in this paper should not be interpreted as an exhaustive list of features, and it should be noted that features may also be subject to removal.

Contents

1 Disclaimer	6
2 Motivation	11
2.1 Why Cardano?	11
2.1.1 EUTxO	11
2.1.2 Proof of Stake	11
2.1.3 Native Assets	11
2.1.4 Interoperability	11
3 Introduction	12
3.1 Synthetic Assets	12
3.1.1 Classes	12
3.2 Collateralised Debt Positions (CDPs)	12
3.3 The BUTANE Protocol	12
3.4 The Team	12
3.5 Features and Innovations	13
3.5.1 Faster Liquidations	13
3.5.2 Diverse Collateral	13
3.5.3 Stronger Peg	13
3.5.4 Action Composability	13
3.5.5 Cheaper Fees	13
3.5.6 Upgradable Governance	14
4 Protocol Details	15
4.1 Collateralisation	15
4.1.1 Creation	15
4.1.2 Repayment	15
4.1.3 CDP Adjustment	15
4.1.4 Liquidations	16
4.1.5 Redemptions	16
4.1.6 Collateral Equalisation	16
4.2 Oracles	16
4.3 Maintaining Price Stability	16
4.3.1 Trading Bots	17
4.3.2 Collateral Adjustments	17
4.3.3 Treasury Hedge	17
4.3.4 Mark Price	17
4.3.5 Peg Stability Intuition	17
4.4 Collateral-Management delegation	18
4.5 Bond Market	18
4.6 Implementation	18
4.6.1 Smart Contracts	18
4.6.2 Open-Source Release	18
4.6.3 Architecture	18
4.6.4 Upgradability	19

5 Governance	19
6 Development Scope	19
7 Tokenomics	20
7.1 Pro-Rata Sale	22
7.2 Vesting Schedule	22
7.3 Circulating Supply	24
7.4 Governance	24
8 Security	25
8.1 Security Policy	25
8.1.1 Open-sourcing	25
8.1.2 Audit	25
8.1.3 Formal Verification	25
8.2 Protocol Crisis	25
8.2.1 Zero-Day Validator Vulnerabilities	25
8.2.2 Treasury Default	25
9 Links	26
Bibliography	27

List of Figures

Figure 1: A CDP (left) opened to mint synthetic tokens (right)	15
Figure 2: Overview of the “Pepperoni” topology	19
Figure 3: Distribution of \$BTN	22
Figure 4: \$BTN Circulating Supply	24
Figure 5: \$BTN Circulating Supply Dilution	24

List of Tables

Table 1: Examples of possible synthetic assets	12
Table 2: Protocol Roadmap	20
Table 3: Properties of \$BTN	20
Table 4: Distribution of \$BTN	21
Table 5: Team Vesting schedule	23
Table 6: Private Sale Vesting schedule	23

2 Motivation

The Cardano DeFi landscape is beset by inefficiencies and bottlenecks that preclude the development of a truly scalable and open financial ecosystem. **BUTANE** aims to establish universal standards for Cardano DeFi by:

- Offering a flexible and efficient platform for the streamlined creation and management of synthetic assets ([Section 3.1](#))
- Developing interoperable and modular mechanisms for oracle-agnostic price feeds and upgradable governance
- Crafting an inclusive protocol designed to accommodate a broad spectrum of Cardano assets, thereby enhancing liquidity and user engagement

2.1 Why Cardano?

Cardano's academic edge distinguishes it from other blockchains and provides unique advantages for DeFi protocols.

2.1.1 EUTxO

The EUTxO model enhances scalability by facilitating parallel transaction processing, an essential feature for high-throughput financial platforms. Moreover, the incorporation of complex data into transaction outputs allows for stateful and conditional contract logic, thereby offering greater flexibility in asset management and governance mechanisms without compromising efficiency ([Manuel MT Chakravarty, James Chapman, MacKenzie, et al., 2020](#)). The model offers a deterministic, cost-effective fee structure, a superior choice for DeFi applications, which enhances accessibility for a broader audience while enabling scale and throughput.

2.1.2 Proof of Stake

Cardano offers an efficient, sustainable, and cost-effective blockchain consensus mechanism via their Ouroboros Proof of Stake (PoS) system. This ensures long-term sustainability and scalability while maintaining decentralisation ([Kiayias et al., 2017](#)).

2.1.3 Native Assets

Cardano enables the creation and management of native tokens without requiring smart contracts. This simplifies the asset management process and reduces the costs involved, as transferring assets is as seamless as transferring ADA ([Manuel MT Chakravarty, James Chapman, MacKenzie, et al., 2020](#)).

2.1.4 Interoperability

Cardano's architecture is designed for interoperability, whereby DeFi protocols can seamlessly interface with one another. This allows for new platforms to contribute greatly to the DeFi ecosystem as a whole.

3 Introduction

3.1 Synthetic Assets

Synthetics are tokenised derivatives, leveraging oracle smart contracts to track the price of their underlying asset. They extend the traditional derivative model, whereby an investor can trade the underlying asset without needing to physically own it, with the benefits of blockchain interoperability (Rahman et al., 2022). Synthetic assets offer exposure to a wider variety of assets, bridging the gap between DeFi and TradFi.

