Fair Forks Incentivize Protocol Rejuvenation

Sam Williams
sam@arweave.org

Abhav Kedia
abhav@arweave.org

DRAFT-3.
March 15, 2022

Abstract

The two most prominent methods of protocol governance in blockchains and crypto networks today are DAOs and forks. While both of these governance methods have gained popularity and success in various implementations, they suffer from serious problems ranging from lack of incentives for good governance to platform risk for their developers and users.

We propose a third method of blockchain governance that aims to capture the best features of both of these modes – **fair forks**. Fair forks are a non-coercive coordination system that rewards good governance and innovation. They build upon existing methods of forking in blockchains and add an incentivization layer and a fork resolution mechanic.

1 Introduction

For healthy long-term governance of cryptonetworks and decentralized protocols, we propose the following desired characteristics:

- **Platform Integrity:** There should be protocol-level assurances that the platform will not change their rules of engagement for users, developers and service providers on the platform. In cases where there must be breaking changes to the protocol, a previous unchanged version of the protocol must exist for continued use. This property is explained further in the next section (2.1.2 - I).
- **Incentives for Innovation:** Developers and entrepreneurs should have sufficiently powerful financial incentives to maintain and improve the protocol in the long run.
- **Incentives for Good Governance:** There should be financial incentives for community members to effectively direct the protocol towards its goals.
- **Community Cohesion:** Community members should have an incentive to band together and work towards the goals of the protocol instead of viewing protocol updates in an adversarial light.

Armed with the lens of these desirable properties, we can examine existing models of governance in cryptonetworks. These trade-offs are expanded upon in greater detail in the next section, but broadly we summarise them here in Figure 1.

DAOs	Forks
• PROTOCOL EVOLVABILITY • COMMUNITY COHESION	• PLATFORM INTEGRITY
• LACKS INCENTIVES • NO PLATFORM INTEGRITY • PLUTOCRACY	• LACKS INCENTIVES • ADVERSARIAL COMMUNITY RELATIONS

Figure 1: Existing Governance Mechanisms

We observe that the above is a high-level summary of frequently observed features of protocols using these governance mechanisms. Individual governance implementations might differ among protocols, and the lines between their properties are often finer than the categorization provided here. Nevertheless, we find that it is instructive to view existing protocols from this perspective.

1.1 Table of Contents

This introductory section laid out the specific properties that our new governance mechanism seeks to optimize for. The rest of this paper is organized as follows:

- In section 2, we provide an examination of governance structures and incentives in DAOs and forks.
- In section 3, we introduce **Fair Forks**, a social protocol that incentivises good long-term governance of a protocol without introducing the drawbacks identified with DAOs and forks.
- In the penultimate section on Multi-Fork Resolution, we discuss the possible paths and decisions that a network will take when multiple fair forks are active.
- In the final Discussion section, we explore extensibility and applicability in generalized blockchain

settings, along with tradeoffs and implementation decisions.

2 Contemporary Models of Governance

2.1 DAOs

Decentralized Autonomous Organizations have many meanings and definitions in the crypto ecosystem. Therefore, we provide here a definition for DAOs that is relevant to our discussion.

2.1.1 Definition

In the rest of this paper, we use the term DAO to refer to entities which exhibit each of the following three properties:

- Lives on the internet and exists autonomously.
- Is governed by code (automation) at its core, and real-world actors (individuals and organizations) at the edges.
- Contains some form of internal capital that is used to determine voting power in decisions concerning (among other things) modifications of the protocol.

This internal capital in DAOs today is most often called a governance token. Most of the defining properties of DAOs as described here have been cited before[5].

DAOs are the most commonly encountered mode of organization today in smart contract based decentralized applications (dApps). Common examples include media organizations like BanklessDAO, DeFi protocols like Olympus, Uniswap and Compound, and curation/collection DAOs like PleasrDAO and ConstitutionDAO [17, 23, 7]. Further, under the above definition, we note that mutable-blockchain networks like Polkadot and Tezos fall under this same category [18, 22].

2.1.2 Benefits and Drawbacks

In this part, we discuss commonly observed properties of DAOs that are deployed today, while acknowledging that future DAO structures may improve upon current drawbacks.

The core benefits of DAOs emerge from their ability to enable protocol upgrades in a decentralized setting while typically also maintaining community cohesion. In addition, DAOs enable collective asset ownership, management and curation[3].

Unfortunately however, many DAOs today reintroduce a number of problems that plagued centralized platforms of the web2 era. Infact, DAOs behave like companies in that they enable coercive updates and incentivise value extractive behaviour. More precisely, some of the problems with existing DAOs include:

I. Breaking Platform Integrity

The services rendered by DAO-based protocols are not immutable and can subsequently break **platform integrity -** assurances that the platform will not change their rules of engagement. The centralized web2 world is rife with examples of companies breaking platform integrity [24]. One of the core promises of decentralized networks is that participants can rely upon the protocol's offering remaining stable over time. This immutability enables developers and users to make deeper investments in the protocol – basing entire businesses around its model – without fear that the platform will change underneath their feet.

In layer 1 blockchains, Polkadot and Tezos are examples of coin voting systems that allow upgrades to the network without hard forks. While this introduces flexibility, it also potentially breaks platform integrity.

