Fair Forks: Towards Incentivized Protocol Governance

Sam Williams
sam@arweave.org

Abhav Kedia
abhav@arweave.org

October 13, 2022

Abstract

In this paper we introduce Fair Forks, the first step towards a form of fork-based futarchy. In this system, 'refounders' are rewarded for implementing protocol upgrades, which are adjudicated for acceptance via a market mechanism. Through fair forks, market participants are incentivized to vote in favour of proposed upgrades that increase net protocol value by buying or selling tokens associated with proposed upgrades of the protocol. Collectively, this system rethinks protocol governance as a pro-social, incentivized and market-based process, rather than a risk-center arising from a tragedy of the commons. Despite possessing a number of significantly beneficial properties, Fair Forks in their current design fall short on a few key aspects: they introduce high volatility in protocol value and create uncertain conditions for dependent applications during the refounding process.

Before describing Fair Forks, we first examine existing protocol governance mechanisms. In particular, we focus on traditional blockchain forks and DAOs, including a number of real-world examples. We observe that while these mechanisms create protocol adaptability, they do not encapsulate incentives for governance participation or, in the case of forks, even continued community cohesion.

In the process of outlining Fair Forks, this paper contributes a new model to describe the often precarious linkages between blockchain networks and their names.

Although we do not plan deployment of this mechanism as currently formulated, we present it here along with broader insights regarding protocol governance, for analysis and to serve as a stepping stone for future work and improvements.

1 Introduction

In this paper, we detail a constitution-based approach to protocol governance. This mechanism builds on the natural "forking" governance structure of blockchain networks to enable the following properties:

- Non-coercive upgrades to the protocol.
- Permissionless and incentivized innovation.
- Preservation of community cohesion through periods of protocol change.

Rather than operating at the technical layer, this new mechanism creates an overarching *social* protocol for governance of networks by establishing a concrete link between a protocol's name and the network of computers that constitute its canonical instantiation.

We observe that a social system for definitively resolving the name of a protocol to the network of computers and shared state to which it refers has been ill-defined in the first decade of blockchain deployment. This ambiguity has led to a number of high-impact protocol crises with great uncertainty about the version of the network deemed "canonical". Consider the case of Bitcoin, where the prominent blockchain news website "Bitcoin.com" repeatedly referred to the network we now know as "Bitcoin Cash" as the canonical fork of "Bitcoin" for a period of time between 2017-2018 [5]. Further, at the time of writing this paper, the *r/btc* sub-reddit still referred to Bitcoin Cash as "Bitcoin", despite its 3-letter name being the ticker for the canonical Bitcoin network.

In the case of Ethereum, the reversal of the "DAO Hack" led to contention surrounding which version of the chain is appropriate to call "Ethereum". This crisis was largely resolved by the decision of the Ethereum Foundation to support the forked version of the protocol as the canonical one, exemplifying the outsized influence of a conventional centralized institution in the governance of a "decentralized" protocol [28, 10].

The ill-defined linkage between name and network opens a dangerous pathway to reduced social cohesion in decentralized communities. Specifying such a link is particularly important in blockchains, where in case of forks and upgrades each stakeholder must independently assess *which* network is the valid chain. We specify a pathway to create deliberately engineered social linkages between the names of blockchain protocols to their concrete instances. Further, we utilize such linkages to create a pro-social and well incentivized governance mechanism for the protocol.

Despite their beneficial properties, we do not intend to deploy the Fair Forking social protocol in their current form. We provide examples of potential failure scenarios in the current design, and suggest pathways for future exploration that improves on it.