3.1.1 Classes

The scope of possible synthetics is limited solely by what can be accurately priced. If a price feed could be created for an asset, a synthetic can be made for it. Common examples include:

- Fiat currencies, like USD
- Tangible commodities, like gold
- Indexes derived from real prices, like inverses

3.2 Collateralised Debt Positions (CDPs)

CDPs are debt obligations created upon the locking of collateral into a smart contract. CDPs are closed either by their owner repaying the outstanding debt (and redeeming the collateral), or in the case of debt default, at which point the position is liquidated. This liquidation event nullifies the CDP, placing the owner at a loss, while the loan position is repayed by the liquidator.

3.3 The BUTANE Protocol

BUTANE is a decentralised synthetics platform built on the Cardano blockchain. Synthetic assets are minted via multi-asset CDPs, which maintain a price peg via overcollateralisation and a repayment mechanism for redeeming collateral. Liquidations sustain debt health, allowing other users to takeover or repay undercollateralised CDPs. Cardano Plus smart contracts facilitate all actions on the platform.

Name	Description
\$BTCb	Tracks the price of BTC
\$USDb	Tracks the price of USD
\$\$SOLp	Tracks the inverse price of SOL

Table 1: Examples of possible synthetic assets

3.4 The Team

The BUTANE team is responsible for the initial development and launch of the protocol, as well as bootstrapping the governance mechanism (see the roadmap detailed in Section 6).

3.5 Features and Innovations

The protocol introduces groundbreaking developments in the synthetics space for Cardano. This section outlines the primary objectives, which include achieving unprecedented levels of liquidity, enhancing the safety of liquidations, and building a robust, decentralised protocol. What follows are the key innovations that the protocol brings to the Cardano ecosystem.

3.5.1 Faster Liquidations

BUTANE features an innovative atomic liquidation system, where each CDP liquidation operates independently and without coupling. This design minimises platform congestion and greatly enhances scalability. Moreover, the atomicity ensures liquidation transactions are more compact, leading to increased throughput. These aspects collectively expedite the liquidation process.

3.5.2 Diverse Collateral

BUTANE introduces a dynamic approach to collateralisation. Users can lock multiple tokens when depositing collateral, each of which have distinct, configurable weights. This approach has multiple benefits:

- Risk can be diversified as the user can build a portfolio of tokens to be used as collateral
- Fewer hurdles and barriers encourages more user participation, resulting in a greater amount of total liquidity in the protocol
- Collateral portfolios can be managed via fine-tuned adjustments of the proportions of each token

Parameters for the creation of CDPs are determined via governance.

3.5.3 Stronger Peg

The accelerated and seamless execution of liquidations results in more reactive price adjustments. Additionally, the diversity in collateral deposits ensures price changes in individual assets have an overall lesser effect on the total collateral value. Features such as bad debt absorption via the protocol treasury as well as CDP redemptions also aim to provide additional layers of defense against undesirable depegging scenarios. See [Section 4.3.5](#) for more details.

3.5.4 Action Composability

CDP actions are entirely composable, permitting more complexity with seamless user experience. Benchmarks highlight performance of up to 61 CDP actions per transaction, providing unparalleled atomicity and efficiency.

3.5.5 Cheaper Fees

CDP fees are realised in the form of linearly-accruing interest. The ability to efficiently maintain a strong peg instills confidence in the valuation of BUTANE synthetics, with confidence there can be less hedge, enabling lower fees. The action composability engine is also lightweight and highly optimised, resulting in smaller transaction sizes and execution units.

3.5.6 Upgradable Governance

BUTANE introduces a novel governance mechanism that employs unique ownership tokens for each synthetic asset class. This allows for the independent adjustability of each synthetic, thereby enhancing the protocol's upgradability. Additionally, the system incorporates a forwards compatibility system for transitioning synthetics to new protocol versions.

4 Protocol Details

This section highlights the core functionalities and concepts underlying **BUTANE**. A full protocol specification with concrete definitions and formulae is available in the protocol’s [yellow paper](#).

4.1 Collateralisation

Collateralisation is the mechanism that allows users to mint synthetics.

4.1.1 Creation

Users can mint synthetic assets by initialising a CDP ([Section 3.2](#)) containing a portfolio of permitted collateral tokens. Ownership of this new position can be encoded by an NFT bond, which plays a pivotal role in a specialised market that eases the repayment and liquidation of CDPs (see [Section 4.5](#)).

CDP health is determined as a weighted ratio of the total deposited collateral against the position’s outstanding synthetic debt. Each collateral token has a configurable “weight” which indicates the token’s effective borrowing power. A token with a weight of 2, for example, would indicate that a user could mint up to half of the value of that token deposited as collateral.

