JIFM JOURNAL OF INSURANCE AND FINANCIAL MANAGEMENT

# Tokenomics Designs and their Parallels in Traditional Finance

Afonso Carvalho [a,*]

[a] *University of Porto, First Principles Research*

**ARTICLE INFO**

***Article History***

| | |
|---|---|
| Submitted | 15 May 2022 |
| Accepted | 22 May 2022 |
| Available online | 02 Jun 2022 |

***JEL Classification***

B26; G12; G15
O31; G32; G23

***Keywords***

Crypto
DeFi
Decentralized Finance
Cryptocurrencies
Blockchain
Tokenomics
Valuation

**ABSTRACT**

As more and more mechanisms for utility and value accrual are explored for cryptocurrencies and tokens, a comprehensive list and analysis of the different types of token economics designs currently being employed can be a useful starting place either for people getting into the space or for teams considering their own implementations.

Furthermore, many if not most people outside of crypto still have the mental model of a currency as what all tokens are trying to be. In 2022, this way of thinking is too reductionist and leads great investors and builders to underestimate or even dismiss the space.

Journal of Insurance and Financial Management

*Corresponding Author:
afonso@carvas.org

## Introduction

This article is written in a way that frequently compares effects of tokens' economics to the foundational concepts in finance such as shares, profits or dividends. The intent of this structure is to leverage knowledge and heuristics many readers will already have from traditional finance.

However, tokens are not equity and protocols are not companies. All parallelism drawn is simply for producing better explanations via analogy.

These were the mental models that first led my own interest in tokenomics and decentralized finance to develop, so it may prove to be a useful starting point of view to others as well.

## Earnings in Traditional Finance

If a traditional company has profits, there are four main ways to use them:

1. It can simply **hold** them as reserves on the balance sheet. This increases optionality and stability:

    a. Optionality: In the advent of a market downturn, a healthy balance of cash or cash equivalents will be worth more since it can be deployed to acquire potentially undervalued assets (other companies, its own stock, etc);

    b. Stability: if demand decreases or competitors drive down margins, strong reserves assure the company can continue to pay employees and meet general expenses without depending on profits, on having to issue debt or on incurring dilution.

2. It can distribute them directly to owners.

    **Dividends** are the most straightforward concept here. The company can simply pay a part of its earnings to its shareholders, proportionally to their ownership.

3. It can purchase its own stock on the open market.

    **Buybacks** are another popular mechanism for driving value from earnings to shareholders. Companies use their profits or balance sheet to buy their own stock and then 'retire' the shares purchased thereby reducing the total number of shares outstanding. This then leads to each share representing a larger percentage ownership of the company (the denominator decreased) driving up earnings per share and theoretically each share's value.

4. It can **reinvest** the earnings.

    By far the broadest of these categories and can take many forms: everything from hiring, acquisitions, CaPex, R&D or accelerating marketing and growth would fall into this category. Shares of a company have intrinsic value from entitling owners to the company's assets (balance sheet, physical assets, intellectual property, etc), to its future earnings and to having voting rights over big decisions (governance).

Shares of a company have intrinsic value from entitling owners to the company's assets (balance sheet, physical assets, intellectual property, etc), to its future earnings and to having voting rights over big decisions (governance).

* * *

Many tokens employ designs that resemble each of the value accrual mechanisms mentioned above. We will explore just four main buckets in this text and cover one or more in production examples for each model: governance tokens, dividend yielding tokens, buyback and burn and credit insuring dilution.

## Plain Governance Tokens

One of the simplest forms of token designs is a token whose utility and value is solely to vote on the respective DAO or protocol's governance decisions and proposals.

This mechanism gives token holders some, most or all the power (depending on where the protocol is on the decentralization spectrum) over the project's future direction, as well as, importantly, over its treasury holdings and use.

If a DAO were a company, its treasury would be its balance sheet. Treasuries will normally hold the project's own token, stablecoins or even other assets such as ETH or other project's tokens. Fees or earnings made by the protocol usually accrue to the treasury as well.

