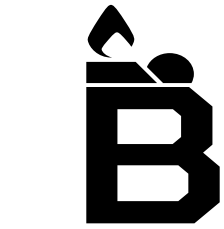
The BUTANE PROTOCOL

White Paper

The Butane Team, *September 2023*

This page intentionally left blank



BUTANE

An advanced synthetics platform for the Cardano blockchain.

Butane Team

15 September, 2023

`v1.0`

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.

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 Cheaper Fees 13
3.5.5 Upgradable Governance 13

4 Protocol Specification **14**
4.1 Collateralisation 14
4.1.1 Creation 14
4.1.2 Repayment 14
4.1.3 CDP Adjustment 15
4.1.4 Liquidations 15
4.1.5 Collateral Equalisation 15
4.2 Oracles 15
4.3 Maintaining Price Stability 15
4.3.1 Trading Bots 16
4.3.2 Collateral Adjustments 16
4.3.3 Treasury Hedge 16
4.3.4 Mark Price 16
4.3.5 Peg Stability Intuition 16
4.4 Collateral-Management delegation 17
4.5 Bond Market 17
4.6 Implementation 17
4.6.1 Smart Contracts 17
4.6.2 Open-Source Release 17
4.6.3 Architecture 17
4.6.4 Upgradability 18

5 Governance **18**

6 Development Scope **18**

7 Tokenomics **19**
7.1 Liquidity Event 21
7.2 Vesting Schedule 22
7.3 Governance 24

8 Security **24**
8.1 Security Policy 24
8.1.1 Open-sourcing 24
8.1.2 Audit 24
8.1.3 Formal Verification 24
8.2 Protocol Crisis 24
8.2.1 Zero-Day Validator Vulnerabilities 24
8.2.2 Treasury Default 25

9 Links **26**

Bibliography **27**

List of Figures

Figure 1: A CDP (left) created to mint synthetic tokens (right) 14
Figure 2: Overview of the “Pepperoni” topology 18
Figure 3: Distribution of the native token 20
Figure 4: Distribution of tokens for the liquidity event 22
Figure 5: Pre-governance **$BTN** release schedule 23

List of Tables

Table 1: Examples of Synthetic Assets on **BUTANE** 12
Table 2: Development scope of the **BUTANE** team 19
Table 3: Properties of the native token 19
Table 4: Distribution of the native token 20
Table 5: 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 (Chakravarty, Chapman, MacKenzie, Melkonian, Peyton Jones, 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 (Chakravarty, Chapman, MacKenzie, Melkonian, Müller, 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:

- Established currencies, like USD
- Tangible commodities, like gold
- Stocks and other assets traded on a stock market

3.2 Collateralised Debt Positions (CDPs)

CDPs are positions created upon the locking of collateral into a smart contract. They are used in DeFi lending platforms when a user wishes to take out debt and is required to deposit sufficient collateral. CDPs are closed either by the user repaying the 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 Plutus smart contracts facilitate all actions on the platform.

Name	Description
$BTCb	Tracks the price of BTC
$USDb	Tracks the price of USD
$NASDAQb	Tracks the Nasdaq Composite index

Table 1: Examples of Synthetic Assets on **BUTANE**

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, which will launch separately (see the roadmap detailed in Section 6).

The team will dissolve upon the full implementation of the protocol, allowing **BUTANE** to autonomously manage its operations. By this milestone, the protocol will aim to be fully self-sufficient and sustainable. The preliminary deadline for this event is 15-Aug-2024.

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, which encompass both the valid tokens to be deposited and their associated weights, 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. See Section 4.3.5 for more details.

3.5.4 Cheaper Fees

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.

3.5.5 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. Additionally, the system incorporates an innovative mechanism for transitioning collateral liquidity between different protocols. Further details on this feature will be elaborated in upcoming paper releases.

4 Protocol Specification

4.1 Collateralisation

Collateralisation is the mechanism that allows users to mint synthetics.

4.1.1 Creation

Each synthetic asset class has an associated set of parameters, referenced using an ownership token. These parameters specify the allowed tokens for collateral and their respective weights. Users can mint synthetic assets by initialising a CDP (Section 3.2) containing a portfolio of the allowed collateral tokens. Ownership of this new position is represented 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). Users are free to mint as many synthetic tokens as they desire, provided the CDP remains in a "healthy" state, defined as follows:

Let $\{c_1, c_2, ..., c_n\}$ be the amounts for a collateral position with n tokens, and similarly $\{p_1, p_2, ..., p_n\}$ and $\{w_1, w_2, ..., w_n\}$ be the market price of the i'th token with respect to the synthetic asset (as given by a price oracle) and weights for each token, respectively. Then,

$$\text{BC} = \sum_{1 \leq i \leq n} \frac{c_i \times p_i}{w_i} \tag{1}$$

$$\text{HF} = \frac{\text{BC}}{s} \tag{2}$$

Where s is the amount of the synthetic to mint/borrow, BC is the Borrowing Capacity, and HF is the Health Factor.