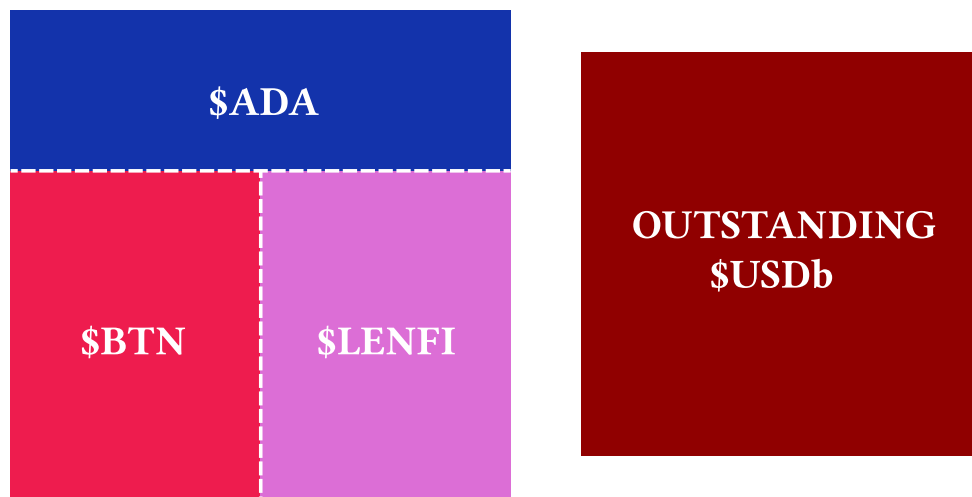


Figure 1: A CDP (left) opened to mint synthetic tokens (right)

4.1.2 Repayment

Repaying a CDP entails burning a portion of the outstanding synthetics, which reduces the total borrowed amount and improves the position’s health. When the entire outstanding synthetic position is burnt, the CDP is closed, and collateral unlocked.

4.1.3 CDP Adjustment

Users have the flexibility to deposit into or withdraw from their collateral portfolio at will, a feature termed ‘Collateral Adjustment’. They can also adjust the outstanding amount of synthetic assets for a CDP by either minting or burning tokens, according to their risk tolerance.

Consider User X, who intends to mint **\$USDb** tokens. In this theoretical, the **BUTANE** community has approved ADA and MIN as eligible collateral with weights of 1.5 and 2,

and USD prices of \$1 and \$0.1, respectively. User X opens a CDP by depositing 1500 ADA and 0 MIN. They calculate that this gives them a borrowing capacity of $\frac{1500 \cdot 1}{1.5} = 1000$ **\$USDb**. They mint 800 **\$USDb**, giving their CDP a Health Factor of 1.25. Later, the USD price of ADA moves to \$0.9, reducing User X's Borrowing Capacity for their CDP to 900 **\$USDb** and its Health Factor to 1.125. To maintain the initial health factor, User X deposits an additional 150 ADA.

Over time, User X opts to switch their collateral from ADA to MIN. To preserve a Borrowing Capacity of 1000 **\$USDb**, they compute the required MIN deposit to be $\frac{2 \cdot 1000}{0.1} = 20000$, assuming the USD price of MIN remains at the original \$0.1. User X deposits the MIN and fully withdraws their ADA, keeping the CDP overcollateralised.

4.1.4 Liquidations

When a CDP is deemed unhealthy (Section 4.1.1), the protocol permits its liquidation as a risk mitigation measure against potential value loss. In this situation, two courses of action are possible by a liquidator: either taking over the CDP or closing it. To execute a takeover, a liquidator can elevate the Health Factor to 1 or higher by depositing supplemental collateral. Upon doing so, they assume ownership of the CDP and generate a new CDP bond. Alternatively, the CDP can be terminated via the liquidator repaying the outstanding synthetic amount, redeeming the collateral for themselves.

In the event of liquidation, the original bond associated with the CDP loses all utility and is subject to burning.

4.1.5 Redemptions

In certain conditions, users can redeem their synthetic holdings for their underlying value by repaying a portion of the debt of a CDP and withdrawing an equivalent amount of collateral value. The conditions for CDP redemptions are flexible and upgradable via a control NFT, authorized either by the wallet or script which holds it.

4.1.6 Collateral Equalisation

Every form of collateral is distinctly characterised by its weight parameter; this remains the sole differentiating factor among various collateral tokens. Beyond this, all eligible assets for collateralisation are treated uniformly. This standardisation provides users with unparalleled flexibility in shaping their collateral portfolios and enables the utilisation of any CNT as potential collateral.

4.2 Oracles

Oracles serve as the arbiters for both the valuation of CDPs and the target prices of synthetic assets. **BUTANE** takes an oracle-agnostic stance; its price feed architecture is crafted to be lightweight, modular, and extensible, accommodating virtually any oracle provider within the Cardano ecosystem.

4.3 Maintaining Price Stability

The **BUTANE** protocol employs a multi-faceted approach to ensure the stable pegging of synthetic asset prices, utilising market bots, targeted liquidation procedures, and the platform's dynamic collateral adjustment feature.

4.3.1 Trading Bots

BUTANE spearheads the development of an efficient, competitive bot marketplace within its platform by offering community-driven resources to facilitate the creation and operation of trading bots. The primary objectives of this initiative are twofold: to expedite time-sensitive economic processes such as liquidations and to offer an additional entrypoint for users to engage with the platform. Automated systems react more rapidly to market shifts and offer precision via algorithmic adjustments, ensuring a more robust price peg.