Two current examples of this token type are UNI and LDO, the governance tokens of Uniswap and Lido respectively. They have slight but interesting differences:

1. **UNI**:

    a. Brief context on the protocol: Uniswap is a decentralized exchange of the AMM type [1][2][3]. Traders pay fees (from 1 to 30 basis points depending on the pair) but these go to liquidity providers (LPs) to Uniswap's pools. In other words, Uniswap as a project hasn't turned monetization yet since the protocol itself doesn't accrue any fees nor generates earnings from the billions of dollars traded through it everyday.

    This prioritises growth and moat building over short term profits and is a classic strategy many startups use outside of crypto.

    b. A particularity of the UNI token is that holders can, at any time, collectively vote to turn on a protocol fee [4]. If or when this happens, just like LPs receive fees for the liquidity they provide to the DEX, Uniswap's treasury would also receive a small fee from every trade executed, similar to what currently happens in centralized exchanges such as Coinbase or FTX.

    The possibility of this fee switch being turned on by governance can be seen as giving UNI tokens intrinsic value, since real cash flows to the holders would follow. Similarly, Amazon was unprofitable for many years before reaching a scale at which making profits was sustainable, but AMZN shares had value during both periods.

2. **LDO**:

    a. Brief context on the protocol: Lido allows people to stake assets (such as ETH) while remaining liquid on those positions and still able to use derivative tokens (e.g. stETH) across DeFi, as collateral or otherwise. For this, Lido takes a fee as a percentage of the staking rewards that accrue to the assets staked through it [5][6].

    b. Contrary to Uniswap, the Lido DAO already has revenues and earnings from the fees its products generate. These fees accrue to Lido's treasury which is controlled by the LDO holders via governance.

    These tokenflows currently work in a way analogous to retained earnings in a company (earnings not distributed to shareholders) and also provide a justification for LDO having intrinsic value.

## The x Model: Distributing earnings

What we're calling 'The x Model' here is the token design popularised by Sushiswap's **xSUSHI** [7]. Brief context on the protocol: Sushiswap is a decentralized exchange that operates with the CFMM design [8]. In every trade executed through it, there's a 0.25% fee given to liquidity providers and a 0.05% fee for the protocol itself. The latter, times the volume traded via the DEX, can be thought of as the (gross) profit the protocol generates.

Under this model, holders of a governance token have, at all times, the possibility of staking it and in exchange receiving "the x version" of that same token (i.e. staking SUSHI to receive xSUSHI).

Staking and therefore holding the x token has two main benefits:

1. A part of or all **fees** generated by the protocol are paid directly to holders of the x token in a similar way to how profits generated from a company can be paid to shareholders via dividends (although this analogy is mechanistically imperfect here, see *Note 1*).

2. **Voting power** is enabled. Usually, in protocols employing this token design, only the x versions of their governance tokens have voting rights in governance decisions [9].

This design seems to be more of a direct improvement than a trade-off compared to the traditional way employed by companies of distributing dividends to shareholders, due to staking (and therefore reduced sell pressure) being necessary to make the token a productive asset.

## Buyback and Burn

In the same way that traditional companies can use their earnings to buy their own stock, protocols and DAOs can also use profits generated to purchase their own token in order to reduce circulating supply and/or have sustained buy pressure for their token.

**MKR: Classic Buybacks**

Brief context on the protocol: MakerDAO allows users to borrow DAI — a stablecoin whose value remains pegged to 1 USD — by depositing into a vault a greater value of collateral (such as ETH or WBTC) than the amount borrowed [10]. Borrowers of these loans pay, in DAI, what is called a "Stability Fee" to take them. This fee is mechanistically similar to the interest rate a borrower would pay to borrow dollars from a traditional bank, but goes entirely to Maker instead of being split between the bank and the lenders.

Maker then uses these profits to regularly purchase its governance token — MKR — on the open market and burn the amount purchased. From all designs we cover in this article, this is one of the closest ones to its parallel in traditional finance: the stock buybacks using earnings described above.