If $\text{HF} > 1$, the position is deemed overcollateralised and healthy. Otherwise, it falls into an "unhealthy" state and may be liquidated.

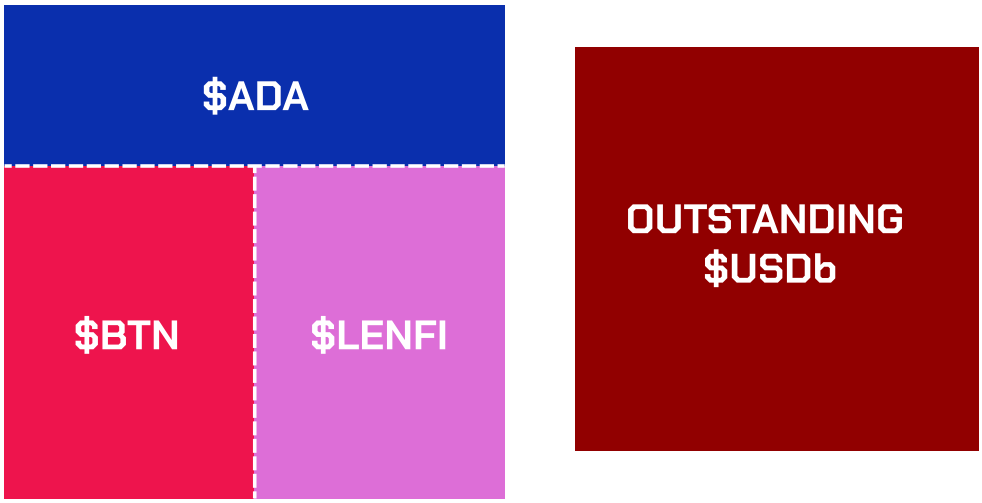


Figure 1: A CDP (left) created to mint synthetic tokens (right)

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 Factor, allowing the owner

to withdraw a portion of their locked collateral. When the entire outstanding synthetic position is burnt, the CDP is closed, and all locked collateral is released.

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 establishes a CDP by depositing 1500 ADA and 0 MIN. They calculate that this gives them a Borrow 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 the CDP's Borrowing Capacity 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 and healthy.

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.

4.1.5 Collateral Equalisation

The values of collateral assets within a CDP are standardised via their weight parameters. Beyond this, all eligible assets for collateralisation are treated uniformly. This provides users with unparalleled flexibility in shaping their collateral portfolios and enables the utilisation of any asset on the Cardano blockchain as potential collateral.

4.2 Oracles

Oracles provide data feeds which determine 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 entry-point 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

A reserve treasury functions as a failsafe against the risk of depegging. 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 liquidated into the treasury, whose resources are then allocated to acquire synthetics and repay the CDP via an auction process.

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 an underlying asset disrupting the price peg of its associated synthetic.

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 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 (see Section 8.1), 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 Section 6.

