DELPHI DIGITAL

Insights: CryptoEvolution

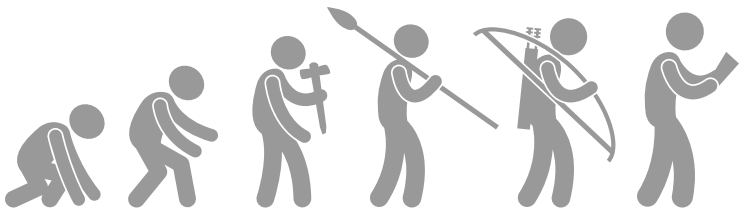
February 2019
85 Broad Street
New York, NY, 10004
www.delphidigital.io

Lead Analyst

Tom Shaughnessy was the founder and lead crypto analyst at 51percent Crypto Research before merging and becoming a part of the Delphi Digital team. Tom focuses on providing institutional crypto research spanning extensive reports on specific projects to unbiased thought pieces on the industry for analysts, hedge funds, family offices asset managers and investors. Tom also hosts the company's research podcast which features top founders of major projects. Prior to 51percent, Tom was on the cloud and communications equity research team at Oppenheimer. Tom graduated with a B.S. of Finance and holds his Series 7,63,86 and 87 licenses. Tom also host's Delphi's official research podcast, *Chain Reaction*.

Executive Summary

CryptoEvolution is necessary for survival



Introduction

Any system that wants to be here tomorrow has to be constantly evolving today. This encompasses plants, humans and even companies like Facebook or assets like cryptocurrencies. In this report we introduce the concept of CryptoEvolution; one of the driving factors behind whether or not a platform will survive and thrive or drift and die.

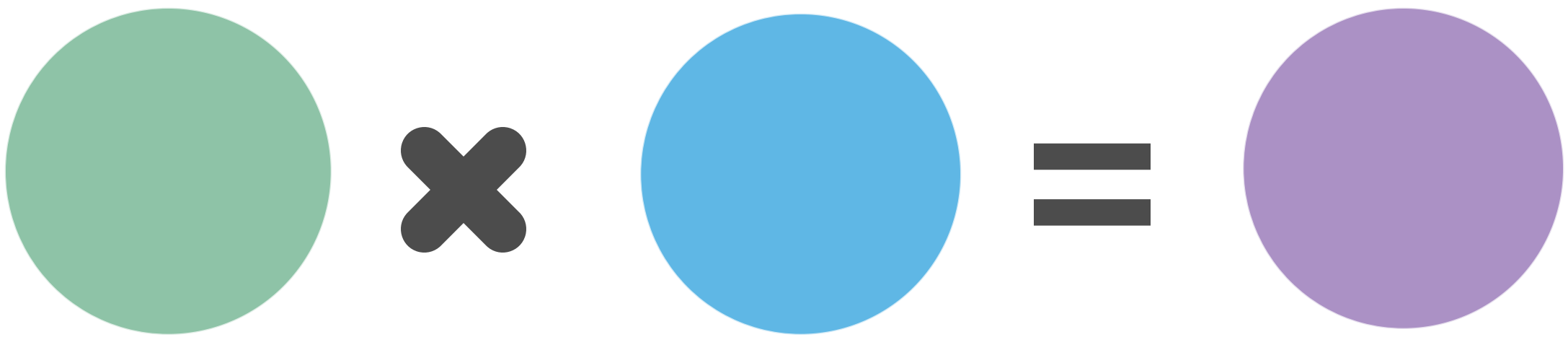
We believe this will help all stakeholders (developers, investors, analysts) select viable protocols, and weed out those which aren't fit for the future.

CryptoEvolution Formula

The ability for a project to evolve, is critical for its success over time. There are many types of projects in the space ranging from cryptocurrencies (Bitcoin, Decred, Litecoin), Public Smart Contract Platforms (Ethereum, Tezos, EOS) and private blockchains (AWS, Azure) and all are subject to the grinding market forces that require these platforms to adapt, or die.

The CryptoEvolution formula we introduce is based upon two variables. The first variable of the formula is the presence of a killer community, or a well-researched, global base of developers who are able to research upgrades and properly code them into worthwhile upgrades.

The second variable is an actual way to implement changes to a platform. This may sound easy, but it is extremely hard to enact changes on some platforms.



Breaking Down The Variables

For example, in Bitcoin, one would have to convince the entire global base of nodes (10,000+) to run a certain software implementation. Whether it be a maintenance upgrade, or a contentious change, it can become insurmountable to signal an upgrade and attract enough interest (nodes and miners) to enact a change in real time, with enough support to protect the network from a security standpoint. We note this is a feature of Bitcoin in our opinion (the inability to easily change) but this could have dire implications over the long term if changes are necessary.

On the first variable, the “strength” of a community is a subjective and vague metric, but there are areas where we can glean insight into the competence of a community. While we focus on developers here, a vibrant community requires stakeholders of all type beyond developers, these parties span normal businesses to retail investors and researchers.

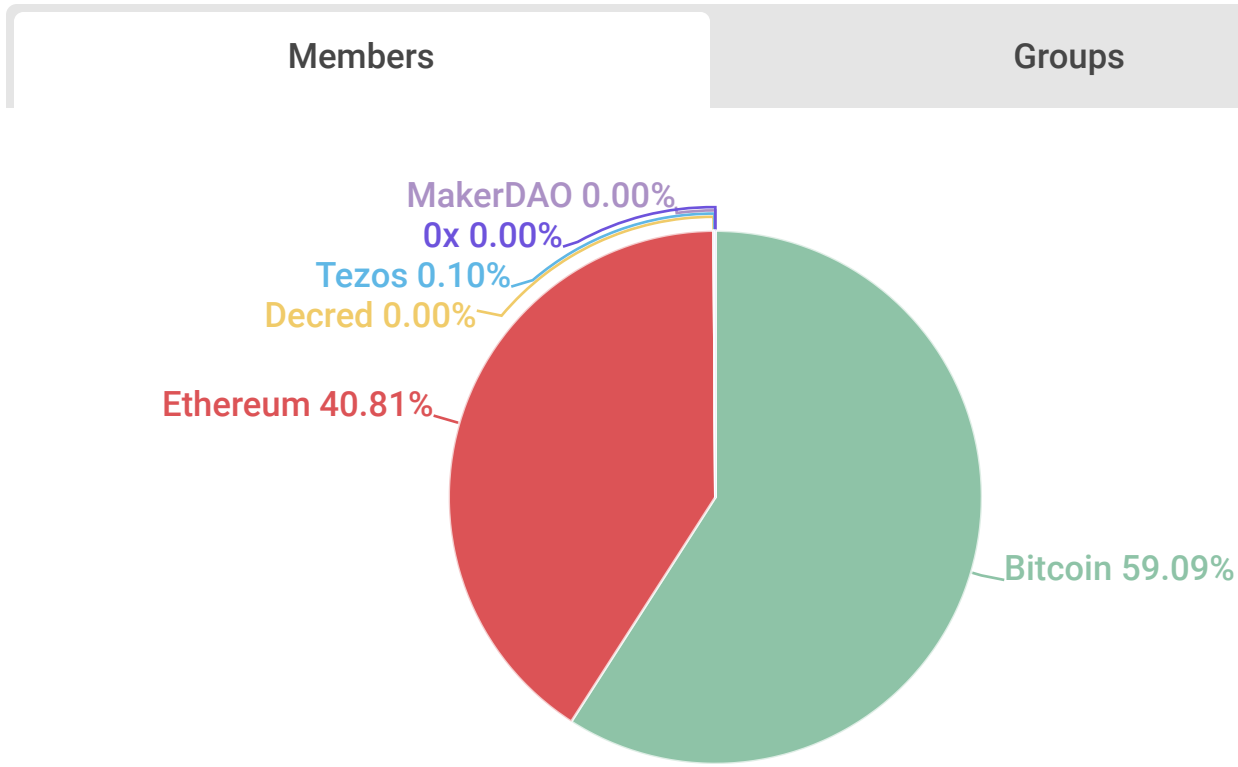
One metric we could look at is the number of global meetups, where stakeholders meet to learn, develop and debate changes. While it's clear Bitcoin and Ethereum have the strongest Meetup numbers, the type of stakeholder isn’t clear - whether retail investors or developers or funds. This early in crypto, the focus should be on the development community, since they are the construction workers building the foundations, roads and bridges which viral use cases will be built upon.