Another example of DAOs breaking platform integrity is fee changes in DeFi protocols. This has happened with liquidity pool fee structures in many protocols (including Curve[9], Uniswap[19], etc.) which are mutable by governance, and mean that users and downstream application developers cannot rely on the protocol's fees to remain stable over time.

II. Plutocracy

DAOs are often structured as a plutocracy. Governance tokens represent voting rights, and these tokens are usually tradeable. This exposes the protocol to coercive updates by what is typically a wealthy minority of community members.

An analysis of the most prominent DeFi DAOs today show extremely high Gini coefficients for governance [10]. Among Compound, Uniswap, Sushiswap and Yearn, it was found that just 2-7 voters decide the outcome of every governance proposal [11]. Notably, this is comparable to the board size of many large traditional technology firms.

III. Lack of Incentives for Good Governance

DAOs do not normally provide financial incentives for good governance. This often leads to a Pareto distribution where, on one-end, the majority of DAO participants have little incentive to participate, and on the other end, a wealthy minority (which could have non-trivial conflicts of interest) can make decisions that are suboptimal for the protocol itself. This can be broken down as a number of distinct issues:

- Few governance participants. Failure of governance proposals because of insufficient voter turnout demonstrates that token holders have little incentive to participate in governance [21].
- Large participants may have conflicts of interest in the governance of the protocol. Lack of direct reward/punishment for the quality of governance de-

cisions means that the conflicting incentives often dominate. As a consequence, governance decisions that are even knowingly poor quality are enacted inside the protocol. Curve's yield wars are a prime example of this phenomenon playing out in practice [2, 6].

- Lack of incentives for good governance creates space for those with ulterior motives to take significant roles in governance. This can give rise to dangerously self-interested 'protocol politicians' that may have complex motivations beyond financial gain [8].

Some experiments in incentivised DAO-based governance are already underway [4, 13], but they are early and as yet unproven.

IV. Insufficient Incentives to Reward Early Innovators

Traditional early-stage startups grow as a result of extremely powerful incentives for a small number of founders (typically 1-3). Their ownership stakes in the startup typically represent such a high proportion of their net assets that it consumes a very large amount of their focus. Such powerful incentives are considered necessary to make valuable companies.

While DAOs with truly decentralized ownership at inception have seldom been tested, we do not expect them to fare well in terms of innovation incentives. This is because the market capitalization of a DAO at inception places a fundamental limit on the number of people that can be sufficiently powerfully incentivised to actively focus on developing the protocol. Early stage DAOs have relatively low market cap at inception, so a very large community with decentralised ownership would vastly diminish each member's personal incentives to grow the value of the DAO.

Specifically, consider the financial incentive strength for a founding member. Provided that her ownership in the DAO has some value - her DAO Ownership Value (DOV), and some amount of Net Assets (outside the DAO), then her financial incentive can be modeled in approximately the following fashion:

$$Incentive = \frac{DOV}{DOV + NetAssets}$$

Provided the DAO has a non-zero valuation and equal token distribution, the DOV for members above can be calculated:

$$DOV = \frac{MarketCap}{Members}$$

Subsequently, the number of people that the DAO can likely command the attention and focus of can be modeled as follows:

$$Members = \frac{MarketCap * (1 - Incentive_{Threshold})}{Incentive_{Threshold} * NetAssets_{Mean}}$$

With a $\$10M$ valuation, an incentive threshold of 0.9 (atleast 90% of my networth should be in DAO ownership to commit fully), and an average net-worth of $\$400K$ US [1], this works out to only 2 people that are sufficiently incentivised to fully commit to the DAO.

We note of course, that the calculation above is only instructive and not a binary function of the incentive threshold. Nonetheless, it demonstrates our point - that early stage DAOs cannot be both decentralized and have sufficiently incentivised founders from the onset. At the present time, most early-stage DAOs address this issue by centralising control of tokens amongst a small 'founding team' - essentially rendering themselves a plutocracy. This, of course, mirrors the activities of a traditional startup – further compounding all aforementioned risks.

2.2 Forks

The traditional way to settle governance disputes and perform upgrades in layer 1 blockchains is through forks. Since there are many definitions, we include here a taxonomy of forks to make explicit the types that we are concerned with in this paper.

2.2.1 Taxonomy of Forks

At the highest level, blockchain forks are of two types: *state-preserving* and *state-resetting* forks.

State-Preserving Forks

These types of forks preserve the state of the blockchain prior to the fork. Such forks can be further subdivided depending on whether the rules for block acceptance have changed [20]:

- **Process-based forks**: Forks where there is no change in the protocol's underlying rule set for block acceptance. These can arise naturally as a result of network delay (when two miners mine blocks at the same height at almost the same time). They can also arise as a result of malicious actors that deliberately hold back mined blocks, for example, in selfish-mining [14]. Although the frequency and nature of such forks may be impacted by parameters that could be controlled by governance (such as block time), process-based forks are not themselves mechanisms for governance and therefore will not be considered in this paper.

- **Protocol-based forks**: Forks where the block acceptance rules change between the child and the parent network. In protocol-based forks, miners and validators upgrade their software to adopt the new 'version' of the protocol. These forks are further subdivided into three categories [12]:
  - *Soft forks*: Forks where the set of rules for block acceptance become more restrictive, i.e. the set of transactions that will be accepted by

nodes operating on the new software is strictly a subset of the transactions that are accepted by nodes on the older version. Since blocks formed by the new nodes are still accepted by old nodes, such forks are also backwards-compatible.