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

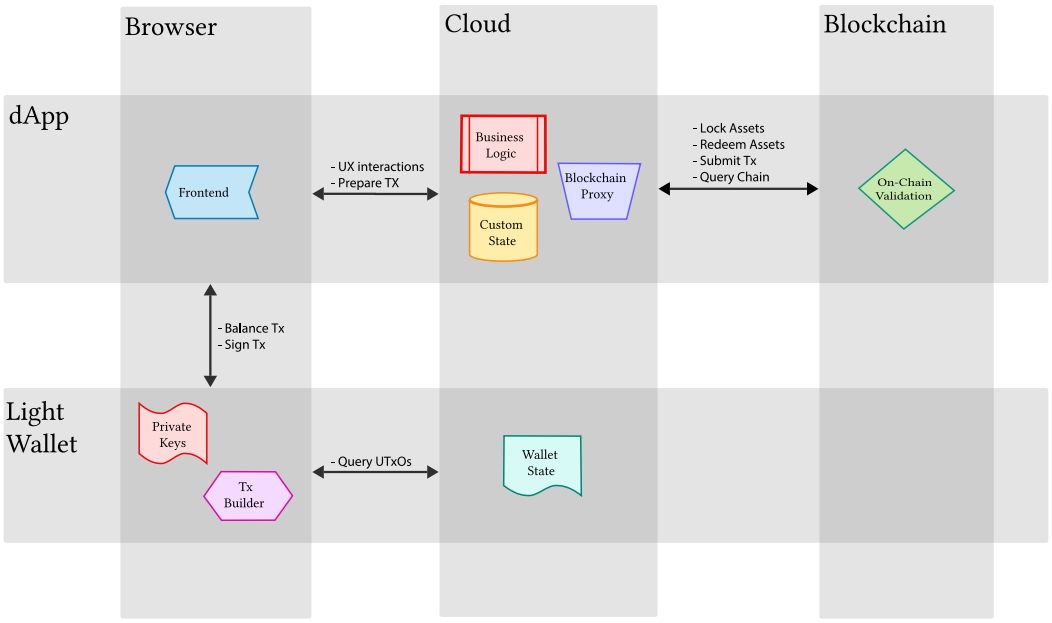


Figure 2: Overview of the "Pepperoni" topology

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 the 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 seperately to mainnet. (See Section 6)

6 Development Scope

The **BUTANE** team (Section 3.4) is focused on launching an initial protocol that will first be deployed on a Cardano testnet for 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).

Task	Target Date
Launch Testnet	Late December
Finish Auditing	Q1 2024
Launch Mainnet	Q1 2024
Open-source Protocol (Section 4.6.2)	Q1 2024
Decentralised Governance	Q3 2024

Table 2: Development scope of the **BUTANE** team

Decentralised governance aims to be initiated in conjunction with the final release of tokens, as outlined in the vesting schedule (Section 7.2).

7 Tokenomics

BUTANE has a native token (the "Butane token") with ticker **$BTN** (View on Cardano Scan).

Name	**BUTANE** -Token
Ticker	**$BTN**
Asset Fingerprint	asset1vv3wgsx9xpg5gpl4629mparm7hlpqnavpdwnj3
Total Supply	25,000,000.000000

Table 3: Properties of the native token

It is distributed as shown in Table 4:

Name	Allocation	Percent
Total Supply	25,000,000.000000	100%
Protocol Treasury	13,750,000.000000	55%
Liquidity Event	5,000,000.000000	20%
Team	3,500,000.000000	14%
Partners	1,000,000.000000	4%
Community Contributors	750,000.000000	3%
Private Offering	750,000.000000	3%
Airdrop	250,000.000000	1%

Table 4: Distribution of the native token

The protocol treasury is reserved for future distributions of the token, such as rewards or new allocations.

The allocations for the team and partners are vested, as well as the tokens sold in the private offering (see Section 7.2). Community contributors can be rewarded via the community contributors fund. This may be used to reward people who write content, make graphics, or positively contribute to the **BUTANE** community. The airdrop allocation is used in various airdropping events, such as the event hosted through Twitter.