4.3.2 Collateral Adjustments

Collateral holders possess complete discretion over their collateral portfolios, enabling them to shift between assets with different stability profiles based on their risk appetite and market outlook. This feature acts as a buffer against sudden adverse price movements in any collateral asset, as users can reallocate to more stable assets. The robustness of this system is further enhanced by integration with the automated bot marketplace, which can streamline and optimise collateral management activities.

4.3.3 Treasury Hedge

When the value of a CDP falls below that of its corresponding synthetic asset, liquidation incentives vanish, as the synthetic becomes more valuable than the collateral. In these cases, the CDP is absorbed by the treasury, and the collateral value locked within becomes redeemable. The treasury is allocated funds which act as a hedge in these circumstances.

4.3.4 Mark Price

The protocol adopts a “Mark Price” mechanism, a dynamic approach which averages asset prices from price feeds over a specified window of time, effectively dampening the impact of sudden market shifts. By aggregating prices in this manner, the Mark Price balances short-term volatility against longer-term market movements, offering a more dependable valuation of the asset and reducing the likelihood of extreme volatility in underlying assets disrupting the price peg of their associated synthetics on BUTANE.

4.3.5 Peg Stability Intuition

Let P^S denote the market price of a synthetic asset and P_*^S its oracle-established price. The deviation $\Delta P^S = P^S - P_*^S$ represents the disparity between these two prices. Given that CDPs undervalued relative to their synthetics are managed by the treasury safeguard, we can posit that all unhealthy CDPs can be liquidated at a profit. In a well-calibrated system, ΔP^S should converge to zero, effectively maintaining the price peg. These sections delve into how BUTANE’s core mechanisms collectively contribute to this stability.

A. Arbitrage

When $\Delta P^S > 0$, users can mint synthetic assets at P_*^S and sell at P^S , reducing ΔP^S due to increased supply. When $\Delta P^S < 0$, users can purchase at P^S and liquidate/repay/redeem CDPs at P_*^S , increasing ΔP^S due to reduced supply.

B. Liquidation Strategies

The flexibility of liquidations allows for any price action in the price feed to be instantly reflected on the market.

- **Debt Repayment**

Let S be the supply of the synthetic asset and D be its demand. When synthetics are burnt for debt repayment, S decreases. A decrease in S while holding D constant or increasing will increase the price, thereby reinforcing the peg.

- **CDP Takeover**

Assume C_{old} to be the collateral in the at-risk CDP and C_{new} the new collateral that will make the CDP healthy. This increases the overall protocol liquidity, L , from $L_{\text{old}} = C_{\text{old}}$ to $L_{\text{new}} = C_{\text{old}} + C_{\text{new}}$. The enhancement in liquidity adds a safety margin that further secures the peg.

4.4 Collateral-Management delegation

Since the bond NFT linked to each CDP signifies ownership over the collateral portfolio, users have the option to lock this bond in a smart contract that delegates CDP management authority. This feature enables users to outsource the adjustment of their collateral position to an external service provider, who may charge a fee for the service. Consequently, users can mint synthetic assets without the obligation to actively manage their own CDPs.

4.5 Bond Market

The bond market features an order book that facilitates the closing of CDPs by allowing users to buy synthetics using portions of the collateral. In this system, User A contributes the bond, while User B contributes the synthetic asset. Once the CDP is closed, User B receives a fee, and User A receives any remaining collateral. This eliminates the need for manually purchasing synthetics to close a CDP.

In addition to contributing the bond, User A has the option to contribute additional assets to purchase the synthetic. This means that synthetics can be bought using assets that are not part of the original collateral, thereby offering greater flexibility in the closing process.

User B, who provides the synthetic asset, has the advantage of always being able to see the best offer available. This acts as an instant market sell option that they can execute, allowing them to easily withdraw the value of their synthetics.

4.6 Implementation

4.6.1 Smart Contracts

The BUTANE platform's validator scripts are written in the [Aiken programming language](#). As part of our security policy, rigorous testing and thorough auditing of the codebase are conducted to ensure its robustness and security. An off-chain SDK will be made available in the future to assist with the building and submission of transactions.

4.6.2 Open-Source Release

The platform's source code will be made publicly available under a BSL license, in accordance with the schedule outlined in [Table 2](#).

4.6.3 Architecture

The dApp architecture employs a "Pepperoni" topology, as defined in ([Carmuega, 2022](#)). The web app integrates with backend services to streamline the construction of transac-

tions. These transactions are then signed by the user’s wallet before being submitted to the network.