– *Hard forks*: Forks where the set of rules for block acceptance are loosened, i.e. the set of transactions accepted by new nodes is strictly a superset of the transactions accepted by old nodes. Such a fork is not backwards compatible, as blocks proposed by new nodes will not be accepted by older nodes.

– *Bilateral forks*: In bilateral forks, the rules for block acceptance are incompatible both ways.

State-Resetting Forks

These types of forks only fork the code of the original blockchain, make the desired edits, and attempt to bootstrap a network from scratch. This means that account balances or other forms of state or utility from the original network are not carried to the forked network over in the case of state-resetting forks.

2.2.2 Benefits and Drawbacks

The core benefit provided by blockchains that rely on fork-based governance is that of platform integrity. A protocol is only mutable by forking, and even when this happens, an older version of the code and network continues to exist. This is in alignment with one of the core promises of the decentralized internet.

However, there are several problems that arise when any of the different kinds of forks are used as the primary form of governance and protocol upgrades. These include:

I. State-Resetting Forks Reset Community Alignment

For stateless forks, there is a complete loss of community incentives to participate in bootstrapping a new network. The utility of the network is not preserved when only the code is forked as the community of miners, developers and users face overwhelming switching costs from the parent network. This can lead to aggressive and perverse incentives designed to bootstrap community in forked versions of protocols, such as "vampire attacks" [16].

II. State-preserving Forks Provide Limited Innovation Incentives

For state-preserving forks, although there are some incentives for good governance, they are often limited to large stakeholders, again leading to a plutocracy. In particular there are no incentives for the developers of a new fork to expend time, capital and effort for getting stakeholder buy in to move a network in the desired direction and achieve the goals of the protocol.

As a result, founders turn to state-resetting forks if they want to improve the protocol. This nullifies the claim to value that prior contributors (via skills or financial investments) have made to the protocol so far.

III. Encouraging Adversarial Relationships

For both types of forks, there is an adversarial relationship between stakeholders of the child and the parent (original) network, since it is in the interest of the asset holders to preserve the value and utility of their own network. Stakeholders in the parent network may see the proposed fork as a threat to the "memetic prominence" of the parent. This creates fear, uncertainty and doubt, potentially eroding the value of the original as well as any derivative networks.

In view of the aforementioned shortcomings of forks and DAOs as identified here, in the next section we propose **fair forks**, a novel social protocol for incentivizing good long-term governance of a cryptoeconomic protocol.

3 Fair Forks

Fair forks are a social protocol that capture the adaptability benefits of DAO-based governance, while maintaining platform integrity guarantees offered by traditional blockchain fork-based governance. Fair Forks are an extension of traditional hard forks in blockchains.

A **fair fork** refers to any fork that adheres to the Principles outlined in this section as well as the protocol guidelines specified by the original founders (or drivers) of the protocol they seek to fork in the protocol's **Founding Constitution**. Developers of a fair fork of a protocol outline a **Refounding Proposal** with goals, methods and rewards for the proposed protocol upgrade at the time of the fork. We refer to the developers of a fair fork as **refounders**. For the period of the refounding, these refounders are expected to act as "benevolent dictators" of the protocol - although always operating within the bounds of the fair forking guidelines, the Founding Constitution and their own Refounding Proposal. Figure 2 below shows the major pieces involved in a fair forking update.

The refounders' adherence to this fair forking social protocol is independently adjudicated by each impacted party, community member and asset holder and does not rely on centralised or authority-delegated decision making.

As a result of their unique design as detailed in this section, fair forks introduce good governance incentives - missing from both prior systems studied in this paper. Also with fair forks, previously adversarial elements of fork-based governance are replaced with positive-sum collaboration incentives among community members.