**EIP-1559: A special case of Buyback and Burn**

Since the implementation of EIP-1559 in August of 2021, the value of ETH, the native asset of the ethereum blockchain, is tied to the network's usage demand.

The other examples of protocols mentioned in this text are all application layer DeFi protocols meaning they exist on a blockchain and provide a financial service, be it exchanging tokens or borrowing against one's assets. The parallels between them and traditional financial services companies are much more straightforward than the one we will review now.

But blockchains themselves are also protocols that generate economic value, though their product is much more comparable to an internet provider than to a bank in terms unit economics: Blockchains sell blocks [11].

Oversimplified context on blockspace: Every blockchain can handle a limited number of transactions per period of time due to two factors: block size and block time.

A block is the unit by which blockchains register new valid transactions that are added to the history of transactions on that chain. Relevant to the scope of this article, a new block contains all the new transactions that are to be included in the blockchain's new state.

Blocks themselves are bounded in size [Note 2], effectively determined by the number of transactions and their respective required computational effort. This limit is called block size.

Depending on the blockchain, a new block takes some time to be generated and included. This metric is called block time. In the case of the ethereum blockchain, the average block time is currently around 14 seconds [Note 3].

On the one hand, block size and block time determine the supply of blockspace a blockchain offers: x number of transactions of y complexity can be executed per second.

On the other hand, users, DAOs, protocols and, increasingly, other chains [12] want to execute transactions on the blockchain. Everything from performing swaps, paying back loans, trading NFTs, executing or deploying smart contracts. This represents the demand for the blockspace.

Ethereum and many other smart contract blockchains employ a gas market to match this supply and demand. In order to get one's transaction included in a block, users will have to pay what is called a gas fee. The value of this fee follows basic microeconomics and is the price at which demand for blockspace matches the supply available (approximately). Gas fees

are normally paid in the native cryptoasset of the blockchain in question: in the case of ethereum, gas is paid in ETH.

Enter **EIP-1559:**

After the introduction of this upgrade to ethereum, a large portion of every gas fee paid (the base fee) is *burned*: that amount of ETH is removed from the total supply in existence [13][14].

Mechanistically and financially, the sum of burnt ETH in gas fees can be thought of as revenue that the ethereum blockchain immediately and invariably allocates to buying back its native asset.

This mechanism correlates the demand for transacting on the ethereum blockchain with the rate at which ETH is being burnt and hence with ETH's supply contraction.

How this becomes a mechanism for value accrual to the native asset of a popular blockchain should, at this point, be somewhat clear. There are, however, two extra steps in the justification.

First, gas fees have to be paid in ETH, hence as long as people want to use ethereum to build or transact there will be assured demand for ETH itself. Secondly, once ethereum transitions to Proof-of-Stake*, ETH holders will be the ones validating transactions and being rewarded proportionally to the size of their holdings.

An analogy in traditional finance would be if companies had to pay for AWS cloud computing services with amazon stock, a portion of which would then be retired, lowering the number of amazon shares outstanding.

## Loss Insurance via Dilution

Another prevalent design envolves relying on the market value of a protocol's tokens to effectively insure the health of the protocol and its users' funds under all circumstances, such as extreme volatility (to the downside).

This model is common in protocols where debt is issued and risk has to be managed.

There are two main distinct examples of this model: **MKR** and **AAVE**.

### MKR: Everyone backstops losses

Further overview of the protocol: Loans taken out via Maker are overcollateralized which theoretically ensures borrowers will eventually pay off their debt in order to regain access to the assets they deposited (that should be worth more at all times).

If the USD value of one's collateral drops below a certain threshold, Maker will forcefully auction it off and repay the debt issued against it using the proceeds generated.

However, in extreme cases such as fast and deep market crashes, it is possible to end up with collateral positions whose market value has fallen below the DAI debt issued against them. If this happens, we have a case of bad debt [15]: credit that Maker issued and that can't be expected to be paid back (fully).