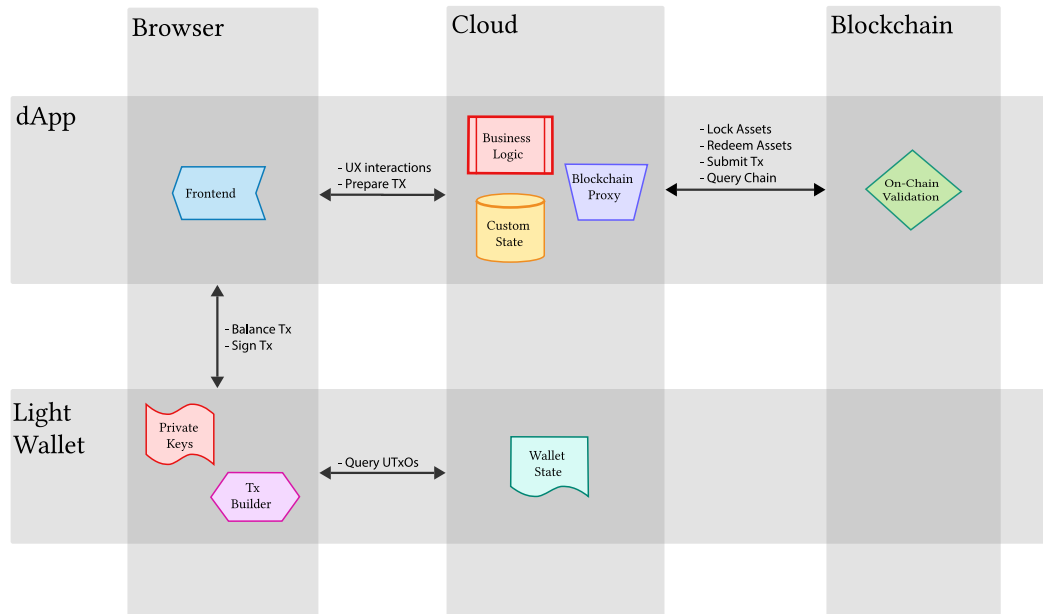


Figure 2: Overview of the “Pepperoni” topology

The app’s backend services efficiently present the current ledger state of all CDPs / parameters from the smart contracts to any querying clients. Transaction submissions are accepted, however only those which interact with BUTANE pass filtering.

4.6.4 Upgradability

Certain contract components, like governance modules and oracle interfaces, require flexibility and configurability to align with the protocol’s long-term objectives. Additionally, Cardano’s infrastructure will undergo future modifications that our protocol ought to be able to seamlessly integrate with. These factors necessitate a core infrastructure that can be painlessly upgraded to accommodate changing requirements. Upgradability can be achieved through two principal mechanisms: NFTs, which are tracked to an associated controlling script, or by modifying parameters within the datum of a UTxO.

A. Price Feeds

The protocol’s price feeds mechanism is designed for adaptability and extensibility. The encoded price data is passed into a script redeemer, which is invoked with a stake withdrawal validator. This allows governance to upgrade the implementation of the feeds. As an example, proposals could be made to integrate new oracle providers.

5 Governance

Governance is scheduled to launch separately to mainnet (See [Section 6](#)). Governance actions are detailed in the protocol’s [yellow paper](#).

6 Development Scope

The protocol is to be first deployed on the [Cardano Preview testnet](#) for a thorough evaluation. After successful auditing to ensure its security and effectiveness, the protocol will

then be deployed on Cardano’s mainnet. After a successful mainnet launch, the team plans to launch governance mechanisms that will make use of the protocol’s native token (see [Table 2](#)).

Milestone	Target Date	Status
Testnet Launch	25 Jan. 2024	Completed
Token Sale Event	23 Feb. 2024	Completed
Audit Completion	Q2 2024	In Progress
Open-Sourcing of Protocol Contracts (Section 4.6.2)	Q2 2024	Pending
Mainnet Launch	Q2 2024	In Progress
Decentralised Governance Launch	Q3 2024	In Progress

Table 2: Protocol Roadmap

7 Tokenomics

BUTANE has a native token (the “Butane token”) with ticker **\$BTN** ([View on Cardano Scan](#)).

Property	Value
Ticker	\$BTN
Asset Fingerprint	asset1aysa4jzmlp6aym80knej09f64vcjy03dqm23k
Policy ID	016be5325fd988fea98ad422fcfd53e5352cacfed5c106a932a35a4
Total Supply	25,000,000

Table 3: Properties of **\$BTN**

It is distributed as shown in [Table 4](#):

Name	Allocation	Per- cent
Total Supply	25,000,000.000000	100%
Public	10,750,000.000000	43%
Protocol	6,625,000.000000	26.5%
Team and Partners	4,250,000.000000	17%
Treasury Hedge	2,250,000.000000	9%
Private Sale	750,000.000000	3%
Miscellaneous	375,000.000000	1.5%

Table 4: Distribution of \$BTN

The protocol treasury is reserved for future distributions of the token, such as rewards or new allocations. The Miscellaneous allocation is reserved for other use cases such as the token airdrop hosted through X.

The allocations for the team and partners are vested, as well as the tokens sold in the private offering (see [Section 7.2](#)).