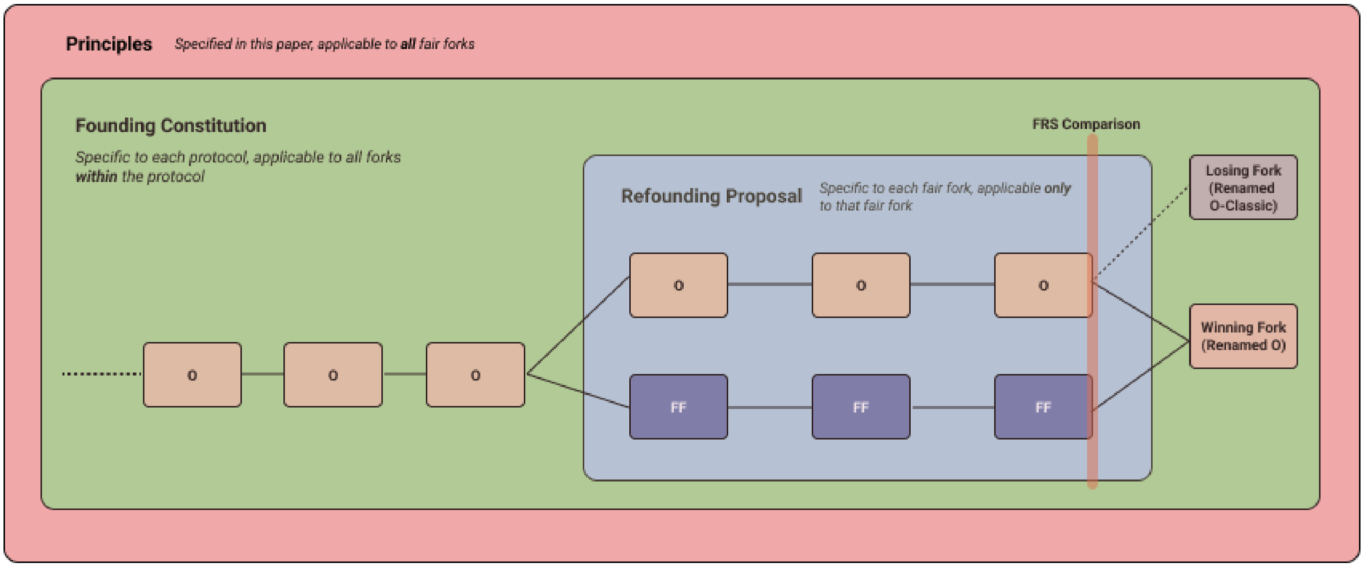

Figure 2: Fair forks

3.1 Principles

We now outline the principles behind a fair fork. Additionally, each network will specify its variant of the fair forking protocol in its Founding Constitution, which is ideally instantiated at protocol inception and permanently stored. In order for a fork to be called fair - it must adhere to every clause in this section and every requirement specified in the protocol's Founding Constitution.

In this part we outline some principles that are applicable to all fair forks, and in the next part we outline the rationale for these principles. We then go on to describe the Founding and Refounding documents that must be provided by the original founders of a cryptonetwork and each refounder in a fair fork, respectively.

The principles are:

1. **State Persistence**: At the time of forking, state should be perfectly replicated between the fair fork and its parent.

2. **Refounding Proposal**: Every fair fork must declare a Refounding Proposal. The Refounding Proposal is a document provided by the refounders that outlines

   (a) A name for the forked network (during the refounding).

   (b) A detailed explanation of the proposed changes to the protocol.

   (c) A path and timelines for achieving these changes.

   (d) A reward in terms of new token issuance for the re-founders and developers of the fair fork.

   Parameter bounds and guidelines for the Refounding Proposal are set at the protocol-level by the Founding Constitution.

3. **Fork Resolution**: After a period specified in the Refounding Proposal, the Fork Resolution Score of the parent and the fair fork are compared. If the fair fork scores higher on this metric then it is deemed successful. This triggers **fork resolution** (see below).

4. **No Imitation**: When multiple fair forks are active at the same time, forks must not steal features or proposed upgrades from each other or signal that they intend to do so.

3.1.1 Fork Resolution

In the context of a fair fork, fork resolution refers to the event where the original name and ticker of the protocol and, in most cases, the utility of a protocol is subsumed into the fair fork upon its success. Further, a reward is likely unlocked for the refounders per the Refounding Proposal. Specifically, fork resolution has 3 potential components:

- **Name Resolution**: If the fair fork at the time of fork resolution performs better than the parent fork according to the Fork Resolution Score, then the fair fork attains the right to adopt the name of the canonical network. The parent fork's name will subsequently revert to its original name. If the parent was the root network, then it should be renamed in a 'classic' style – unless an alternate has been outlined in the original Founding Constitution.

- **Protocol Utility Resolution**: If it intends to do so, a fair fork must clearly outline a path for subsuming the utility of the original network into itself upon success. The re-founders must lay out in the Refounding Proposal their intentions with respect to this process, and provide a clear path to this "merging" as the fork draws closer to resolution.

- **Success Rewards**: A fair fork may have a portion of its re-founding rewards tied to the successful resolution of the fork.

After fork resolution is complete, the refounders' "term" as benevolent protocol dictators should be deemed by the community as terminated, as the refounding is complete. This returns the protocol to its default state of neutrality as regards community leaders.

3.2 Rationale

In this part, we provide a rationale for each of the Principles and show how their components compliment one another.

3.2.1 State Persistence

The requirement for state persistence naturally removes all state-resetting forks from consideration. There are three primary reasons why this is important:

- State-resetting forks do not preserve the utility of the network at inception, and hence lose community cohesion around the protocol.

- State-resetting forks lose established community incentives for maintaining a fork. These include incentives for miners to mine on the network and incentives for developers to build on it.

- Finally, state-resetting forks do not adequately reward parties that have contributed value to the network and time to the development of the prior fork.

3.2.2 Refounding Proposal

The Refounding Proposal is a document released by the re-founders at the time of forking that outlines their intended changes to the protocol, a path to achieving these changes, and tokens to be released as a development budget and rewards during the period of the refounding. Such a declaration is necessary to get community buy-in for adopting and building upon the proposed fair fork. The Refounding Proposal is explained in greater detail below (3.4).

Forking systems without re-founder rewards only make good governance financially lucrative for large stakeholders. Refounder rewards also create social cohesion around state persistence – refounders are no longer required to create a stateless fork in order to allocate themselves any tokens. Finally, these rewards create powerful incentives for entrepreneurially minded community members to improve or rejuvenate the protocol.

3.2.3 No Imitation Rules

When multiple fair forks are active at the same time, a no-imitation rule is necessary to prevent fair forks from potentially influencing and manipulating the resolution of forks not directly on their own path (see section 4 on Multi-fork resolution).