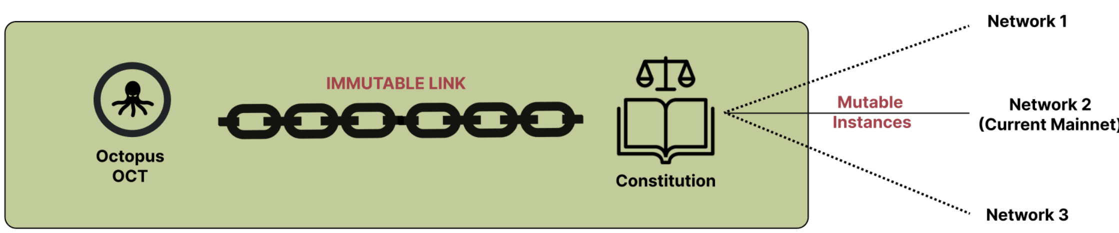

Figure 1: A (fictional) Octopus Protocol and its concrete instantiations

1.1 Desirable Governance Properties

We begin by considering desirable properties for protocol governance mechanisms. For healthy long-term governance of cryptonetworks and decentralized protocols, we propose the following characteristics as desirable:

- **Platform Integrity:** There should be protocol-level assurances that the platform will not change its rules of engagement for users, developers and service providers. In cases where there must be breaking changes to the protocol, a previous unchanged version of the protocol must exist for continued use, if desired by stakeholders of the network. This property is explored in greater detail 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 be effective stewards, steering the protocol towards its goals.
- **Community Cohesion:** Community members should have an incentive to work together to improve the protocol, instead of protocol upgrades leading to contention and fracturing stakeholder relations.

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 2.

Notably, the above is only a high-level summary of protocols that employ 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 broadly instructive to analyze existing protocols from this perspective.

1.2 Table of Contents

This introductory section laid out the frame of analysis used to explore the properties of blockchain governance systems and provided a brief preview of the novel Fair Forking social protocol. The rest of this paper is organized as follows:

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

Figure 2: Existing Governance Mechanisms

- In section 2, we provide a deeper examination of governance structures and incentives in DAOs and forks.
- In section 3, we formally introduce **Fair Forks**, a social protocol that incentivizes good long-term governance of a protocol without introducing the drawbacks identified with DAOs and forks.
- In section 4, we outline potential governance scenarios for networks that employ the fair forking protocol.
- In section 5, we outline drawbacks with the current design, and explore the consequences of a protocol-wide futarchy implemented between active networks.
- In the final two sections, we explore extensibility and applicability in generalized blockchain settings, along with tradeoffs and implementation decisions and conclude with a summary of existing and proposed governance systems.

2 Current Governance Mechanisms

In this section we discuss the benefits and pitfalls that arise from the traditional mechanisms of blockchain governance; DAOs and forks.

2.1 DAOs

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

2.1.1 Definition

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

- Exists inside a decentralized network.
- Is implemented by code (automation) at its core, and influenced by real-world actors (individuals and organizations).
- Contains an internal allocation of power that is used to determine voting rights in decisions concerning (among other things) modifications of the protocol. This allocation is often (but not always) maintained via a governance token.

This definition of DAOs is in line with the one commonly used in the Ethereum community[8], but also elsewhere in the crypto ecosystem.

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 ConstitutionDAO and PleasrDAO [20, 27, 11]. Further, under the above definition, we note that mutable-blockchain networks such as Polkadot and Tezos meet the necessary criteria to be regarded as DAOs [21, 26].

2.1.2 Benefits and Drawbacks

In this section, 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 changes in a decentralized setting while typically also maintaining community cohesion. In addition, DAOs enable collective asset ownership, management and curation [6]. Unfortunately, many DAOs today re-introduce a number of problems that plagued the centralized platforms of the web2 era. In fact, DAOs behave like companies in that they enforce coercive updates and gravitate towards value extractive behavior as a result of their token-weighted governance structures. More precisely, some of the problems with existing DAOs include:

I. Breaking Platform Integrity

The services rendered by DAO-governed protocols are not immutable and can subsequently break platform integrity – assurances that the platform will not change their rules of engagement. The history of web services is rife with examples of companies modifying their product and breaking platform integrity guarantees [29]. 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's mechanics will change.

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

Another example of DAOs breaking platform integrity guarantees is highlighted by fee changes in DeFi protocols. This has happened with liquidity pool fee structures in many protocols (including Curve [13], Uniswap [22], 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 shows extremely high Gini coefficients for governance [14]. Among Compound, Uniswap, Sushiswap and Yearn, it was found that just 2-7 voters decide the outcome of every governance proposal [15]. Notably, this number is even lower than the board size of many large traditional technology firms [25].

