RAID

by Sam Porter

Decentralized word-of-mouth marketing service

As of today internet personality bubble reaches absurd levels, if this will continue, a mere mention by an internet celebrity could cost tens of thousands and much more in the future. It is generally believed that buying internet personalities' time or creating an ad-trailer should be expensive and it’s worth it, however it appears than a new more effective alternative to this already exists and actively being used. And it appears that it is certainly possible to achieve this in a decentralized manner when the employer and the worker don't need to know anything about each other except the stake, eliminating the need of assembling a marketing team or trying to apply to real-life jobs.

What ad trailers and internet personalities attempt to do is not just to sell, but to start a *discussion* to increase awareness, to pump up the popularity of the product. Word-of-mouth marketing, proof-of-discussion, whether it's praising or sick burning, FUD or optimistic insights, blind cult following or elaborate arguments, - the discussion behind the product is what really promotes the product. Celebrities and ads are just a third-party and it is certainly possible to eliminate this third-party and pay directly for discussion and mentions instead. A mass discussion by nobodies for nobodies.

RAID speculative value is fundamentally required as an auto-moderation measure. Market peak buyers are more likely to have less stake and less reputation, maintaining the quality of the service, decreasing (or even eliminating, depending on chosen route) any need to moderate the campaign by an employer. This is the token which will provide income to socially inept, traumatized, schizophrenic, mentally challenged and physically disabled people, so that they will never be kicked out of their homes for being unable to adapt to

life. Hopefully, someday in the future shitposting job in RAID will reach close to minimum wage levels of salary.

RAID solves blockchain wealth distribution problem by implementing old like the world CeFi feature - active income(salaries). With it, RAID can expect Gini coefficient closer to real world CeFi levels than any other blockchain project. This pushes decentralization security standards on another level.

Employers setup and fund campaigns in Raid Market contract with chosen keywords or topics on chosen websites, workers commit to these campaigns by discussing certain posts or anything eligible(matching keyword) for paid discussion. By default, workers are allowed to express genuine opinion on every topic, it can be positive or negative, sincere or a blatant lie, and, depending on the resource, workers by default have the right to completely derail the discussion, talk about weather, discuss investments, etc. Workers will still get paid for unrelated discussion as long as it for example bumps the thread, or adds another comment to discussion making it look more heated and popular. Again, it mostly depends on the resource and a forum could simply ban/remove unrelated posts. As posts need to be witnessed by oracles, a worker has to ensure that his post won't be removed.

Ppp – pay-per-post is a variable which defines how much workers get paid for a post in USD value. As RAID token price increases, the amount of RAID being paid to workers decreases and vice-versa. This creates a certain confidence for a worker in the amount of money he will receive regardless of market volatility. USD index is monthly and is average price of RAID token last month. This creates confidence for the employer that a campaign he ordered this month will give him certain output. As a side strategic side effect, which will be discussed more in Part 3, it can potentially make early adopters marketing gods.

Campaign settings are planned to be flexible, allowing to setup rules for conventional marketing strategies(soulless shilling). Campaigns will also have an option to be set up as non-editable to attract funding from other potentially interested employers. Employers can fire workers, or, can setup noFiring to true, which will create piece of mind for workers. Employers can also set onlyManualApproval to true, so that only approved workers can join.

Allowing conventional marketing strategies is meant to make RAID understandable. I do not believe it is actually required, and it could easily become harmful for RAID, as it's basically censorship, so it might be disabled in the future as quickly as it was implemented. RAID marketing paradigm promotes critical thinking, which is, as I believe, a virtue. If Employer' product is good, he can assume that Worker holds a bag, so he will receive a natural quality output for a low pay. RAID is simply ineffective for scamming people as long as there is no moderation from the employer. Since the product is the most important part of marketing, I genuinely fail to understand why would you need to lie about a good product, why would you need to shill it, you just need to make people aware. Let them choose your product

without manipulation, let your product speak for itself, allow people to think for themselves. Of course this paradigm will be perceived as silly by many marketing professionals. We will see what's better: paying to influencers or influencing influencers.

Eventually, on websites which support nicknames workers will eventually be able to talk about anything with anyone anywhere as long as they have keyword in their nicknames.

General technical principles

1.Accuracy is expensive.

- Stone Age math whenever worth it, minimum Solidity store loads and writes.

- Packed structs if more than one value of a struct is altered by a function.

- Store numbers with less decimals where possible and convenient. Restrict accuracy where possible and convenient

- Hardcoded addresses and values whenever possible to, again, reduce store calls.

- Inaccurate Transfer Contract will be introduced later, briefly it's a bulk sender which allows to perform certain actions in a collective queue. The cost of Inaccurate Transfer for the end user can be potentially reduced to 1 store write as trustless version and to 1 emitted event as a trusted/trustless version at the expense of waiting until the queue gets filled and executed.

2. Decentralization is the most valuable concept of our times.

- Bitcoin forks are more centralized than Bitcoin. If it will be required then top holders of Litecoin could be found and influenced in a way that allows the government of a nation where top holders reside to acquire a lot of control over Litecoin. BCH and BSV wealth distributions are considerably better than Litecoin, still worse than Bitcoin. A huge dump has the potential to weaken the security of the network, and after that it can be reorged in any way required. Today, cryptocurrency is potentially regulatable and mutable as is. There are ways to change this.

3. No mandatory auto-updates. No hidden tracking.

- RAID dares not only to support this standard, but to promote it and make it the only acceptable standard. Auto-updates will be always disabled by default(if possible, Chrome browser does not allow that)

4. Free open-source.

- If it wasn't for free open-source, if no free libraries would exist, it could take years for me to develop RAID. And RAID could be a puzzle for something greater. Somebody could eventually use it to create something critically important.