3.2.4 Fork Resolution

Fork resolution provides a mechanism to maintain long term community cohesion. The reasons behind each subcomponent of fork resolution are:

- **Name Resolution**: Reassigning names to successful fair forks keeps the canonical chain reference succinct. A successful fair fork is also considered as the 'correct path' for upgrading the main fork, per the Founding Constitution.

- **Protocol Utility Resolution**: Failure to include utility convergence can destroy value provided by the networks if that value is delivered after the resolution step. This effect arises as neither network would be able to guarantee mechanics after resolution. Further, without utility resolution, either branch of the protocol is likely to decline during forking due to uncertainty of the honoring of commitments made by it.

- **Success Rewards**: Some networks might choose to reward refounders in full or in part only in response to successful conversion to canonical network. This further incentivises community cohesion around protocol changes that are seen as beneficial to the vision of the protocol.

3.3 Founding Constitution

It's expected that each network will make its own specification of the fair forking social protocol and enshrine its guidelines and parameter bounds in a document called the Founding Constitution. The specifications and parameters to be provided by each implementing network in the Founding Constitution include:

- The Fork Resolution Score mechanism.

- Maximal re-founder reward rate (if applicable).

- Any and all other protocol specific limitations that refounders must abide by.

3.3.1 Fork Resolution Score

The Fork Resolution Score (FRS) is specified in the Founding Constitution and is used at the time of fork resolution to determine whether the fair fork is successful. This is a critical specification of the Founding Constitution because the Fork Resolution Score will guide the evolution of the protocol.

An interesting subclass of networks that adopt the fair forking protocol is those where the FRS is a function of the market capitalization of the protocol. Analogous to futarchy for DAOs [4], this potentially sets up a prediction market for the valuation of the protocol at the time of fork resolution. This incentivises Refounding Proposals that will ultimately increase the valuation of the entire network, and consequently its fundamental utility.

Fork resolution is done by comparing the FRS of both the parent network and the fair fork. If the FRS of the fair fork is strictly greater than the original fork, it is deemed successful. The FRS must:

- Be a concrete, numeric value.
- Be high resolution (the range of $\text{FRS}(f)$ must be large in order to prevent FRS collisions).
- Ensure that governance moves towards the protocol's original vision and purpose over time.

3.3.2 Maximal Refounder Reward Rate

Each Founding Constitution can optionally specify the maximal applicable re-founder reward rate. Setting a maximal refounder reward rate will likely influence the number of fair forks that will occur in a protocol's community at any one time. A lower cap of rewards per year will lead to a lower incentive to fair fork the protocol. These considerations are discussed further in section 5.

3.3.3 Protocol Specific Rules

The Founding Constitution may also specify a number of additional protocol-specific rules, atop the base fair forking guidelines. For example, the Arweave network's Founding Constitution details that each fair fork must include all of the data from the original canonical branch, omitting the case of severe protocol malfunction (accepting data without associated fee, etc).

Additionally, within this section, each protocol might also specify a path to updating the Founding Constitution itself.

3.4 Refounding Proposal

The Refounding Proposal should outline the vision and intended work to be undertaken during the refounding. Specifically, a refounding proposal must specify each of the following components:

3.4.1 Budget and Rewards Schedule

Each potential re-founder or refounding team of a fair fork, at the onset of the new protocol, specifies a structure for rewards and anticipated expenses. These are released in the form of new tokens that are created at the launch of the fair fork and allocated to the developers of the network, but released over time, according to a schedule provided in the same document. In any fair fork, there must be at least three considerations while specifying the refounding tokens.

- **Schedule of rewards:** The refounding proposal must outline the timeline of rewards that should be received by the refounders and associated team members. Typically, a significant proportion of these rewards should be released on or after the completion of the refounding. This ensures that the re-founders are incentivised for the full length of the refounding period. Notably, the higher the number of minted tokens during the refounding period, the greater the gain in network value will likely have to be in order to justify the value of the fair fork to the network.
- **Expenses:** In addition to rewards, fair forks will likely outline a budget in their Refounding Proposal that covers expenses that they anticipate will emerge. Optionally, these expenses can be denominated in a different currency than the fork's native token, such that stable capital can be assured during the refounding period.
- **Excess:** Fair forks may also outline a mechanism to utilize the excess tokens for the advancement of the ecosystem or burn them.

In all fair forks, the Refounding Proposal's budget and rewards schedules must abide by all of the stipulations and parameters specified in the protocol's Founding Constitution.

3.4.2 Protocol Utility Resolution

In protocols where this is possible, the refounders of a protocol must specify a way to resolve the utility of the protocol upon completion of the refounding. This means that, to the extent that it is possible, the fair fork shall absorb the utility of the parent fork. This specification must be outlined in the refounding proposal at the time of the fair fork, and detailed with more granularity in the period leading up to fork resolution.

Protocols with additive utility (such as Arweave, Livepeer, etc.) are likely to be able to merge a more complete representation of state than protocols with more conflicting state updates. We explore this further in the Discussion section of this paper.

4 Multifork Resolution

In this section, we walk through two instructive scenarios where there may be multiple fair forks active at the same time, and show how the resolution rules apply to preserve utility and canonical name of the protocol under various conditions.

4.1 Scenarios

4.1.1 Non-Crossing Multifork

Sometimes, fair forks may not overlap - i.e. new fair forks of a protocol might be resolved before older ones are considered for resolution. The diagram below gives an example of such a situation.