There are a few nuances that will be discussed later on, but the takeaway is that a viable way to enact changes is worthless without a community that can research and code worthwhile upgrades, and vice versa.

We aren’t drag and dropping upgrades in crypto like building a GoDaddy website, every upgrade needs to be customized and coded from scratch. Developers could copy and paste code over, but then they run into the issue of being a fast follower.

We note, not every meetup occurs through Meetup.com, but it is the largest proxy for tracking meetups. Other sources that can be used to gauge interest are Twitter/Telegram followers but these can be easily gamed in our opinion.

Meetup.com Statistics (as a percentage of total)



Community Metrics

A more developer targeted metric base would be looking at Github statistics, or the place where developers work together on the actual code powering these platforms.

Stars and watchers are less of a development metric in our opinion, and more of a popularity contest, since anyone can use these them to watch or be alerted to changes.

The best metrics for work being done on the actual code (BTC's code, Ethereum's code) is to look at Github additions and deletions. These are the lines of code that are added or deleted over the past year. This demonstrates the work actually being done to improve these platforms, by the parties we want - developers. These metrics can be gamed (adding spaces, copy and pasting etc) but is one of the best metrics we have to work with for discerning developer work.

Github Statistics

Crypto	Stars	Watchers	Commits (Last 365) Days)	GitHub Additions (Last 365 Days)	GitHub Deletions Last 365 Days	GitHub Net Additions
Bitcoin	37,032	3,518	1,874	99,688	71,749	27,939
Ethereum	22,512	2,040	1,035	267,247	127,888	139,359
Tezos	1,306	263	1	11	-	11
Decred	468	91	447	48,664	43,887	4,777
MakerDAO	81	28	174	10309	2809	7500
0x	965	90	7,322	1,367,639	1,532,979	(165,340)

Stars = people keeping track of projects
Watchers = people are notified of changes to the repository
Commit = a file revision (saving a new version)
Additions/Deletions = Lines of code added or deleted

*Does not include the githubs of the projects building on-top of these platforms

Source: OnChainFX

CryptoEvolution Formula: A Few Nuances

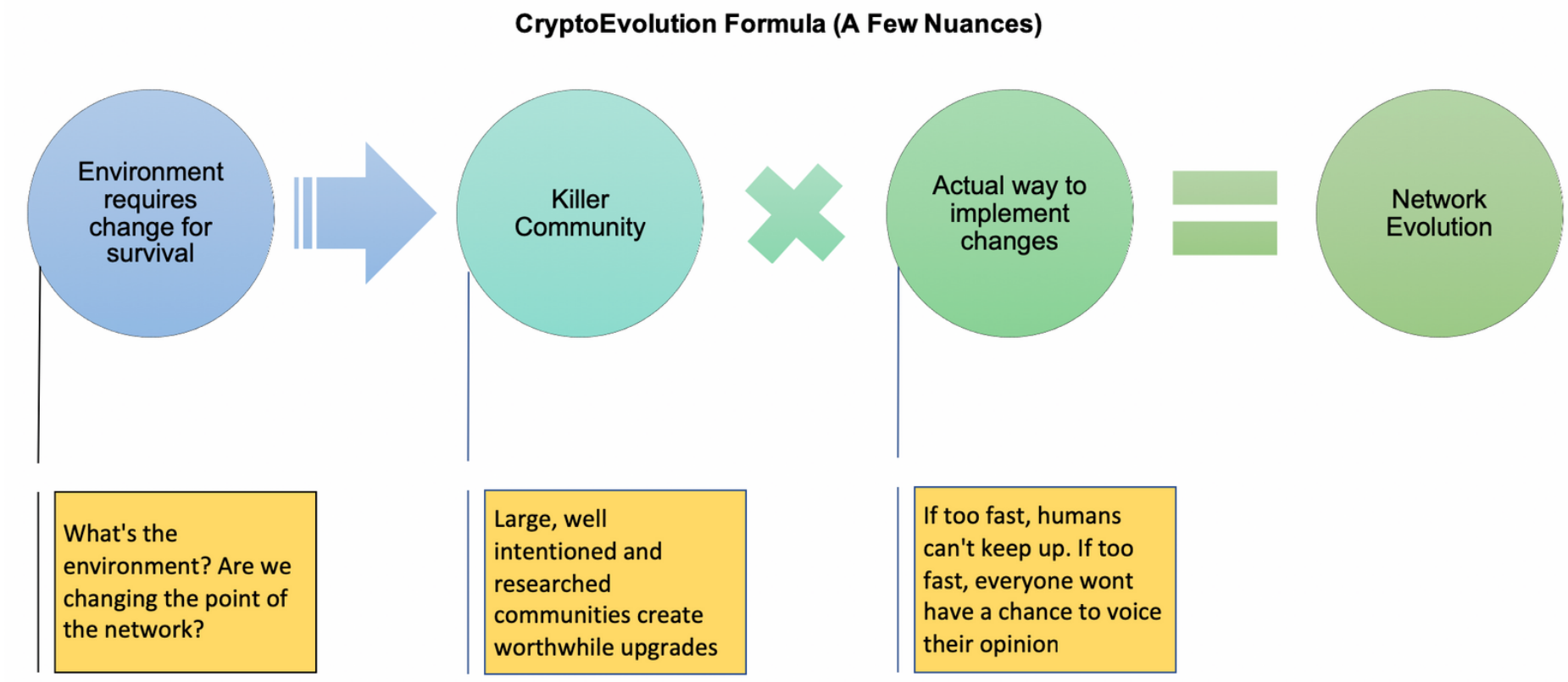
There are a few nuances to our formula worth exploring. The first is whether or not the environment (market) itself requires a crypto platform to change for survival. This is again subjective as many argue Bitcoin's inability to easily change is a key feature, and we agree today since the platform is nearly ten years old and over time layer-1 should be harder to change over time - more on this later.

Further, we are very early in the development of crypto platforms; and it has not been definitively decided what the environment (market) actually is for a lot of these platforms. Our position is that since we are so early, and subject to decades or product/market fit stressors, crypto platforms must be able to change and adapt over time to meet these push-and-pull forces.

The first variable, competent communities researching and coding upgrades, is subject to the magnitude of each change. The number of changes is irrelevant to a protocol if they are not worthwhile. We argue a large number of small changes or a lower number of larger impact changes are both a path to the same result, but the overall magnitude of either way has to be worthwhile to furthering the platform.

On the actual way to implement changes variable, we could face an issue that this metric is too fast - or changes are happening faster than humans can keep up with, known as autonomous software.

We believe we are years away from this potential reality, and even if it occurs, humans can enact checkpoints; for example in Tezos changes are run on a testnet for 48 hours before another human vote takes place to enact changes.