III. Lack of Incentives for Good Governance In the ideal case, protocol governors would be rewarded proportionally to the net utility of their governance activities.

Unfortunately, DAOs do not normally provide financial rewards to participants who vote in favor of measures that are eventually perceived as pro-social. Most DAOs, in fact, do not even reward participants for engaging with the governance process at all. The voter apathy that emerges from this is further compounded by the Pareto distribution of governance-tokens. The result of this distribution is that the long-tail of DAO participants – even if they wanted to – have little impact on governance decisions, while on the other-end, a wealthy minority (which often has non-trivial conflicts of interest) can make decisions that are sub-optimal for the protocol itself [13] [**defi-education-fund-uniswap**]. These issues can be delineated as follows:

- Few governance participants. Frequently, protocol governance proposals fail because of insufficient voter turnout, demonstrating that token holders have little incentive to participate in governance. [24, 1].
- Large participants may have conflicts of interest in

the governance of the protocol. Lack of direct reward/punishment for the quality of governance decisions 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 [3, 9], in which governance participants are openly bribed for voting in a certain way.

- 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 [12].

Some experiments in incentivised DAO-based governance are indeed underway [7, 17], 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 their ownership in the DAO has some value - their DAO Ownership Value (V), and some amount of Net Assets (outside the DAO), then their financial incentive can be modeled in approximately the following fashion:

$$Incentive(i) = \frac{V_{dao}(i)}{V_{dao}(i) + NetAssets}$$

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

$$V_{dao}(x) = \frac{MarketCap}{Members}$$

As a result, the number of people that the DAO can likely command the attention and focus of is:

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

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 [2], 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 [23]:

- **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 [18]. 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 [16]:

  - *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

> "I wanted to point out that hard-forks are very disruptive to markets. They are disruptive to merchants, to markets, to entire ecosystems."[4]
> –*The Block Size War*

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" [19].

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 value that prior contributors (via skills or financial investments) have made to the protocol so far.

III. Forks Encourage 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 forking is a social protocol that captures the adaptability benefits of DAO-based governance, while maintaining platform integrity guarantees offered by traditional blockchain fork-based governance.

A **fair fork** refers to any hard fork of a protocol that abides by all the Principles outlined in this paper and all the guidelines specified by the original creators of the protocol in its **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.

Any fair fork is, therefore, fully specified by a combination of 3 documents:

- Principles as defined in this paper.
- Founding Constitution as defined by a protocol's founders.
- Refounding Proposal as provided by developers of the fair 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 Principles, the Founding Constitution and their own Refounding Proposal. Figure 2 below shows the major pieces involved in a fair fork.

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.