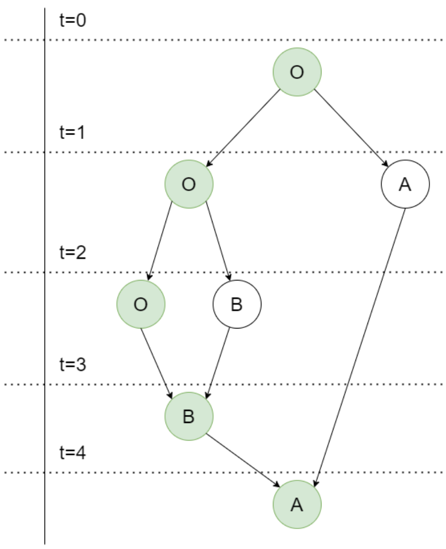

Figure 3: A non-crossing fork example. The green coloring indicates the fork possessing the canonical name

We consider two fair forks of the original network O.

- At time *t=0*, fair fork A is created
- At time *t=1*, fair fork B is created from the original fork O
- At *t=2*, there are three active forks - O, A and B
- At *t=3*, forks B and O are resolved - and B is deemed to be a successful fair fork as the FRS for B is higher than that of O. This causes B to subsume the utility and the name of the original fork O and become the 'canonical' fork.
- In the final time step shown here, *t=4*, forks A and B are compared and the FRS for A is higher than B. This causes A to subsume the utility of B, and adopt the name of the canonical fork.

4.1.2 Crossing Multifork

A second type of multi-fork resolution happens when active fair forks cross-over. This means that the original fork is compared with a previously created fair fork while a current one is in operation. Here is an example of how such a situation will progress.

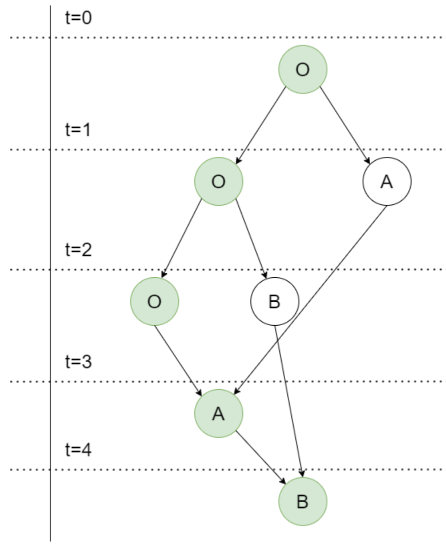

Figure 4: Crossing fork example

- At time *t=0*, fair fork A is created
- At time *t=1*, fair fork B is created from the original fork O
- At *t=2*, there are three active forks O, A and B
- At *t=3*, forks A and O are resolved - and A wins, becoming a successful fair fork. A subsumes the utility and attains the name of the original fork O and become the 'canonical' fork.
- In the final time step *t=4*, forks A and B are compared and the FRS for B is higher than A. This causes B to subsume the utility of A and adopt the name of the canonical fork.

4.2 Market Dynamics

In the case of token or market-cap related Fork Resolution Scores, a prediction market emerges for the value of the forks. As referenced earlier, in this case the fair forking social protocol creates a form of futarchy-based governance [4].

In this section we discuss strategies for navigating fair forks from the perspective of market participants.

4.2.1 Active Participants

Token holders and users of the genesis network can choose to speculate on the prominence of a fair fork over the parent network. This can be done by selling tokens of the network they believe is unlikely to win and buying the token of the other.

In Figure 3 above (non-crossing fair fork), consider the economic value of the tokens that have been minted. At the onset the original network O has a token supply of 100M. Upon creating the fair fork A, the re-founders decide to allocate 10M extra tokens to the themselves over a 4 “time-step” period. After a short-time, a different set of re-founders proposes a relatively minor change (over a smaller period of 2 time-steps) to the original network O and create the new fair fork - fork B. They allocate themselves a smaller mint of 5M tokens over the two-step timeperiod. Figure 5 shows the token supply over the course of the fair forks.

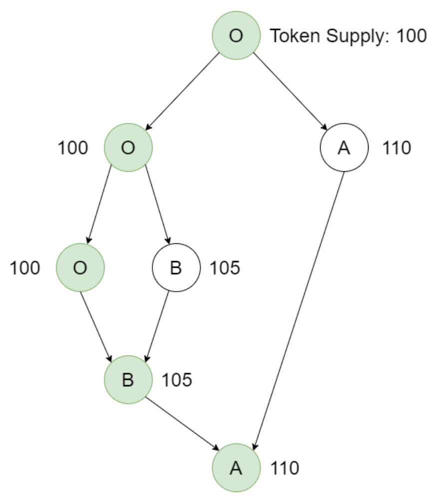

Figure 5: Non-Crossing multi-fork token supply

In this scenario, note that in the final time-step when B is pitted against fair fork A (which has already subsumed the parent fork), asset holders on the canonical network have 105M tokens of B being compared with 100M tokens as part of fair fork A. In such a situation, each holder of B tokens will evaluate whether the value of each of their A tokens will be atleast 5 percent higher than a similar quantity of their B tokens. If that is the case, they have an incentive to ‘defect’ to the other chain (A) and back its development and progress.