Bad debt existing leads to a situation in which some of the DAI outstanding is now undercollateralized. This presents an extreme risk for the stability of DAI and for the trust deposited in the protocol and in MakerDAO.

To overcome this risk, Maker uses its own token as the backstop to cover bad debt: new MKR is minted and sold on the market until enough proceeds are generated to pay off all bad debt in the system (assuring no undercollateralized debt positions are left across Maker vaults) [16].

This happening has two negative effects for MKR holders: first, the total supply of MKR will increase, meaning their MKR position now represents a smaller percentage ownership of the protocol (dilution); secondly, since the MKR issued is immediately sold on the open market, the price of MKR will expectedly fall (at least in the short term) from the increased selling pressure relative to normal market conditions (sell-off).

Game theory behind this design:

MKR holders are the ones governing over all protocol decisions such as which assets are accepted as collateral and their respective risk parameters. Miscalculated decisions increase the chance that bad debt will exist in the future in which case MKR holders would also be the ones getting diluted.

In traditional finance:

- Banks can incur bad debt as well. For example, mortgages are also overcollateralized loans since the underlying real estate should, at all times, be worth more than the cash yet to be repaid. However, if, for example, the housing market crashes (like it did in the United States in 2008 [17]), someone's house can end up with a lower market value than the value of the loan taken against it, leading people to default.
- MKR's backstop mechanism applied in traditional finance is similar to a bank issuing and selling new stock (raising capital by diluting all current shareholders) whenever its holding bad debt and until it can fix its toxic balance sheet and make sure all depositors are made whole.

**AAVE: An opt-in Safety Module**

Brief overview of the protocol: Aave is a protocol for the lending and borrowing of cryptoassets. Depositors provide capital to the market to earn a yield, while borrowers are able to borrow in an overcollateralized (indefinitely) or undercollateralized (for one block) fashion, and pay interest on it [18].

**The risk: Shortfall Events**

Aave effectively carries a liability towards the depositors. The protocol's smart contracts (or borrowers) hold the deposited tokens while Aave issues aTokens [19] to depositors as an IOU that is redeemable 1:1 for the actual tokens deposited.

Just as we saw in Maker's case, there are rare but conceivable events where Aave can experience a loss of funds. A bug in the smart contracts leading to exploits, bad liquidations from insufficient market liquidity of some collateral asset and oracles [20] not properly updating prices are all examples of such risks.

The first and main way Aave insures that depositors would be made whole if such an event were to occur is through a mechanism called the **Safety Module**. The SM is a contract where holders can deposit and lock either AAVE tokens or AAVE/ETH BPT (a token representing 80% AAVE and 20% ETH, in a balancer liquidity pool [21], which isn't necessary to be familiar with in order to grasp the point made here).

This act is called staking AAVE and the protocol incentives it by minting new AAVE tokens daily and proportionately distributing them to stakers.

The capital locked in the Safety Module can then be partially sold off (up to 30% of it) to cover a deficit created by one of the aforementioned shortfall events, thereby making depositors whole.

If the 30% aren't sufficient to cover the entirety of the debt, new AAVE will be issued (an event called Recovery Issuance [22]) and auctioned off in a similar way to the dilution mechanism employed by Maker.

Mechanism and game theory analysis:

1. On the one hand, in Maker's case, the owners (MKR holders) constantly incur a tail risk of being diluted in case of bad debt entering the system.

2. On the other hand, AAVE holders have two choices:

    a. Take risk: They can stake it in the Safety Module and collect yield (i.e. receive newly minted AAVE), thereby increasing their ownership of the protocol over time. That reward is justified since they are effectively contributing more to the success of the protocol than AAVE holders that choose not to stake it: in case of a Shortfall Event, this group will be the first to have their holdings slashed to cover Aave's deficits.

    b. Pay for other holders to take the tail risk: These stakeholders can passively hold the token (not stake it in the SM) and accept a small level of dilution over time (the new AAVE issued to incentivize group 1. that is increasing the token's total supply). This dilution can be seen as effectively the cost to pay for insurance: they will be the last ones slashed to cover bad Shortfall events.