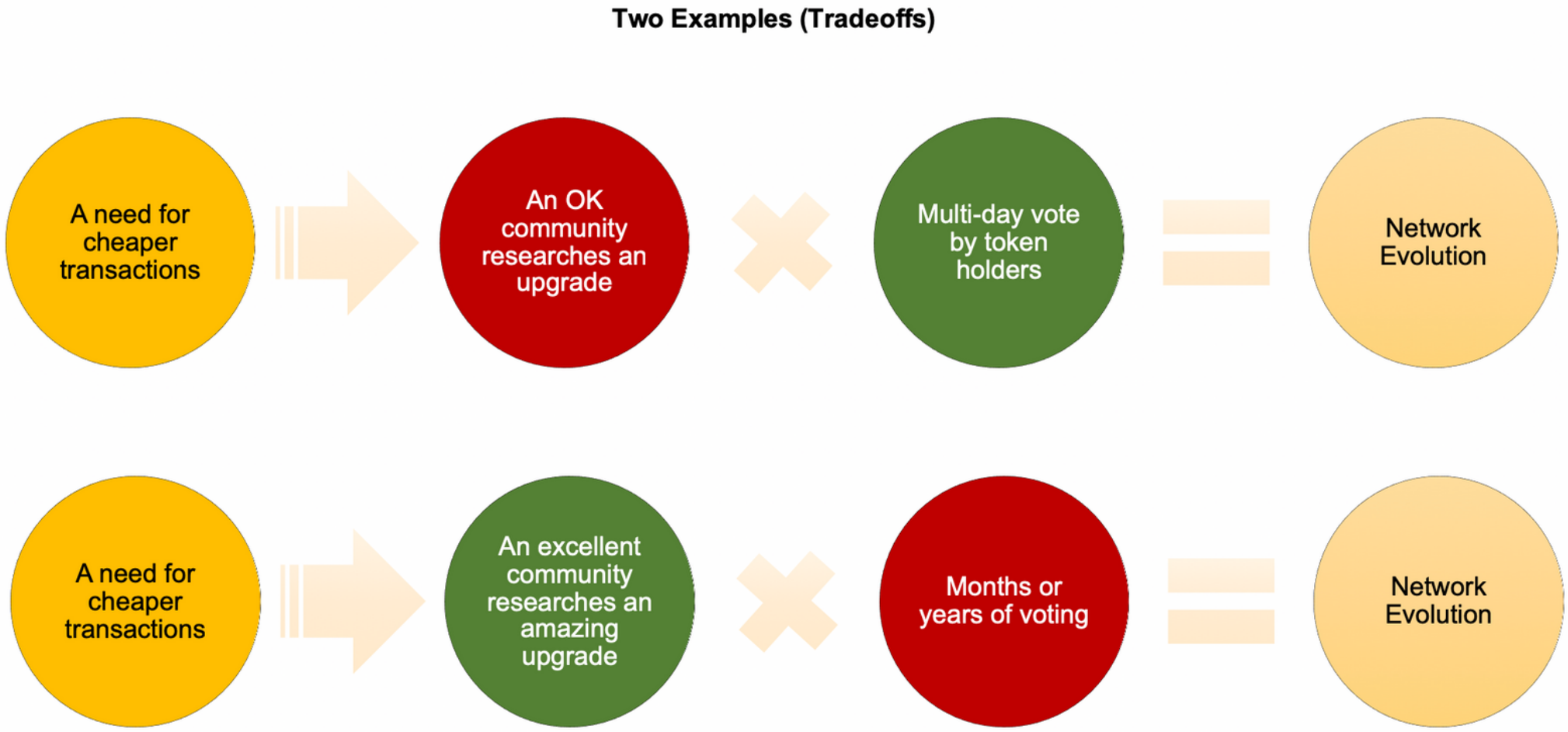


Tradeoffs Example

One example of evolutionary trade-offs can be seen through two hypothetical crypto platforms. Both platforms have a need for cheaper transactions. The first platform has a mediocre community (variable 1) but a fast way to enact changes (variable 2). The second platform has an amazing community but a long voting process to enact changes.

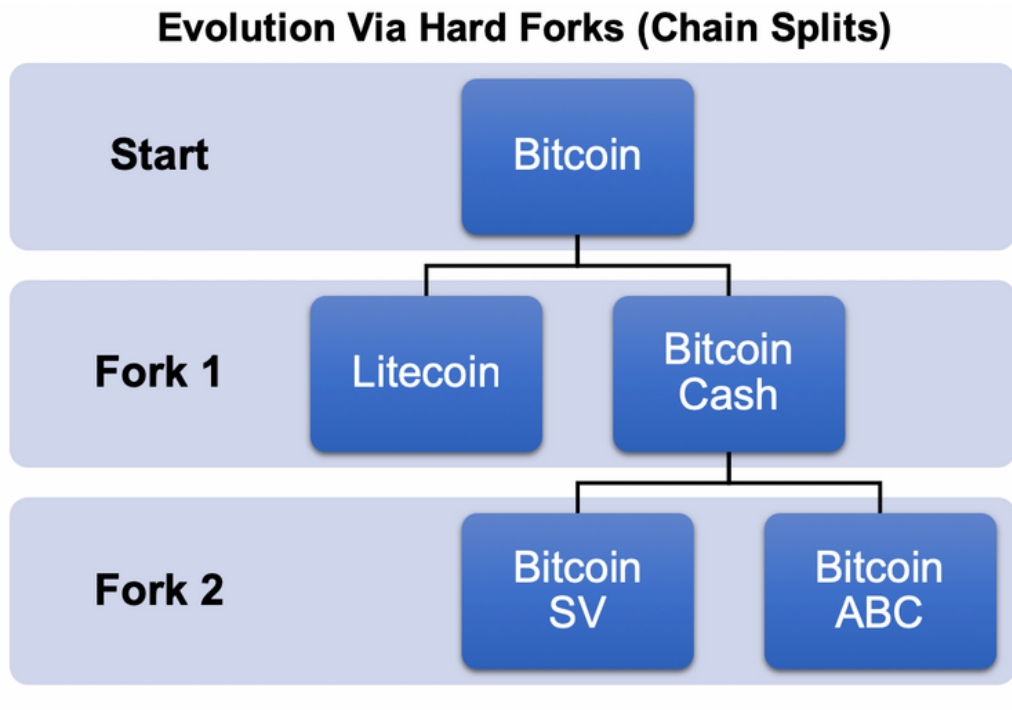
The takeaway is that both communities can achieve the same goal with different tradeoffs; platform 1 may implement buggy code but platform 2 may take months or years to actually enact the change. The strongest evolutionary platforms will feature the best of both worlds; a killer community to research them and a fast way to implement changes.

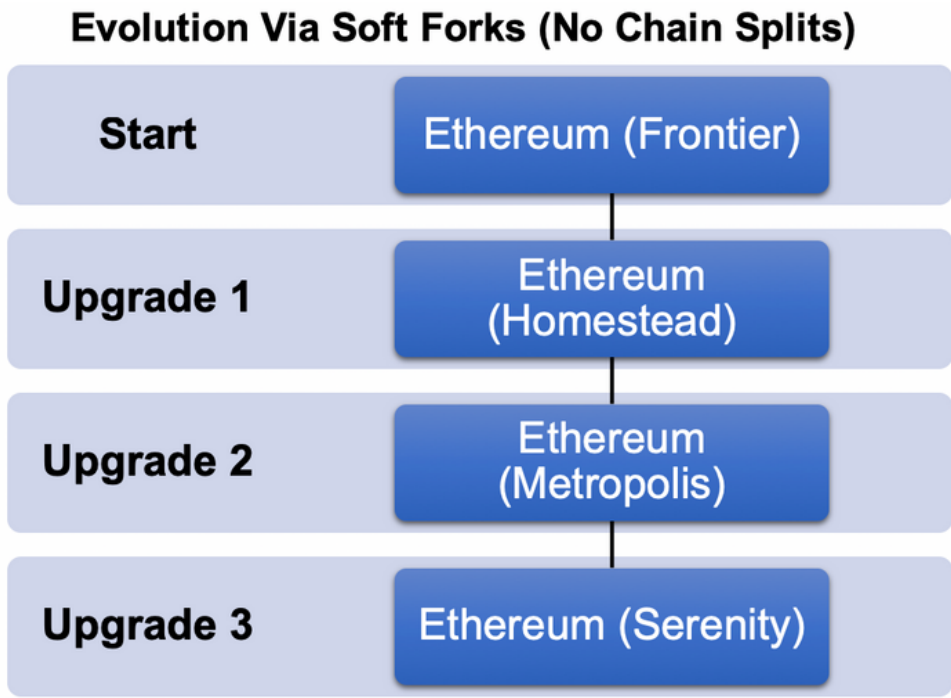
This isn't to say that platforms can enact remedies to help solve these tradeoffs; for instance the "Ok community" platform could spend its foundation's capital to fund research or the "slow upgrade" community could incentivize users with rewards to vote faster or more frequently.