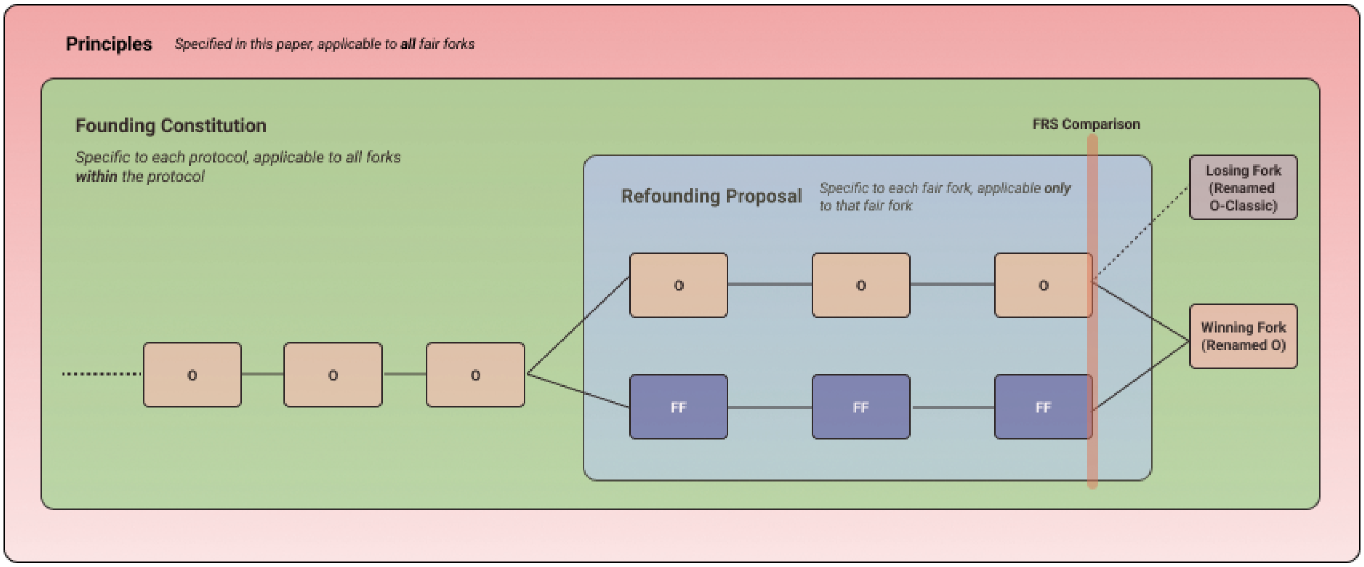

Figure 3: Fair forks

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.

3.1 Principles

We now outline the principles for fair forks.

The principles are:

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

2. **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).

3. **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.

These principles are applicable to all fair forks, and protocols implementing fair forking will additionally specify their own instantiation of the fair forking protocol in a Founding Constitution– a document that is ideally created at protocol inception and permanently stored. Fair forks must also abide by every requirement specified in the protocol's Founding Constitution (see §3.3).

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.

- **Utility Preservation**: 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.

In this part we have outlined principles that are universally applicable to all fair forks. 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.

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 prevents all state-resetting forks from being considered fair forks. 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 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 a successful upgrade and "heir" to the name of the main fork.
- **Utility Preservation**: 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 calculation.
- 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 [7], 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 collision resistant (high resolution) - it should be improbable for two distinct network to have the same FRS.
- Ensure that governance moves towards the protocol's original vision and purpose over time.

3.3.2 Maximal Refounder Reward Rate

A Founding Constitution might optionally specify the maximal applicable re-founder reward rate for fair forks of its protocol. 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 §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 Octopus protocol's Founding Constitution might state that each fair fork must include all of the transactions from the original canonical branch, omitting the case of severe protocol malfunction.

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 Preservation

In protocols where this is possible, the refounders of a protocol must specify the mechanism that will be used to preserve the utility of the protocol upon completion of the refounding. This means that, to the extent that it is possible, the winning 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 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 Fair Forks by Example

Here, we consider the example of a fictional bitcoin-like protocol called Octopus (OCT) that implements the Fair Forking mechanism and hence specifies a founding constitution. As well as specifying the immutable characteristics of the protocol, the Octopus constitution adopts a market-capitalization based FRS.

Under such a constitution, this section outlines some (hypothetical) fair forking scenarios to illustrate the expected progression of events.

4.1 Scenario: Octopus-FastBlocks

Suppose that an observation has been made within the Octopus community – 99% of blocks occur without a fork. Some enterprising members subsequently propose lowering block confirmation time from its current 20 mins to 4 minutes. It is almost uniformly agreed in the community that such a fork would be beneficial to lower practical confirmation times for users without sacrificing tangible security.

Subsequently, a fair fork is proposed to mint a small reward – 0.05% of the token supply – and a variable budget (upto 0.05%) on top of existing token supply to implement, deliver and market this change. The refounding proposal is released, and 2 weeks later a hard fork is generated, duplicating the network's state. The refounders embark upon a research, development and marketing campaign demonstrating the safety and efficacy of the new fork.

4.1.1 Market Behaviour

Interested exchanges see an opportunity to generate fees by offering a pair that trades this new token OCT-FB (Octopus-Faster Blocks) against the current OCT token.