In sum, AAVE holders can either choose to sufer a small level of constant, daily dilution or have their ownership slowly increase in normal conditions but accept a tail risk of large losses.

The daily amount of AAVE minted and distributed to stakers in the Safety Module is a constant number (determined by governance). This means that if more people stake AAVE, each AAVE token staked will receive a smaller share of the newly minted AAVE.

However, more AAVE staked in the safety module reduces the expected depth of slashing events (a smaller percentage of a larger capital pool can cover the same amount of bad debt). Market participants consider these two factors in their risk/reward calculations until an equilibrium is reached in the amount of AAVE staked in the SM.

## Future Considerations

Tokenomics design is a burgeoning field of research and experimentation. There is an uncountable number of other models already being used by many projects in production and many more being conceived weekly.

This article covers some of the first and better known ones, but only a small fraction of the space. The designs mentioned here are also, for the most part, the ones with closer analogies to traditional companies and shares, hence the parallelism established throughout. Other, newer mechanisms can be much more complex and diverge too far from traditional finance for those analogies to be useful.

We aim to analyse, in subsequent texts, other tokenomics designs as well as the incentives and effects they produce and the game theory involved.

## Notes

1. Sushi doesn't distribute earnings to xSUSHI holders in the same exact way companies do via dividends. While companies make profits in USD and distribute the subsequent dividends in USD too, Sushi makes profits in LP tokens of the respective pools, sells them for SUSHI on the open market and deposits that SUSHI in the pool of SUSHI owned by xSUSHI holders, without issuing new xSUSHI in the process. This effectively increases the number of SUSHI owned per xSUSHI outstanding (numerator increased while the denominator remained constant) all while increasing buy pressure on SUSHI.

   For more information, refer to: https://docs.sushi.com/products/yield-farming/the-sushibar

2. Post EIP-1559, block size actually varies between blocks with demand but that fact is not necessary to the points made in this text. For a deeper dive read: https://notes.ethereum.org/@vbuterin/eip-1559-faq

3. We intentionally oversimplified how gas and blocks work in ethereum. For a deeper dive on the actual mechanics, there is no better resource than the ethereum docs themselves. Highly recommend reading: https://ethereum.org/en/developers/docs/

## References

[1] Hayden Adams et al. Uniswap Whitepaper. 2018.

[2] Hayden Adams et al. Uniswap v2 Core. 2020.

[3] Guillermo Angeris et al. An analysis of Uniswap markets. 2019.

[4] Introducing UNI, Uniswap Blog. 2020

[5] Vasiliy Shapovalov, How Lido Works, Lido Blog. 2020.

[6] Kasper Rasmussen, 2021. Introducing LDO, Lido blog.

[7] What is xSUSHI?, Sushiswap Docs.

[8] What is SushiSwap?, Sushiswap Docs.

[9] Proposals and Voting, Sushiswap Docs.

[10] Kenton et al. 2020. Maker Protocol 101.

[11] Ryan Sean Adams, 2021. The best product of the decade.

[12] Sam Richards et al. 2022. Layer 2 scaling, Ethereum Docs.

[13] Vitalik Buterin, EIP 1559 and Fee Structure.

[14] Vitalik Buterin, EIP 1559 FAQ.

[15] Alicia Tuovila, et al. 2021. Bad Debt, Investopedia.

[16] Flopper: The Maker Protocol's Debt Auction House, MakerDAO Docs.

[17] Financial crisis of 2007–2008, Wikipedia.

[18] Aave Protocol Whitepaper, 2020.

[19] aToken Valuation: How does the market and economic theory value aTokens?, Aave Document Portal.

[20] Asset Risk: Methodology, Aave Document Portal.

[21] Weighted Pools Use Cases: Aave Safety Module, Balancer Docs.

[22] Aavenomics: Safety Module, Aave Document Portal.