Major Forms of CryptoEvolution

The actual evolutionary step of crypto networks can take many forms, the two most popular are hard forks (upgrades that require chain splits where a new token and protocol created) and forks that do not require a chain split which we refer to as soft forks for simplicity (an example is Ethereum with its Homestead upgrade). A hard fork can arise when a subset of a community breaks away, makes code tweaks or upgrades, and runs their own chain with their own token. We've seen this happen with Bitcoin dozens of times (Litecoin, Bitcoin Cash, Bitcoin SV, Bitcoin ABC etc).





The other option is having a community focused less on forks, and more on a series of upgrades that can improve the platform without hard forks. For instance, Ethereum's roadmap features several steps with the goal of not forking the community out. Other platforms such as Tezos and Decred are also resistant to chain splits (contentious forks where new chains are created).

There is no right answer, forks allow anyone to start their own chain with whichever changes they would like and are subject to market forces to drive adoption or not. In Bitcoin's case a user would "gain" all of the forks anyway, so they are riding the evolutionary wind on the backs of several horses. We believe most users sell forks, or don't claim them though, and stick with the main original asset negating the evolutionary aspect of forks.

The ability to hard fork is a key feature for crypto innovation, forcing developers and community thought-leaders to constantly be improving (the fight against developers becoming content).

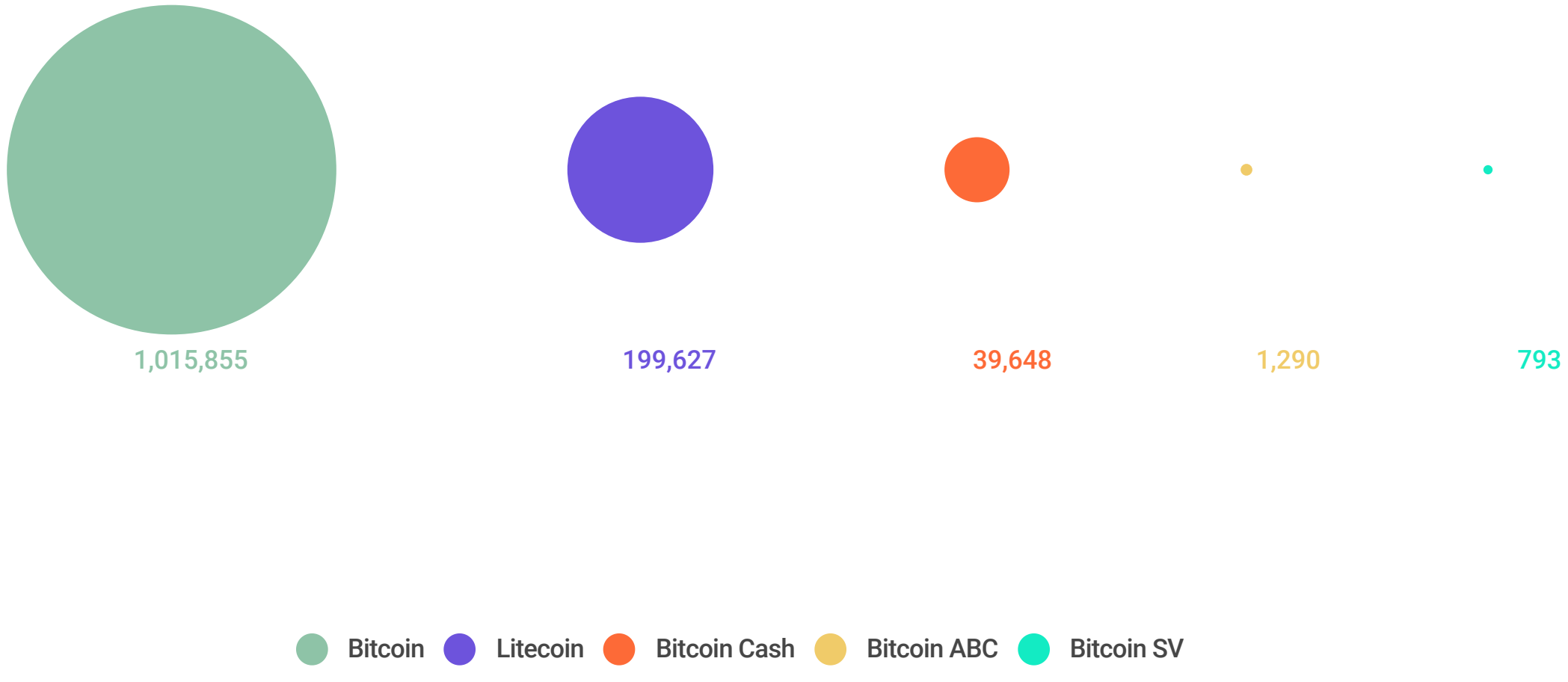
Chain Splits Can Fracture Communities

Our issue with sticking with hard forking as a main upgrade medium, instead of attempting to maintain a community, is that part of the community is broken off each time a fork happens.

One could argue if Bitcoin never forked, those developing on its forks would be instead working on the original Bitcoin code. While there are overlaps in developers and followers for each fork, there is only so much time in the day to work on a protocol.