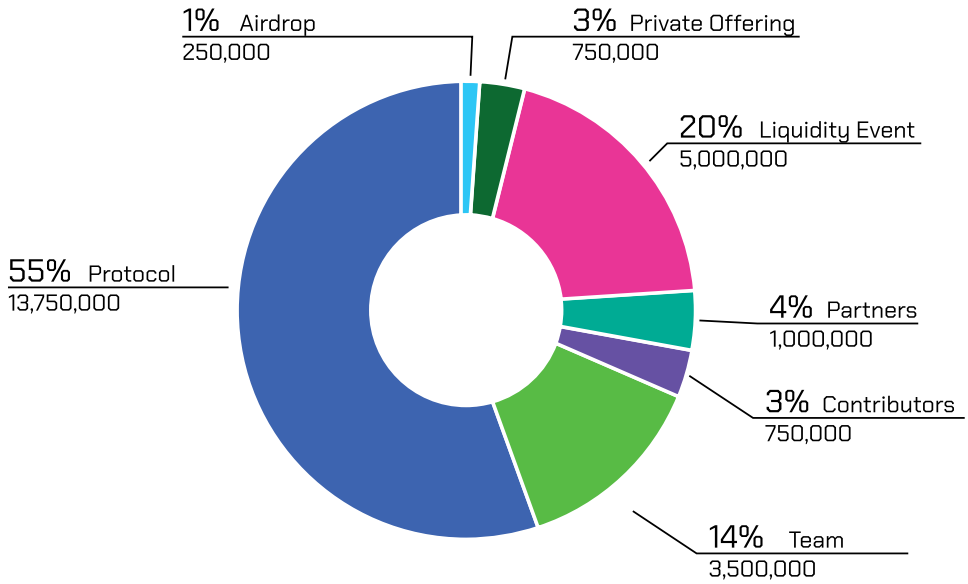


Figure 3: Distribution of the native token

7.1 Liquidity Event

The liquidity event serves as an initial mechanism for setting a fair market price for **$BTN**. During this event, 3,750,000 **$BTN** will be distributed through a sale mechanism, and an additional 1,250,000 **$BTN** will be used to create a liquidity pool on a DEX. Any wallet may participate in the sale. The amount of **$BTN** a participant receives is proportional to how much ADA they deposit, relative to the total amount deposited by the community. For example, if a total of 6,000,000 ADA is committed, a participant who committed 2,000 ADA would receive 1,250 **$BTN** and a participant who committed 6,000 ADA would receive 3,750 **$BTN**.

The ADA collected during the event will be allocated to three initiatives:

- 33% is allocated to the creation of a DEX liquidity pool, paired with 1,250,000 **$BTN**
- 33% is allocated to the protocol treasury hedge
- 33% is given to the team

The liquidity event does not serve as a fundraiser for the development budget of **BUTANE**. Rather, it aims to set a fair token price and distribute tokens in a decentralised and transparent manner. The 33% allocation to the team serves to offset the effective loss from the 20% of **$BTN** being distributed to the public.

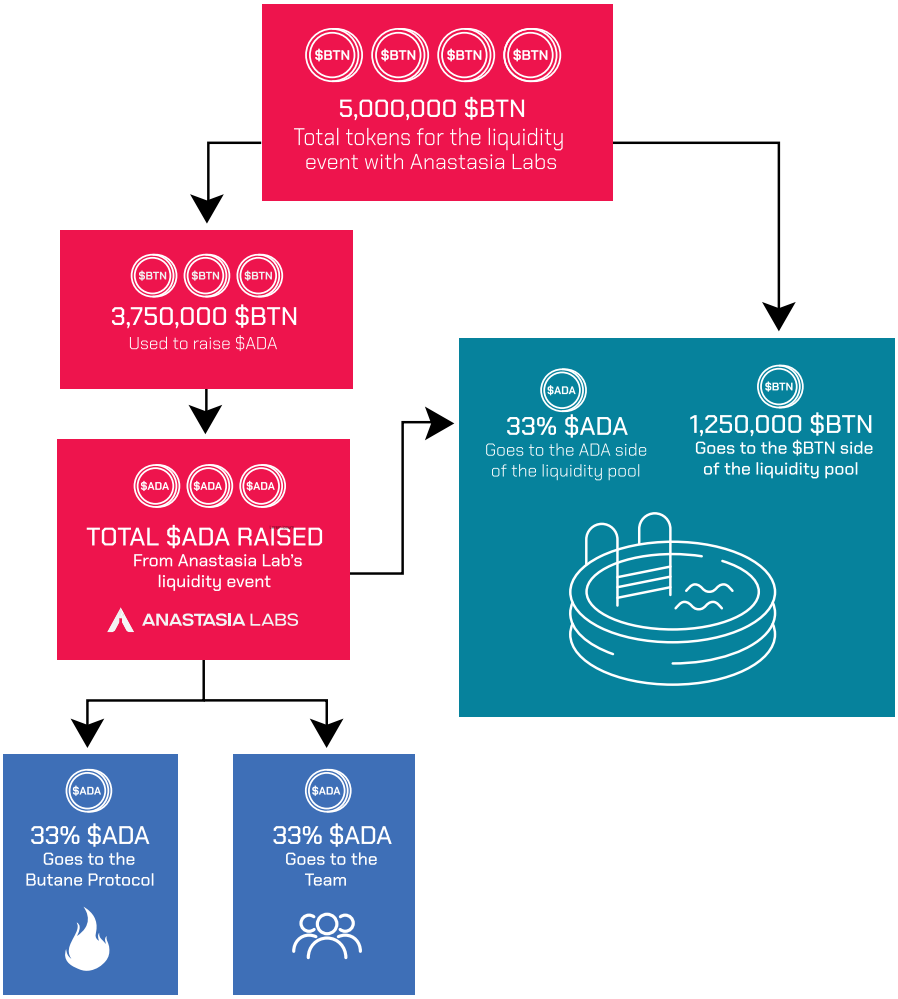


Figure 4: Distribution of tokens for the liquidity event

7.2 Vesting Schedule

Tokens allocated to team members, advisors, and private sale participants are subject to a vesting schedule. The vesting period runs from November 15, 2023, to July 15, 2024. During this period, a constant fraction of tokens, approximately 2.33%, will be released each month.