Such incentives to defect are particularly pronounced in cases where the FRS depends on the market cap of the fork. We expect that due to the Efficient Market Hypothesis [15] the market’s belief about the underlying fundamentals of each fork will eventually guide its development to increase the fundamental value of the protocol. Over time, this will lead to better fair forks with greater utility value-add upgrading the protocol.

4.2.2 Passive Token Holders

Asset holders in the original coin can choose not to partake in the fair forking governance protocols. They can buy and hold the token of the genesis network, and over time accumulate a basket of derivative tokens that potentially hold value. Further, other participants in the ecosystem are incentivised to increase the value of these basket of tokens.

Further, in Figure 5, the re-founders of B may have rewards that they have accumulated on chain B after its successful resolution over O, but the same re-founders do not have a proportionate stake in chain A. If they do not seek to participate in voting between chains A and B (in the future fork resolution), then their “passive hodling” strategy is to rebalance their holdings so that they have an equal quantity of both A and B tokens.

4.3 Feature Duplication

Again considering the example of Figure 3, it is important that at timesteps 2 and 3 - when all three forks are active - that the fair fork A not include (or even signal potential inclusion of) any features from B. If this is not the case and the refounders of A decide to copy features from B, then this has the potential to impact the resolution between O and B. When the FRS is linked to community participation or market capitalization, the community may have no incentive to back the current fair fork (and reward re-founders of B by diluting their own tokens) if all the features of this will be included in the next resolution, between O and A.

4.4 Naming Considerations

In the case where a fork is ‘temporarily canonical’, for example in Figure 3 - where B is temporarily the canonical fork between timesteps 3 and 4- it must revert to its original name upon a subsequent ‘loss’.

Specifically, in the same example, say the original network O is named AR (for Arweave). Fair fork B upon success is granted the name and ticker for AR, while the original network O is deemed AR-Classic. In the next face-off between forks B and A, A succeeds to acquire the canonical name of AR. In such a situation B must go back to adopt its name and ticker before its resolution with O. That is, it does not gain the right to be called AR-Classic (despite having previously been successful over the chain now called AR-Classic).

5 Discussion

5.1 Maximal Refounder Reward Rate

The maximal re-founder reward rate is specified in the Founding Constitution by the founders of the protocol.

This is a percentage that represents the proportion of tokens that may be minted per year that the fork is underway.

A greater (maximal) reward incentivises more fair forks. Over a long enough time line, more forks should lead to a more robust, higher quality protocol. However in the short term, more forks may also lead to a more chaotic environment for users of the protocol and potential division within the community.

5.2 Fork Resolution Failure Scenarios

Fork resolution failure might occur when the community does not accept a 'successful' fair fork as the canonical fork upon resolution. This factor arises because every ecosystem participant is left to adjudicate their fork's compliance with the rules by themselves. Rule clarity in the Founding Constitution will be proportionate to fork resolution failure probability. This is because ambiguity in the resolution rules leads to a higher likelihood that ecosystem participants will disagree with the outcome. Multiple fork resolution failures will erode confidence in the ability of the protocol to be upgraded and maintained over time. In particular, the adjudication mechanism for the 'no-imitation rule' is of particular concern as highly incentivised re-founders may find innovative ways to circumvent this rule.

5.3 Trademark Law and Naming

One of the implications of fork resolution is that upon success, a fair fork acquires the name of the parent network. It may be possible to legally bind the owner of the trademark to adhere to the fork resolution decision. In situations where a trademark has been registered, this is the gold standard for any protocol seeking to follow the fair forking guidelines specified in this paper.

5.4 Fair Forking Protocol Mutability

While this paper outlines the first complete version of this protocol, there may be a need to change the fair forking social protocol at a future date. This could be done by building social consensus around changes to this protocol.

5.5 Utility Resolution Applicability

A major component of fair forks that drives community cohesion in contrast to traditional hard forks is the protocol utility resolution mechanic. In cases where the state and utility provided by a protocol is additive (such as Bitcoin, Arweave and Livepeer), utility resolution is relatively straightforward to reason about.

However, in cases where protocol state is not additive, the Founding Constitution must outline clear paths to resolution. For example, in state-computation based networks like Ethereum and Solana - it may be possible to include newly minted contracts and states on the original network from the time of the fair fork, but conflicting updates could be dropped during the fork resolution. In such networks, it is not clear how dApps building on one-chain will port over to successful fair forks.

5.6 Usage Disadvantage

In the design of the fair forks proposed here, we note that the fair forked chain, prior to resolution is likely to be at a disadvantage with respect to usage and community adoption. This is because while upon success, the fair fork will subsume the utility provided by the parent fork, the reverse is not true - the parent fork is not required to absorb the utility of a fair fork that is not promoted to the canonical name.

Moreover, the adoption of the fair fork will depend on a number of factors including incentives for bootstrapping and the relative network/hashrate share of the fair fork might be smaller than the original network in the early stages.

As a result, any fair forks is at an inherent disadvantage to the original protocol from a community and adoption point of view, and it might be given an adjustment during score comparison. This could be done by adding a *disadvantage coefficient* for the fair fork while calculating the FRS, or setting up an FRS that does not correlate directly with present adoption.

This is an area where we believe more consideration is required in order to come to a definitive recommendation.