Reddit Followers

Forks Fracture Communities, Leading Members To Work On Other Projects



Continued

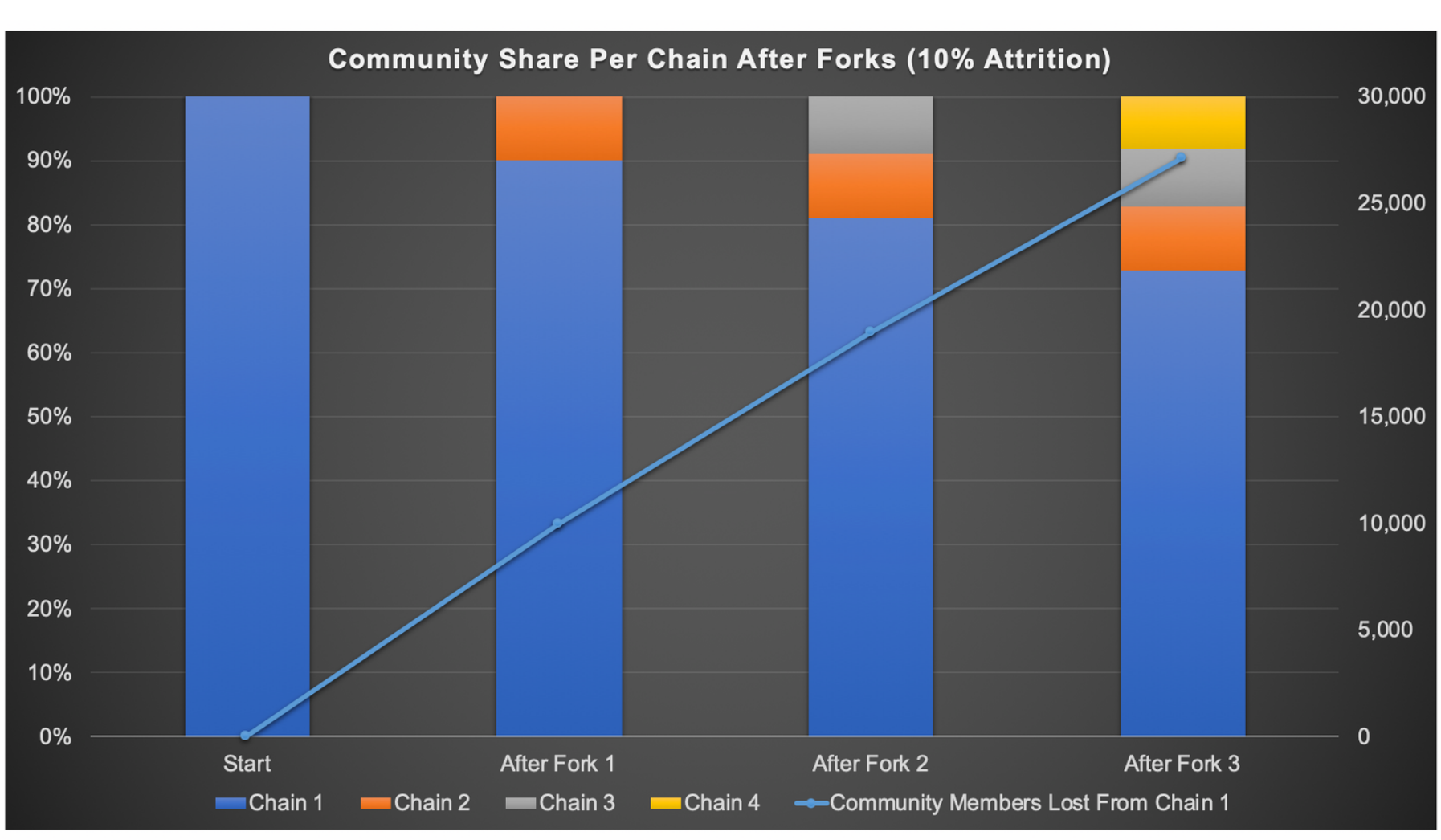
Demonstrated below is a hypothetical example of a crypto community's accretion after each hard fork, assuming 10% of the original chains community goes to each fork (Each fork a fork of the main chain, not a sub chain). After 3 forks a hypothetical crypto community of 100k dwindles to 73,000, a 27% decease. That's 27% fewer ideas and 27% fewer opportunities to CryptoEvolve. We believe our modeled 10% attrition rate is conservative given Litecoin's fork demonstrated a 20% attrition rate.

While we are early in crypto, the more damaging effects of chain splits are the loss of network effects surrounding a project and the potential crack in everything built on top of a platform. For instance, if a viral application is built on top of Bitcoin, and the network forks, then the DApp above would be affected in disastrous ways.

If a security-token platform is built on top of Bitcoin, and a $1B piece of real estate is tokenized with its certificate stored on Bitcoin, and Bitcoin forks, this certificate now lives on two chains. Imagine the issues if two different parties claimed ownership of the Metlife building in New York.

Net, we think its vital for a crypto platform to explore options to implement changes that doesn't necessarily always lead to a hard fork. This becomes distrarous as networks develop overtime as use cases are built on top of them.

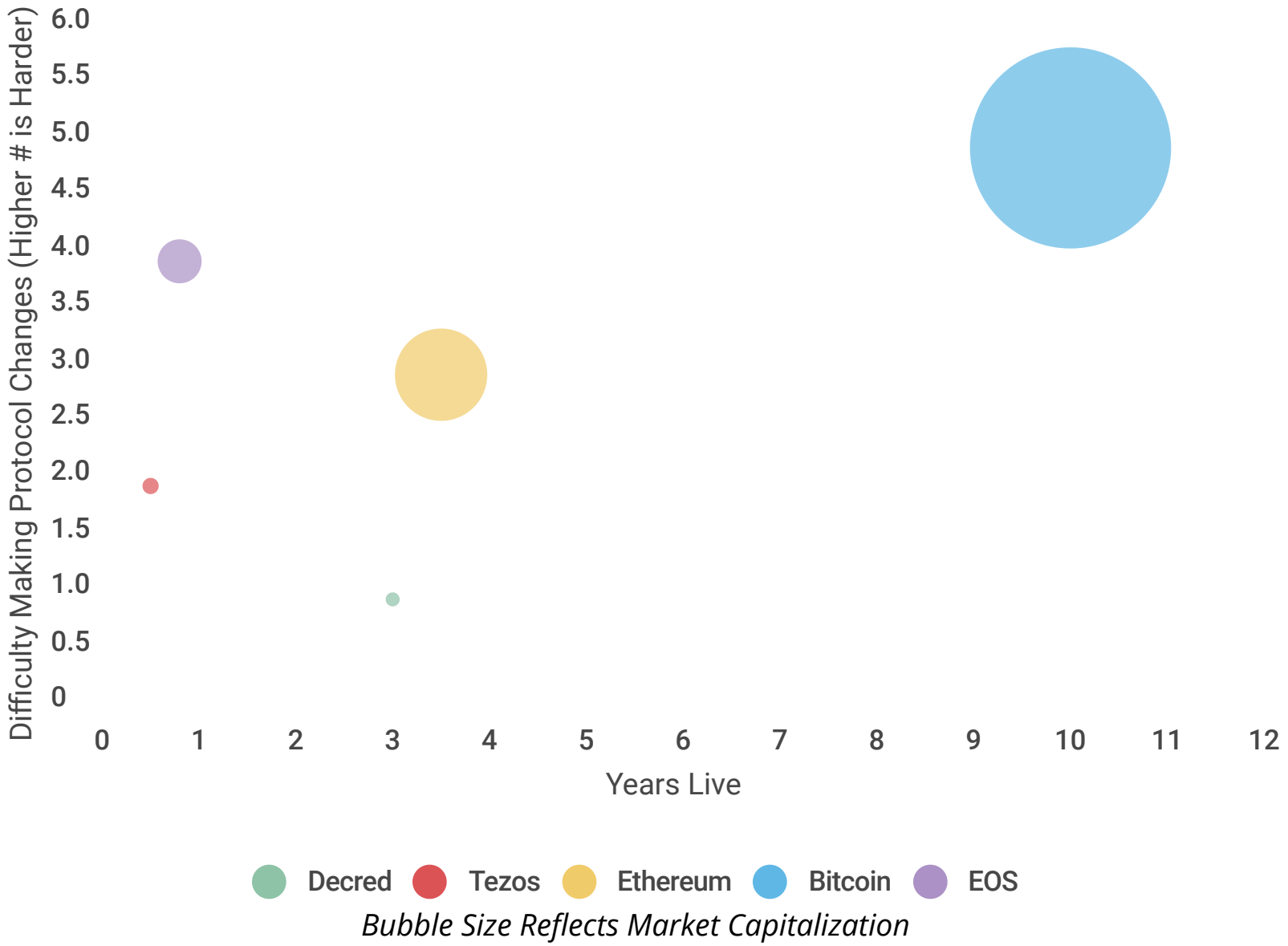
Tezos and Decred have made headway here with on-chain voting and Ethereum has been resistant to contentious forks (beyond the DAO) due to its communities strength.



Harder To Implement Governance Later

Governance corresponds to the second aspect in our CryptoEvolution formula; the ease and speed of implementing changes. Many in the space point to a debate between off-chain governance (community argues outside the chain) and on-chain governance (vote with your tokens on chain). Our position is that on-chain governance is just the formalization in the process for how to enact changes, the off-chain aspects (meetups, discussion, message boards) can still occur.

Our position here is that it is very hard to implement a formal governance structure later on in a crypto platforms life, because the decision to implement one is a governance decision in and of itself, and as we have seen decisions in established protocols usually lead to forks, and that platform wouldn't gain from the implementation of a formal governance system but its fork would. The current experimentation early on in crypto on which governance system is the best is positive for space though as we explore which is the best model.