Market participants are faced with three choices:

- Those uninterested in protocol governance or unsure about which fork is preferable will remain "neutral", not buying or selling either token on the exchange. Since the fork replicates state of the original Octopus network, they now have the same amount of new OCT-FB tokens as their original OCT balance.
- Those that are optimistic about the efficacy of the new upgrade notice that the rest of the community is likely to eventually coalesce around this new upgrade and therefore, sell some of their OCT tokens for OCT-FB, raising the value of OCT-FB relative to OCT. By increasing their proportion of OCT-FB tokens in this way, they are also increasing the value of their tokens upon success of the fair fork.
- A third set of market participants may be skeptical of the new version of the protocol and see an opportunity to sell OCT-FB tokens to gain more OCT, as they believe that the community will eventually reject the proposed upgrade.

Notably, the optimistic and skeptical participants are heavily economically incentivized to educate the market about the advantages of their favored network. That is, after believing that they understand something about the asset that others have not yet accounted for (gaining asymmetric knowledge advantage), market participants are incentivized to take a position and then attempt to lessen their own information asymmetry by educating others about their observations. After lessening this advantage, the market should appropriately price the asset accounting for this new information, and in this process economically reward the purveyor of this knowledge. In fair forks, we anticipate that this lessening of information asymmetry will lead to increasingly well-informed protocol governance.

As the fair fork draws to a conclusion (nears the time of fork resolution), there's likely to be "flocking" behaviour as people see which fork is expected to win and whether the new upgrade will resolve successfully. This flocking behaviour will likely tend the price of one token higher while reducing the value the other, making the resolution of the fair fork clearer.

4.1.2 Resolution

In case the fork succeeds, fork resolution is triggered, i.e., the upgraded protocol adopts the canonical Octopus name and "OCT" ticker. Exchanges, market participants and community members henceforth refer to this successful upgrade as the Octopus network.

New tokens (specified in the Re-founding constitution) are also minted to reward the founders and subsidize the replication of data from the old to the new chain. This last mint occur regardless of whether the fair fork succeeds or fails in resolving to the original network.

After this fork resolution event, the re-founders return to their role as community members, and are not required to be critically involved in future protocol upgrades.

To conclude this example, here is a list of things that will have happened with this hypothetical fair fork:

- The community reached an indicative conclusion that there is value to be gained for the protocol by decreasing block time, without affecting security of the network.
- New founders were incentivized to make the changes and advocate for the proposal publicly.
- A new set of tokens on the new chain "Octopus-FastBlocks" was created that will have value if the chain is useful.
- Active market particpants have been rewarded for engaging in protocol governance and advocacy for the outcome they deem to be most prosocial.
- In the case of a successful fair fork, the value of the protocol has increased to a greater degree than the dilution induced by the newly minted tokens as part of budget and rewards.
- Refounders have been released from their position as protocol leaders and the protocol has been updated and returned to a steady state.

5 Fair Fork Limitations

Fair forks seem to provide us with all of the desirable governance properties that were outlined in Section 1. However, the authors do not intend to deploy this in its current form. This section outlines the current limitations of the Fair Fork design and the following section describes potential avenues for overcoming these issues.

5.1 Extreme Volatility in Protocol Value

When the Fork Resolution Score is the full market capitalization of the network, the active forks of the protocol can expect to see increased volatility in their token price, especially as the fair fork nears the time of decision. Even in the case of a successful upgrade to the protocol (a fair fork that wins upon FRS comparison), the original fork's value just before the fork resolution drops to near-zero.

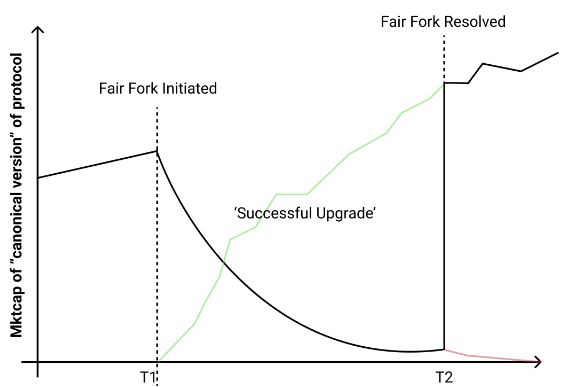

Figure 4: Price Volatilty in a Successful Upgrade

Upon successful resolution of the fair fork, the forked network acquires the name and ticker of the original network, whose value had dropped to nearly zero shortly before. This resolution mechanism would lead to extreme instability and uncertainty in the community and markets surrounding a protocol.