6 Conclusion

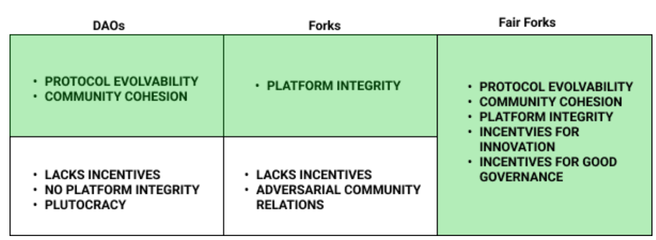

Figure 6: Fair Forks vs DAOs and Forks

In this paper, we have examined several benefits and drawbacks pertaining to existing models of blockchain network and protocol governance. While these forms of organization as they are currently deployed today have several desirable properties, we find that the design and inertia inherent in these systems means that they are unable to simultaneously achieve the required properties for good governance.

With the fair forking social protocol proposed in this paper, we have aimed to provide a path forward for blockchain governance that combines the platform integrity guarantees of traditional forks with the protocol adaptability benefits of DAOs. Further, fair forks add a crucial missing incentivization layer for re-founders of a protocol and optionally, incentives for the market to optimize for good governance and value creation for the protocol.

Provided the rewards of fair forking are sufficiently tuned, entrepreneurs and founders will choose to re-found existing protocols to improve upon them rather than undertake the expensive and wasteful expense of bootstrapping new cryptonetworks. All blockchain-based protocols looking for a viable long-term solution to the problem of protocol governance and rejuvenation may wish to consider **fair forks** as an alternate form of governance.

References

[1] *Average Net Worth of Americans.* URL: https://www.cnbc.com/select/average-net-worth-of-americans-ages-65-to-74/.

[2] Avyan. "Curve Wars and the Emergency DAO". In: (). URL: https://coinmarketcap.com/alexandria/article/curve-wars-and-the-emergency-dao/.

[3] *Building and Running a DAO: Why Governance Matters.* URL: https://future.a16z.com/building-and-running-a-dao-why-governance-matters/.

[4] Vitalik Buterin. "An Introduction to Futarchy". In: (2014). URL: https://blog.ethereum.org/2014/08/21/introduction-futarchy/.

[5] Vitalik Buterin. "DAOs, DACs, DAs and More: An Incomplete Terminology Guide". In: (Aug. 2014). URL: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/.

[6] Vitalik Buterin. "Moving beyond coin voting governance". In: (2021). URL: https://vitalik.ca/general/2021/08/16/voting3.html.

[7] *Compound Governance Overview.* URL: https://compound.finance/governance.

[8] "Cosmos' Founding Team Broke Up Early This Year. The Project Didn't". In: (Aug. 2020). URL: https://www.coindesk.com/business/2020/08/10/cosmos-founding-team-broke-up-early-this-year-the-project-didnt/.

[9] *Curve fees.* URL: https://curve.fi/rootfaq.

[10] Frank A. Farris. "The Gini Index and Measures of Inequality". In: *The American Mathematical Monthly* 117.10 (2010), pp. 851–864. ISSN: 00029890, 19300972. URL: http://www.jstor.org/stable/10.4169/000298910x523344.

[11] Ellen Guo. "Governance Theatre - Starring DeFi". In: (Sept. 2021). URL: https://ei-ventures.medium.com/governance-theatre-starring-defi-a44023abab8a.

[12] "Hard Forks, Soft Forks, Defaults and Coercion". In: (Mar. 2017). URL: https://vitalik.ca/general/2017/03/14/forks_and_markets.html.

[13] Colin Harper. "New Gnosis Dao Bets on 'Futarchy,' a Prediction-Market Governance Model". In: (Nov. 2020). URL: https://www.coindesk.com/tech/2020/11/23/new-gnosisdao-bets-on-futarchy-a-prediction-market-governance-model/.

[14] Emin Gun Sirer Ittay Eyal. "Majority is Not Enough: Bitcoin Mining is Vulnerable". In: (2013). URL: https://www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf.

[15] Andrew W. Lo. "Efficient Market Hypothesis". In: (Aug. 2015). URL: https://alo.mit.edu/wp-content/uploads/2015/08/emh2007.pdf.

[16] Messari. *Sushiswap history and Overview.* URL: https://messari.io/asset/sushiswap/profile.

[17] *Olympus DAO Governance Forum.* URL: https://forum.olympusdao.finance/.

[18] *Polkadot Wiki-Governance.* URL: https://github.com/paritytech/polkadot/wiki/Governance.

[19] *Proposal for Uniswap Fee Reduction.* URL: https://gov.uniswap.org/t/proposal-flip-the-protocol-fee-switch-for-uniswap-dev-team-and-uni-holders/4777.

[20] Fabian Schär. *Blockchain Forks: A Formal Classification Framework and Persistency Analysis.* Feb. 2020. DOI: 10.13140/RG.2.2.27038.89928/1.

[21] Sebastian Sinclair. "Uniswap's First Governance Vote Ends in Ironic Failure". In: (). URL: https://www.coindesk.com/tech/2020/10/20/uniswaps-first-governance-vote-ends-in-ironic-failure/.

[22] *Tezos Governance Overview.* URL: https://wiki.tezosagora.org/learn/governance/tezos-governance-overview.

[23] *Uniswap Governance Homepage.* URL: https://gov.uniswap.org/.

[24] Eugene Wei. "Platform Risk". In: (). URL: https://www.eugenewei.com/blog/2015/3/14/platform-risk.