Bitcoin and Ethereum are two of the largest crypto platforms and neither has a formalized governance system. The effects are clear; Bitcoin has had dozens of forks and Ethereum has had its own governance issues (ETH 1.X, The DAO, deciding on which roadmap items should be explored).

Keep in mind, the first variable of our equation, the killer community, erodes with each fork. As such we believe the more forks, the less competitive a potential community. While this assumes there is no organic developer growth, we wanted to isolate the potential theoretical impact from forks on communities.

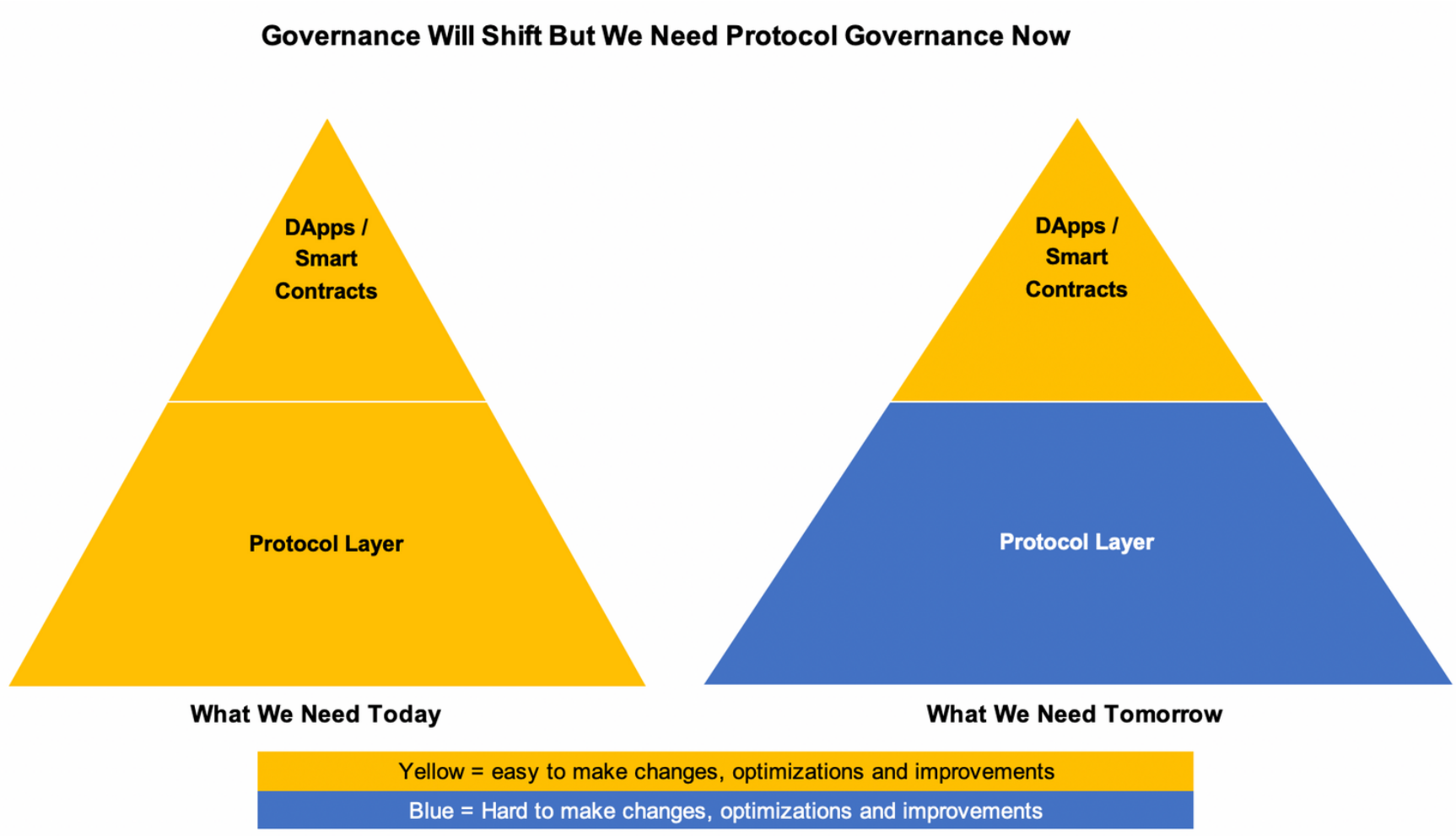
Governance Will Shift Up Over Time

We are very early in crypto, and as previously discussed we believe the foundational layer-1 platforms (Bitcoin, Ethereum, Tezos, Decred et al) must be able to adapt and evolve since definitive product/market fits and technological needs are not set in stone.

Over time, we expect this dynamic to shift, where once layer-1 platforms are evolved and hard to change, the focus on governance will move up to layer-2 where applications and use cases are being built. For instance, once a crypto platform is set in stone, stakeholders will argue changes to the “Crypto Facebook” built on top of one of these platforms, not on the base protocol itself.

The inability, or it being very hard to, change the base protocol will become a feature in future years, and we are seeing that in Bitcoin today - its security and strength comes from it being very hard to change. But we believe, for Bitcoin specifically, this has tradeoffs; its scripting language makes it very hard to build functional programs on. This is demonstrated by MakerDAO ($225M in ETH locked up backing the stablecoin DAI).

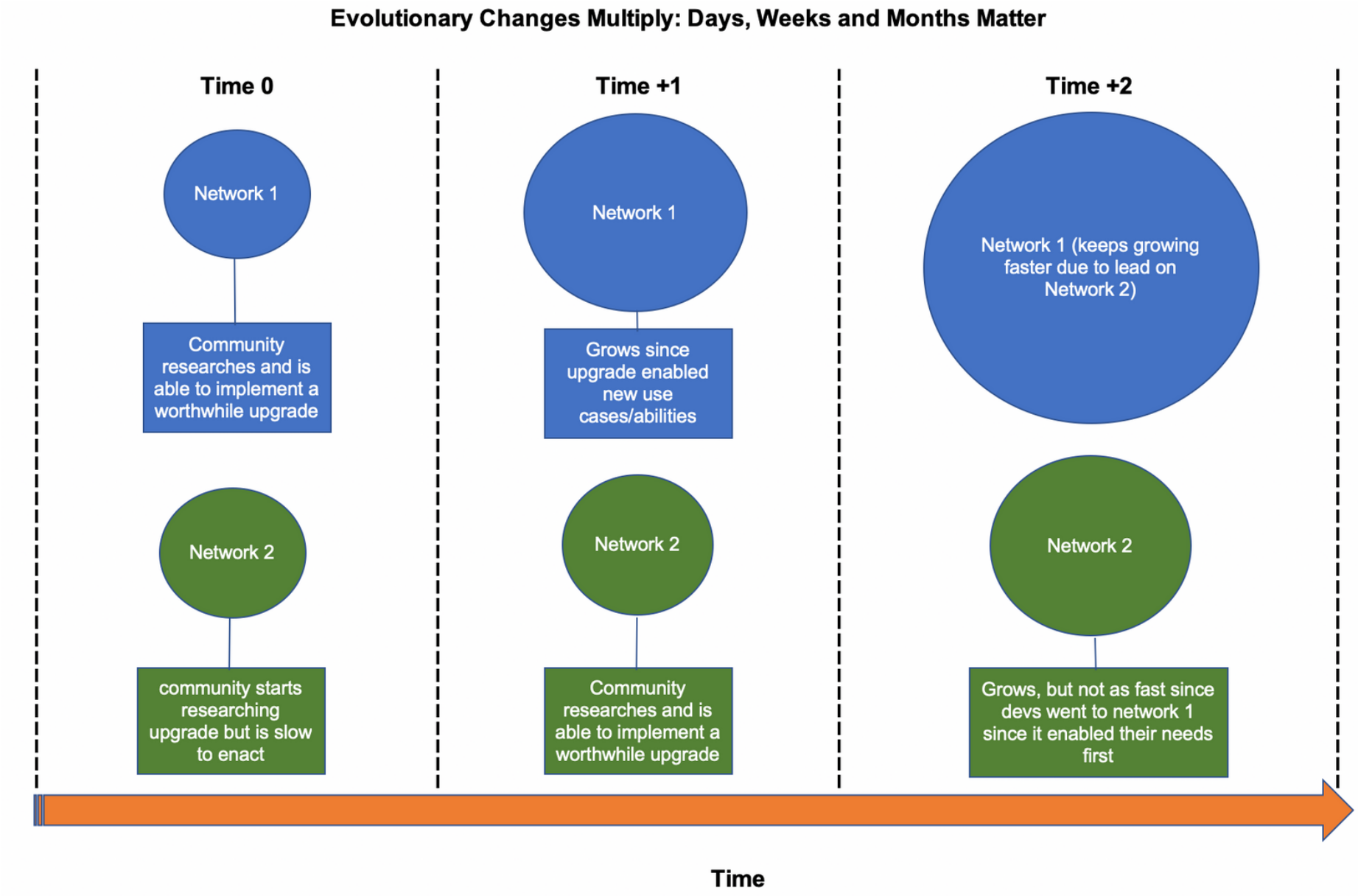
Although, in many respects this is not an issue if we are all honest with ourselves. If Bitcoin is meant to be a digital gold that can’t be manipulated, then its fine as is and its layer-1 should not be subject to fast or rash changes.