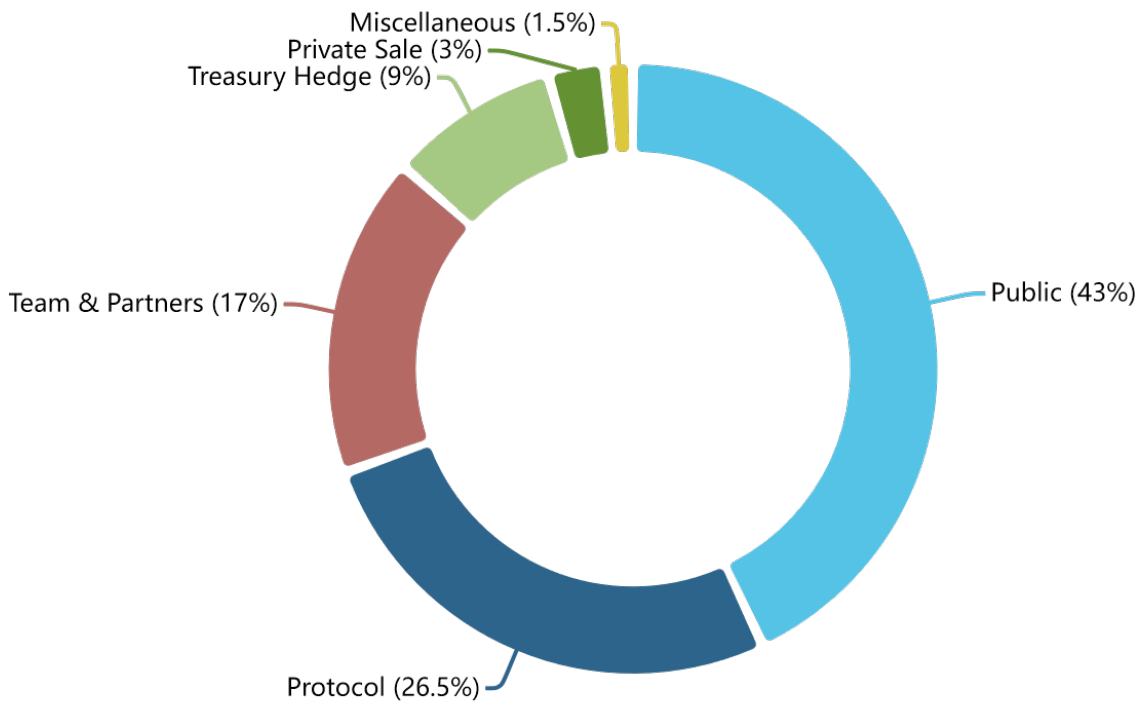


Figure 3: Distribution of \$BTN

7.1 Pro-Rata Sale

The 43% public allocation was distributed via a pro-rata sale mechanism hosted by a [sale portal](#) and [suite of smart contracts](#) developed by the BUTANE team. The event lasted for 24 hours, in which users could deposit ADA to receive \$BTN at a fixed price of 0.9 ADA with a total funding cap of 9,675,000 ADA. Excess ADA was refunded after the event pro-rata. The funding cap was reached within 55 minutes of the sale opening, and a total amount of 49,549,607 ADA was refunded, resulting in 80.47% of each ADA deposit being refunded to participants.

7.2 Vesting Schedule

Tokens allocated to team members, advisors, and private sale participants are subject to a vesting schedule.

The team vesting period runs from August 23, 2024, to July 23, 2025. During this period, a constant fraction of tokens, approximately 1.42%, will be released each month.

Date	UNIX Epoch Time	Cumulative Tokens	Cumulative %
23rd, Aug, 2024	1724371200	354166.666667	1.41667%
23rd, Sep, 2024	1727049600	708333.333333	2.83333%
23rd, Oct, 2024	1729641600	1062500	4.25%
23rd, Nov, 2024	1732320000	1416666.666667	5.66667%
23rd, Dec, 2024	1734912000	1770833.333333	7.08333%
23rd, Jan, 2025	1737590400	2125000	8.5%
23rd, Feb, 2025	1740268800	2479166.666667	9.91667%
23rd, Mar, 2025	1742688000	2833333.333333	11.33333%
23rd, Apr, 2025	1745366400	3187500	12.75%
23rd, May, 2025	1747958400	3541666.666667	14.16667%
23rd, June, 2025	1750636800	3895833.333333	15.58333%
23rd, July, 2025	1753228800	4250000	17%

Table 5: Team Vesting schedule

The vesting for the private sale, which completed August 2023, runs from March 23, 2024, to July 23, 2024. 150,000 tokens (0.6% of the total supply) will be released each month.

Date	UNIX Epoch Time	Cumulative Tokens	Cumulative %
23rd, Mar., 2024	1711152000	150000	0.6%
23rd, Apr., 2024	1713830400	300000	1.2%
23rd, May, 2024	1716422400	450000	1.8%
23rd, June, 2024	1719100800	600000	2.4%
23rd, July, 2024	1721692800	750000	3% (complete)

Table 6: Private Sale Vesting schedule

“Cumulative Tokens” refers to tokens made publicly available through team, partner, and private sale releases. This does not include tokens from other allocations like airdrops or the liquidity event.

The protocol treasury may only be spent through governance, and will be saved until after the launch of the decentralised governance utilities (Section 6).