5.2 Uncertainty for Dependent Applications

During a refounding users, applications and smart contract platforms building on top of the protocol could face uncertainty pertaining to fluctuating token price and lack of clarity on which fork will ultimately be adopted. They have two likely strategies during a refounding:

- Replicate transactions on both networks. This requires duplicating work, and for smart contracts in particular, the environment on both chains might be different.
- Continue to upload transactions to the original network until (at least) fork resolution. In case of a successful fork resolution, applications will have to "port" their state from the current network on to the new network.

Both strategies require handling of edge cases and potentially non-deterministic behaviour.

5.3 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 potentially arises because every ecosystem participant is left to adjudicate their fork's compliance with the rules by themselves. Rule clarity in the Founding Constitution would 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. Fork resolution failures would erode confidence in the ability of the protocol to be upgraded and maintained (under a given Founding Constitution) over time.

6 Alternatives to Fork Resolution

Most of the limitations outlined above occur due to the third requirement of fair forking principles - that of Fork Resolution. In particular, the existence of two forks at the same time in the protocol and the linkage of each of their token prices to the utility and health of the networks means that the volatility induced by a decision market can lead to unpredictable behaviour.

One alternate design for fork resolution might position the decision point *before* the fork has actually taken place.

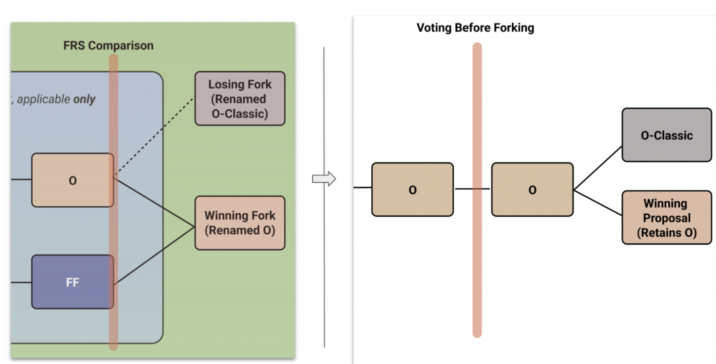

Figure 5: Decision After and Before a Fork

This could potentially be achieved by the creation of a bonding curve (either in protocol or via smart contracts) that leads to a payout of tokens of the forked network in case of success. A part of the refounding budget may be allocated to this decision (say 25%). Subsequently, if the upgrade fork mints 100,000 OCT-FF as part of the refounding budget, 25,000 OCT-FF will be reserved to pay to governance participants that own tokens in the bonding curve contract. A simple futarchy is then created by initializing the bonding curve contract to represents the tokens of the forked network and a maximum supply of 25,000 tokens. If the final price of this token is higher than the price of OCT (adjusted for a time-lock discount), then the fork is deemed victorious, and holders of the contract tokens are released tokens 1:1 from the 25,000 locked OCT-FF tokens.

This proposed alternative also has limitations, for example allowing wealthy malicious actors to buy out the entire supply of the decision token for a (relative to total protocol value) cheap price, subverting the protocol's governance. We believe that further work must be undertaken to truly understand the costs and trade-offs of properly implemented futarchies.

Relative to this bonding curve system, we observe that fair forks are capable of using the full market capitalization of the protocol as economic defense against manipulation. We hypothesize that all governance protocols that have equal or greater economic governance security will in some form resemble fair forks – particularly, that they will inherit the price instability issues of the fair forking system.

7 Discussion

Here we outline possible considerations that arise in the implementation and design of fair forks, and suggest directions for future exploration.