Evolutionary Changes Compound Fast

Evolution happens at an astonishing rate; this force sculpted humans through millions of years of changes. In crypto, we believe the crypto community that has an ability to actually enact changes and a community that can create viable upgrades will attract the lion's share of network effects for a specific market.

Demonstrated above, a community that can solve a problem the fastest, or enable a niche will have a lead on competing platforms because there is no reason to use a competing platform if one platform already enables what a stakeholder needs; assuming these platforms are making the same or similar trilemma tradeoffs (decentralization, security, scale).



CryptoEvolution is another factor, along with interoperability/composability (we wrote about prior) that will drive winner-takes-most dynamics and those platforms which can't evolve will die off.

Further, copy-and-pasting updates (i.e, if Ethereum Classic were to copy a change implemented on Ethereum) is futile in our opinion because the platform to first enact a change will attract the developers who need it the most, first, and they have limited reasons to leave.

CryptoEvolution Rankings

There are many vectors across which to rank the two variables of our CryptoEvolution formula. We denote this is a subjective scoring method, as there are zero clear cut ways to judge the strength of a community, but there are areas which can be explored.

The data we have compiled in the below table lead us to the subjective scoring results we have established on the next page This is not an exhaustive list, but is instead meant to paint a picture to help every stakeholder in a crypto network who is attempting to discern whether or not their network can evolve over time.

Subjective CryptoEvolution Metrics (Layer 1)			
Project	**Project Type**	**Is The Community Large/Smart Enough To Develop Upgrades**	**Difficulty Implementing Upgrades**
Bitcoin	Public Blockchain	Yes (Blockstream, Lightning Labs, large and oldest community)	Very hard. Protocol is not meant to change. Evident in the need to hard fork (Litecoin, Bitcoin Cash etc). Avoiding hard forks prevents a community from being fractured, but also closes the door to community members looking for new functionality
Ethereum	Public Blockchain	Yes (200,000 estimated developers) extremely active development community with 9+ clients and a multitude of teams building new technologies (Prsymatic Labs, Raiden, etc) and numerous research sources (ethresear.ch, Ethhub.io, developer calls). Truffle development suite has over 1.4M downloads and 2,500 DApps are built on Ethereum. OpenZepplin has 400k+ downloads (framework to create easy smart contracts on Ethereum)	Medium. Community consensus drives decisions which are implemented on a roadmap basis. They have been subject to delays recently and goal post moving.
Decred	Public Blockchain	Smallest community, but growing	Medium. Decisions for using treasury funds are voted on. For protocol changes, a majority of nodes need to first implement the change (95% of 1000 most recent blocks must be using software) then if 75% of token holders vote "Yes" the protocol is changed
Tezos	Public Blockchain	Small but growing community. Some very smart teams and researchers (Marigold for Layer-2 announced recently)	Easy. Protocol changes can be voted on with tokens and upgrades can take place without a hard fork . Changes are run on a testnet before being voted on again and then implemented
MakerDAO	DApp Built on Ethereum	Yes but the community is medium sized	Easy, token holders vote on changes through an easy UX on vote.makerdao.com
0x	DApp Built on Ethereum	Yes but the community is medium sized. Nearly 20 relayers being powered by 0x, and new DApps are leveraging its infrastructure such as Veil	No formal governance for token holders

Sources: Delphi Digital, Trustnodes.com, Chris Burniske

CryptoEvolution Rankings

Bitcoin has a great community, but it is very hard to change the protocol so it has a low evolutionary score; this is perfectly fine is a stakeholder's assumption is that Bitcoin's layer-1 does not have to change. Ethereum has one of the strongest communities in our opinion, but implementing decisions is far from an easy process which involves a lot of back and forth across a multitude of different mediums. This is also perfectly fine, since this decentralized way of deciding can lead to involvement across the entire stakeholder spectrum.
Decred and Tezos have smaller communities, but both offer much more clear cut ways at implementing changes through token holder voting (Tezos) and a mix between token holder voting and miner support in Decred.

We include MakerDAO and 0x for context; both are not blockchain platforms but applications built on top of Ethereum. Both have growing communities, but in MakerDAO, MKR token holders can vote on changes whereas in 0x token holders have historically had no governance features. This is set to change as 0x is prepping for its first token holder vote, but we gave 0x a lower score since it's still the first voting event.

The flipside is that 0x has "layer-3" innovation, since there are 19 relayers who are building on-top of 0x, which is built on Ethereum. 0x's community is much stronger than just the work being done on 0x itself. The takeaway is what we alluded to earlier, that governance will eventually move up the stack; instead of governance debates on Ethereum, we will move up to debating changes to the applications built on top of Ethereum, such as MakerDAO and 0x. We do denote that a large subset of developers/stakeholders will stay loyal to an existing platform (I.e. all Bitcoin developers didn't jump ship to work on Monero since it has better privacy) since they have expectations for Bitcoin to implement new features in the future).

The ability to make changes fast could be a detractor to stability, but this is why we argued earlier that layer-1 should be harder to change over time.

Subjective CryptoEvolution Scoring (Layer 1)

Project	Project Type	Is The Community Large/Competent Enough To Develop Upgrades	Ease of Stakeholders (Not a centralized entity) Implementing Changes	Evolutionary Score (out of 100)
Bitcoin	Public Blockchain	8	1	8
Ethereum	Public Blockchain	10	5	50
Decred	Public Blockchain	2	7	14
Tezos	Public Blockchain	3	9	27
MakerDAO	DApp Built on Ethereum	3	7	21
0x	DApp Built on Ethereum	4	0.5	2

*Changes are implemented by the 0x team, token holder governance is a future possibility