7.3 Circulating Supply

The following figures show the circulating supply of \$BTN overtime as various allocations release (excluding DAO-controlled treasury, team liquidity, e.t.c.):

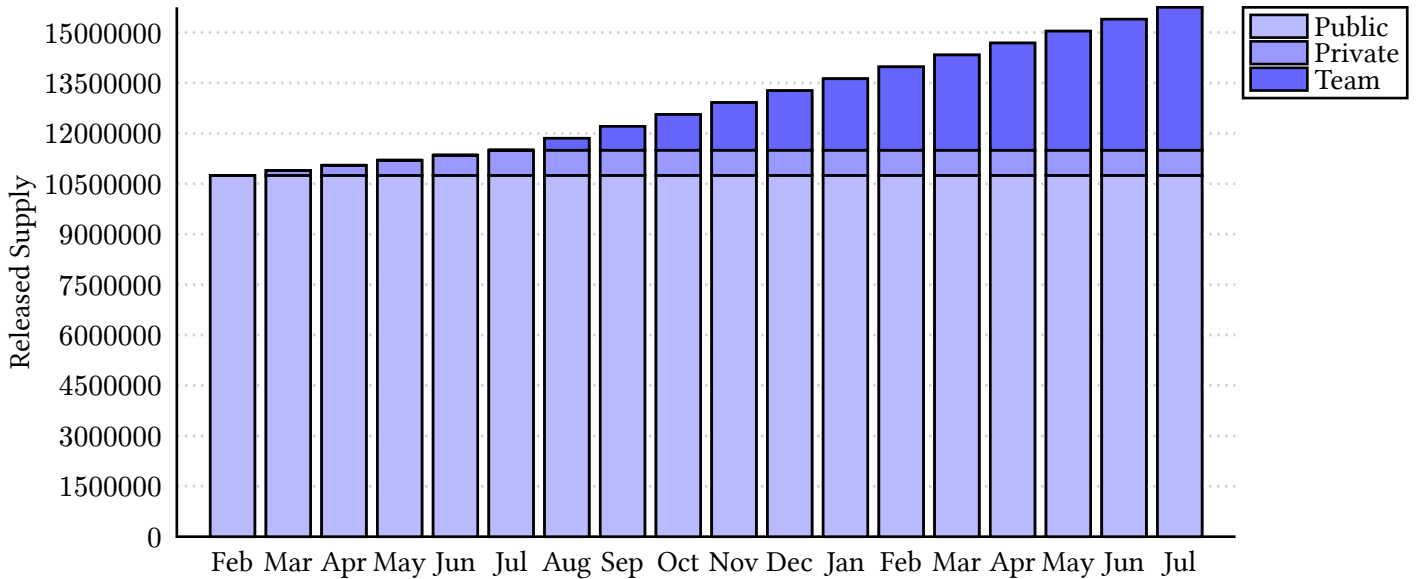


Figure 4: \$BTN Circulating Supply

The following figure highlights how the various allocations of \$BTN are diluted overtime:

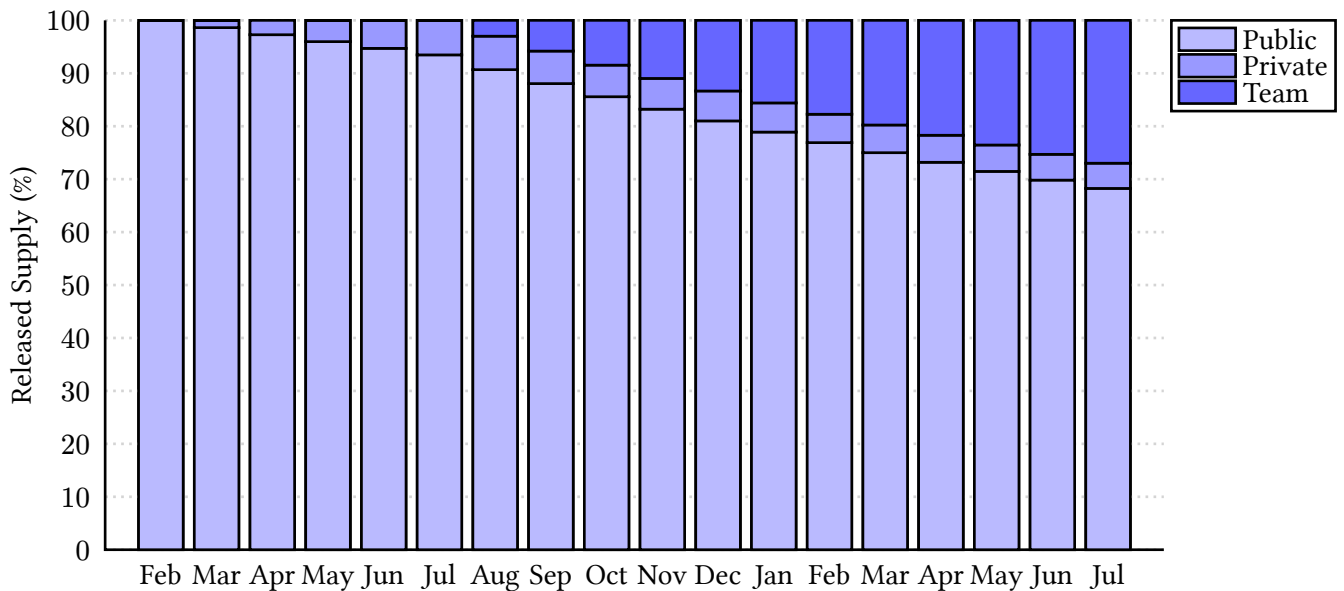


Figure 5: \$BTN Circulating Supply Dilution

7.4 Governance

Each token serves as a proportional voting instrument within the governance framework. These tokens can be staked, enabling holders to propose and cast votes on a variety of matters, including parameter modifications, treasury allocations, and protocol upgrades.

8 Security

8.1 Security Policy

8.1.1 Open-sourcing

BUTANE will be an open-source protocol (Section 4.6.2), conferring enhanced security compared to closed-source counterparts, primarily because of the transparency and scrutiny it invites. When the code is openly accessible, a large community of developers, auditors, and users can examine it for vulnerabilities, errors, or malicious elements.

In a closed-source arrangement, the code is only visible to a limited set of eyes, often within the same organisation, restricting the diversity and number of perspectives that can vet it for security. This “security through obscurity” approach is ineffective and increases the risk of undetected flaws or vulnerabilities that could compromise the contract’s integrity.

Open-source smart contracts inherently foster a more secure and trustworthy environment by subjecting themselves to ongoing community review and improvement.

8.1.2 Audit

As a part of the development scope (Section 6), the protocol has engaged external auditors. These auditors conduct independent assessments of the platform to identify potential flaws, perform comprehensive code reviews, and verify its security, precision, and adherence to industry best practices.

8.1.3 Formal Verification

While formal verification provides an extra layer of security for smart contracts, there are currently no formal verification frameworks available for Aiken, the smart contract language chosen for BUTANE’s development. Therefore, formal verification is not a current option. However, funding of formal verification efforts once the language matures in this area will be considered.

8.2 Protocol Crisis

8.2.1 Zero-Day Validator Vulnerabilities

The protocol identifies the risk of zero-day vulnerabilities—critical, unknown flaws in the smart contracts that could potentially allow unauthorised withdrawal or permanent locking of all funds. Should such a scenario occur, it could result in full losses for holders of Collateralised Debt Positions (CDPs) or synthetic assets. A focus on extensive external review in the protocol’s security policy (Section 8.1) is designed to mitigate this.

8.2.2 Treasury Default

Bad debt may accumulate rapidly in the treasury, which risks a default. This could happen if asset prices fall faster than the system can adapt. In a worst-case scenario, such an accumulation could result in the protocol’s net synthetic position turning negative. This would severely undermine confidence in the protocol and likely prompt a run on synthetic positions. Such a run could de-peg synthetic assets and hamper the protocol’s ability to recover, causing losses for all synthetic asset holders.

9 Links

Website: <https://butane.dev>

Email: contact@butane.dev

Twitter: <https://twitter.com/butaneprotocol>

Discord: <https://discord.gg/butane>

Yellow Paper: <https://files.butane.dev/yellow-paper.pdf>

Bibliography

- Carmuega, S. (2022, December). *0004 Dapp Topologies*. <https://rfcs.txpipe.io/0004-dapp-topologies>
- Chakravarty, Manuel MT, Chapman, James, MacKenzie, et al. (2020). Native custom tokens in the extended UTXO model. *International Symposium on Leveraging Applications of Formal Methods*, 89–111.
- Chakravarty, Manuel MT, Chapman, James, MacKenzie, et al. (2020). The extended UTXO model. *Financial Cryptography and Data Security: FC 2020 International Workshops, Asiausec, Codefi, VOTING, And WTSC, Kota Kinabalu, Malaysia, February 14, 2020, Revised Selected Papers 24*, 525–539.
- Hirniak, J. (2021, October 21). *Axo Protocol Whitepaper THE NEW ERA OF TRADING*. <https://www.axo.trade/whitepaper.pdf>
- Indigo Laboratories, Inc. (2022, November). *Indigo: Synthetic Assets on Cardano*. <https://indigoprotocol.io/wp-content/uploads/2022/01/whitepaper.pdf>
- Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017). Ouroboros: A provably secure proof-of-stake blockchain protocol. *Annual International Cryptology Conference*, 357–388.
- Qin, K., Zhou, L., Gamito, P., Jovanovic, P., & Gervais, A. (2021, November). An empirical study of DeFi liquidations. *Proceedings of the 21st ACM Internet Measurement Conference*. <https://doi.org/10.1145/3487552.3487811>
- Rahman, A., Shi, V., Ding, M., & Choi, E. (2022). Systematization of Knowledge: Synthetic Assets, Derivatives, and On-Chain Portfolio Management. *Arxiv Preprint Arxiv:2209.09958*. <https://arxiv.org/pdf/2209.09958.pdf>