7.1 Naming Considerations

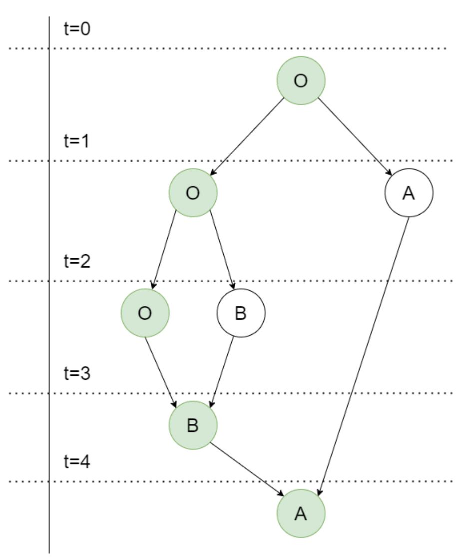

Figure 6: A non-crossing fork example. The green coloring indicates the fork possessing the canonical name

In the case where a fork is 'temporarily canonical', for example in the above figure– 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 OCT (for Octopus). Fair fork B upon success is granted the name and ticker for OCT, while the original network O is deemed OCT-Classic. In the next face-off between forks B and A, A succeeds to acquire the OCT ticker. 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 OCT-Classic (despite having previously been successful over the chain now called OCT-Classic).

7.2 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 more competition for governance. This is akin to many parties united in their patriotism to the nation but differing in ideology competing for government.

7.3 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.

7.4 Utility Preservation 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 and Livepeer), utility resolution is easier 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 yet defined how dApps building on one-chain will port over to successful fair forks.

7.5 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

DAOs	Forks	Fair Forks
• Protocol Evolvability • Community Cohesion	• Platform Integrity	• Protocol Evolvability • Community Cohesion • Platform Integrity • Incentives for Innovation • Incentives for Good Governance
• Lacks Incentives • No Platform Integrity • Plutocracy	• Lacks Incentives • Adversarial Community Relations	• Extreme Volatility in Protocol Value • Uncertainty for Dependent Applications

Figure 7: Fair Forks vs DAOs and Forks

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.

7.6 Empty Forks

Community members will want to watch out for fair forks that spend a significant amount of effort (and refounding budget) on marketing, while making minimal improvements to the core protocol itself.

This factor is of special importance where the FRS is dependent on the "memetic prominence" of the network, such as market capitalization.

7.7 Meme Fortification

Over time as a protocol evolves through the fair forking specification, elements of the original network and purpose might be lost. Protocol founders can preserve this mission (and the "meme" of the protocol) by specifying minimum safeguards that all implementing fair forks should abide by in the Founding Constitution. This helps in "fortifying" the original meme and mission of the protocol upon evolution.

It is important that this fortification be in the clearest possible words, failing which it might be difficult to adjudicate whether fair forks fall within this category.

8 Conclusion

In this paper, we have examined several benefits and drawbacks pertaining to existing models of blockchain protocol governance. While these forms of organization 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 described in this paper, we have aimed to provide the first step towards 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 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 task of bootstrapping new cryptonetworks. We present this mechanism as the first milestone on a path towards more appropriately designed, reasoned and incentivized blockchain protocol governance.

References

[1] 0xdeniz. "Improving governance participation rate at MakerDAO". In: (2021). URL: https://forum.makerdao.com/t/improving-governance-participation-rate-at-makerdao/11706.

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

[3] Avyan. "Curve Wars and the Emergency DAO". In: (2021). URL: https://coinmarketcap.com/alexandria/article/curve-wars-and-the-emergency-dao/.

[4] Jonathan Bier. *The Blocksize War: The battle for control over Bitcoin's protocol rules*. 2021.

[5] Bitcoin.com. "Public Service Announcement". In: (2018). URL: https://web.archive.org/web/20181122191203/https://www.bitcoin.com/public-service-announcement.

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

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

[8] 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/.

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

[10] Vitalik Buterin. "Onward from the Hard Fork". In: (2016). URL: https://blog.ethereum.org/2016/07/26/onward-from-the-hard-fork.

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

[12] "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/.

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

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

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

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

[17] 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/.

[18] 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.

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

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

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

[22] *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.

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

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

[25] Spencer Stuart. "US 2021 Spencer Stuart Board Index". In: (2021). URL: https://www.spencerstuart.com/-/media/2022/january/techbi2021/technology_board_index_2021.pdf.

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

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

[28] Paul Vigna. "The Great Digital-Currency Debate: 'New' Ethereum Vs. Ethereum 'Classic'". In: (Aug. 2016). URL: https://www.wsj.com/articles/BL-MBB-52061.

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