Sources: Delphi Digital, Trustnodes.com

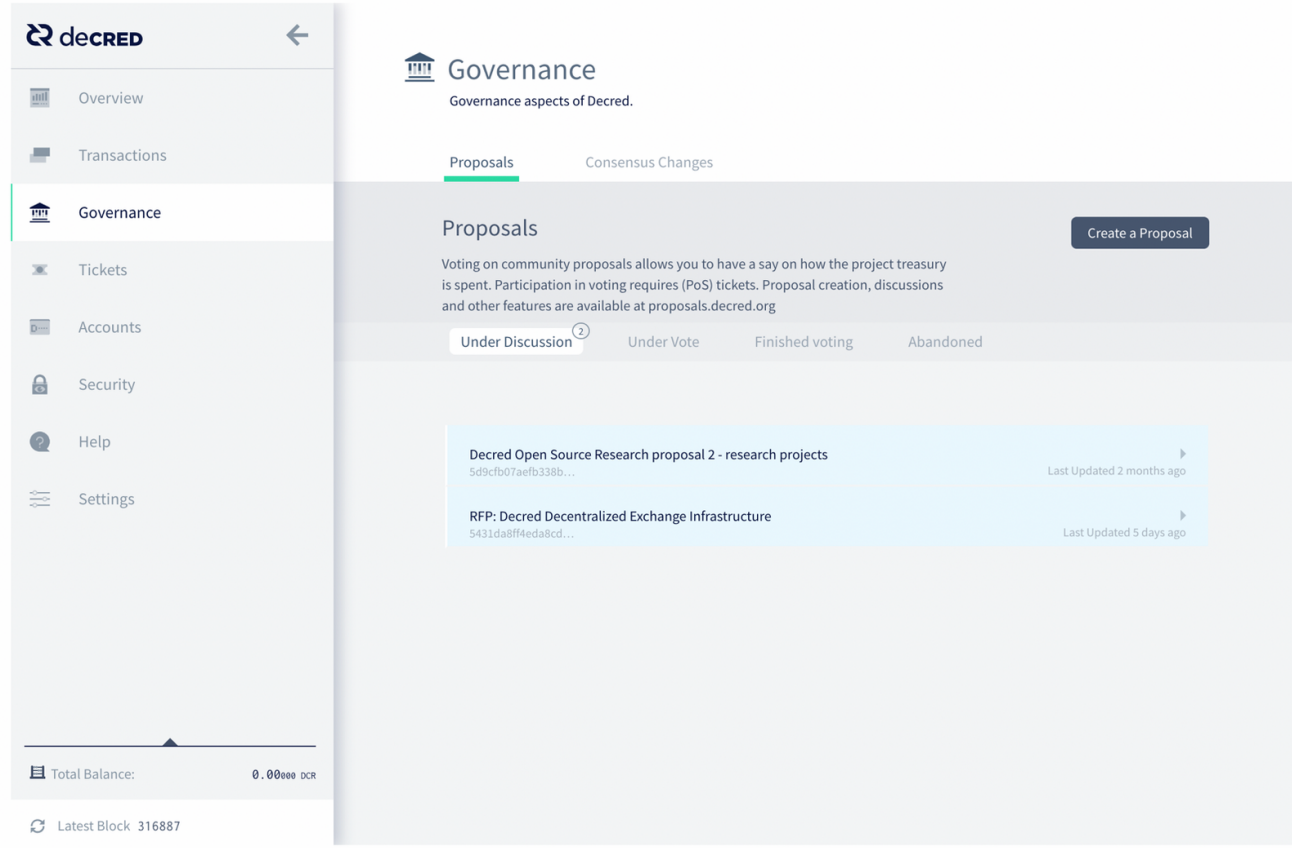
On-Chain Governance Example

We wanted to close by demystifying the process of on-chain governance; which plays into the second variable in our equation.

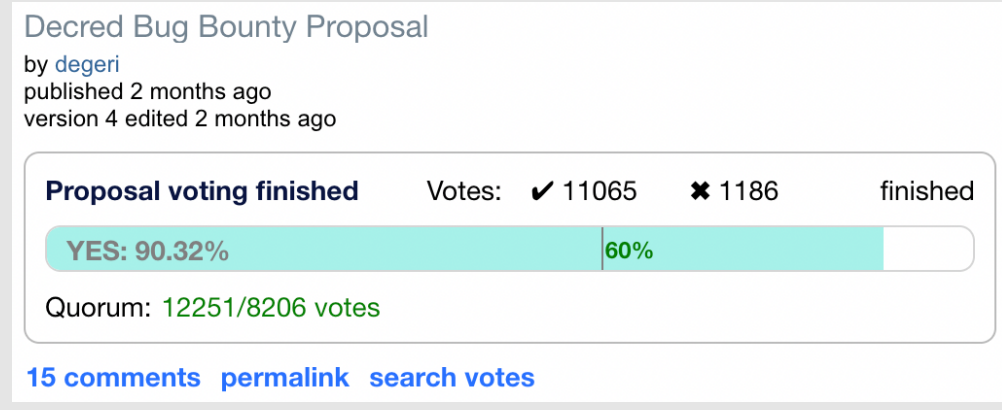
Decred offers a simple way of voting on changes. Once a user downloads Decredition, the main wallet for DCR tokens, a user can easily vote on changes. These changes can be through Politeia proposals (how to use DCR's treasury) or on consensus changes to the protocol itself. Users have to lock up their DCR and purchase tickets to vote, but this is easy, shown on the left sidebar.

We share this example since DCR has innovated on the speed/ease of implementing changes. We believe this is much easier than the signaling of other crypto networks where users have to run new software to implement changes which is a technical hurdle. Lowering the barriers to entry leads to an acceleration of adoption. Millions of people create websites using GoDaddy and Wix, and the majority don't know how to code.

This issues with on-chain governance are low voter turnout and it being prone to manipulation.



The results of votes are also shown in real time so parties can't game which is the popular protocol or proposal change; one example below for Decred's bug bounty program.



Conclusion

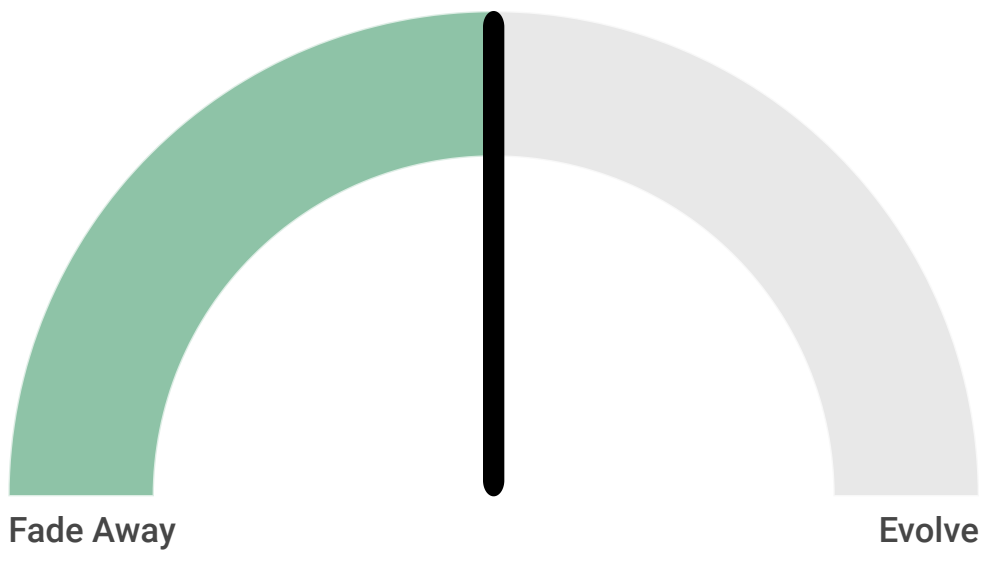
CryptoEvolution

CryptoEvolution is the ability for a crypto network to evolve over time and is enabled by having a killer community to research and code worthwhile upgrades and a viable way to implement changes.

It's logical for all stakeholders to review any crypto projects they are involved in to ensure the project itself can evolve over time, if not it's value could erode away over time.

No Crypto Is Safe

Every crypto is subject to evolutionary forces, and those which are unable to adapt will die off. The caveat is that eventually layer-1 platforms (BTC, ETH etc) will evolve enough that focus will shift to evolution on layer-2 (applications built on top), but we believe we are so early in crypto that evolution has to be a possibility on layer-1 today.



How Fast Is Your Crypto Project Evolving?

DELPHI DIGITAL

85 Broad Street, 17-092
New York, NY, 10004
www.delphidigital.io