Date	UNIX Epoch Time	Cumulative Tokens	Cumulative %
15th, Nov., 2023	1700006400000	583334	2.333336%
15th, Dec., 2023	1702598400000	1166668	4.666672%
15th, Jan., 2024	1705276800000	1750002	7.000008%
15th, Feb., 2024	1707955200000	2333335	9.33334%
15th, Mar., 2024	1710460800000	2916668	11.666672%
15th, Apr., 2024	1713139200000	3500001	14.000004%
15th, May, 2024	1715731200000	4083334	16.333336%
15th, June, 2024	1718409600000	4666667	18.666668%
15th, July, 2024	1721001600000	5250000	21%

Table 5: Vesting schedule

The schedule outlines specific dates and corresponding UNIX Epoch Times for clarity. For example, on November 15, 2023, a total of 583,334 of the vested tokens will be on the market, representing about 2.33% of the total allocation. The percentage of cumulative tokens released increases in similar increments each month, reaching up to 21% by July 15, 2024.

"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. By July 2024, including these other allocations, up to 45% of the total token supply could be in the market.

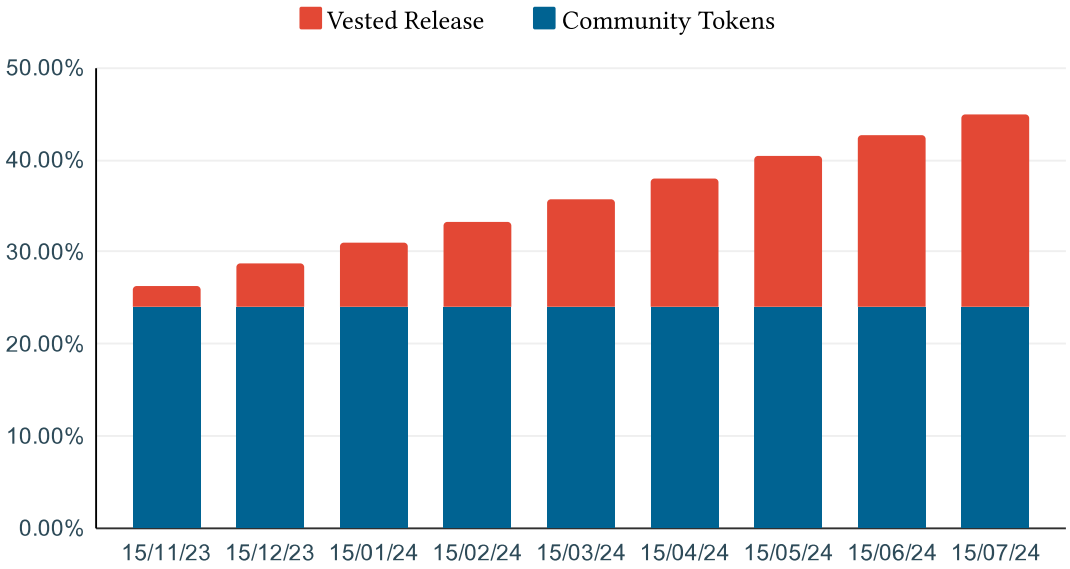


Figure 5: Pre-governance **$BTN** release schedule

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 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 will engage external auditors. These auditors will 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 owners of 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

Bibliography

Carmuega, S. (2022, December). *0004 Dapp Topologies*. TxPipe. https://rfcs.txpipe.io/0004-dapp-topologies

Chakravarty, M. M., Chapman, J., MacKenzie, K., Melkonian, O., Müller, J., Peyton Jones, M., Vinogradova, P., & Wadler, P. (2020). Native custom tokens in the extended utxo model [Paper presentation]. In *International symposium on leveraging applications of formal methods*. Springer.

Chakravarty, M. M., Chapman, J., MacKenzie, K., Melkonian, O., Peyton Jones, M., & Wadler, P. (2020). The extended utxo model [Paper presentation]. In *Financial cryptography and data security: fc 2020 international workshops, asiausec, codefi, voting, and wtsc, kota kinabalu, malaysia, february 14, 2020, revised selected papers 24*. Springer.

Hirniak, J. (2021, October 21). *Axo Protocol Whitepaper THE NEW ERA OF TRADING*. Axo. 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 [Paper presentation]. In *Annual international cryptology conference*. Springer.

Qin, K., Zhou, L., Gamito, P., Jovanovic, P., & Gervais, A. (2021, November). An empirical study of DeFi liquidations [Paper presentation]. In *Proceedings of the 21st ACM internet measurement conference*. ACM
. 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