Base contracts

Ethereum is the blockchain of choice as the most robust censorship resistant chain, and with an assumption in mind that blockchain industry is fundamentally monopolistic in a sense, since the biggest network is always the most secure, which attracts even bigger capital and in turn makes it even more secure. And in case of Ethereum even more censorship resistant. Base contracts will not be owned by the deployer or governance, however some variables in these contracts are changeable within certain hard limits.

First and main contract is "Very slow ERC-20" implementation(VSR ERC-20). The implementation utilizes standard ERC-20 function _beforeTokenTransfer() in such a way that prevents development fund and marketing fund and all other funds from dumping on the market. The function checks how many blocks passed from rewards genesis block and allows to claim only a certain amount per every passed block. Basically developers and all other participants of RAID can only claim rewards within constant emission limits and this hard limit can't be avoided under any circumstance. Even contract addresses declared in _beforeTokenTransfer() happen to be upgradeable, no matter what kind of logic will be present in these contracts, even if they happen to have a bug, the bug in no way will be as devastating as it could be without _beforeTokenTransfer() guard. This function also creates a hard limit on how many workers can participate in RAID as it's important in early development stages to setup oracles reliably.

Second base contract is Founders Contract. Founders Contract uses LGE mechanics proposed by CORE token team with certain differences which I believe most suitable for RAID. Founders Contract is a trust minimized LGE. It automatically creates liquidity on first transaction after last LGE block. I can't transfer Ether from it, nobody can. To ensure

critically required in case of RAID decentralization, the LGE will last for 2 months. Liquidity is not locked at all, instead a strong incentive to keep liquidity is introduced. Rewards for Founders and liquidity providers in general depend not on the amount of liquidity tokens they stake, but on the amount of RAID tokens present in their liquidity shares at the time of staking. So, for liquidity providers the incentive to provide liquidity and stake increases with price going down. Founders potentially get the cheapest possible price for RAID token per liquidity share, therefore their rewards will be the highest as long as they keep staking. As soon as they unstake, they lose the advantage. Founders also lose Founder status as soon as they unstake their liquidity from Founders Contract and become a liquidity provider.

Founder status gives Founders ~150% higher rewards than a normal liquidity provider for first 25 years of the project operation. Because of such a long multi-year hold, Founders, as well as liquidity providers, are able to switch addresses if they feel the need to, which allows them to claim their stake and rewards from a different address. This will introduce a degree of centralization in governance and wealth distribution that is required to counter potential threats discussed in Part 3.

Every Ether deposit is being subtracted by 0,5%, and this 0,5% will be used for audits, bug bounties and development like oracles, servers, RPC, ddos protection(as it starts with centralized oracle and only after moves to completely trustless architecture) and any other expenses required by RAID during LGE.

Public temporary database

RAID will use fast centralized public blockchains as temporary databases. It will start from Matic Network as it will perfectly suits RAID purposes and will create proper general public image. The database has to be blockchain agnostic because modern sidechains are lacking restrictions in functionality and balanced tokenomics(as they are businesses, not ideas), because of which the fees on a particular network can become unacceptably high for RAID workers. RAID creates a legitimate use-case even for Cardano.

Database contract is a simple event emitter with settings variables for oracles to act upon. Workers will emit events in database contract with the information about their posts. Commit-reveal scheme nearly eliminates front-running as well as allows this system to scale to any number of workers and websites. Emitting an event ideally has to be a lot cheaper

than 1 cent. After and if all fast blockchains become more expensive than RAID requires, there are at least 2 solutions to resolve it:

1. Add oracles between workers and blockchains. This solution could also allow to use slow chains like Ethereum Classic.

2. Create super lightweight restricted to certain functionality second layer only for oracles to act upon. Could use Autistic roll-ups(an even lighter version of OVM, specifically dedicated to support oracles with events being wiped regularly).

Or both. Ideally, RAID will have to give a worker a choice: broadcast through an oracle aggregator, or broadcast on his own, in case of censorship or because of any other reason. RAID dependence on centralized chains is around 0, emitted events have to exist for a month maximum, and probably it could be made so, that it would only need a week. Using public blockchains as databases is not just about transparency. It's the only way to properly scale it as a decentralized project, as a censorship-resistant source of truth. The contracts will be deployed per certain amount of workers registered in the network so that it will be able to scale effortlessly. The number will be defined with usage statistics.

RAID will require custom encoding for probably many languages, as UTF-8 is inefficient by blockchain standards. Every community dedicated to specific language can submit an efficient encoding scheme if they feel like it's needed.

Raid Wallet

RAID wallet is a browser extension. As of yet, no ability to connect to any website, no ability to transact either, it's a brick. Extension was supposed to be a Metamask fork from the start, this is how the name "RAID" was born with a logo of one-eyed sage wolf, and if Metamask attacks a logo, we can make it 2D and more detailed, like add Caduceus on the background. It's supposed to be a sanity check to DeFi cuteness, it has to be so manly, to point when becomes gay. However, Metamask has committed heresy against free software license. Irony is such, that as RAID wallet does not connect to any website the probability of it being fished significantly reduces. It's very insecure nonetheless as of yet.

The extension fetches specified form data, stores the post and sends a hash of current post and previous post to the blockchain. It can operate on nearly every website on the internet, any social network or html-js chat, from Twitter to Twitch. Functionality of this extension is

restricted during beta-test to imageboards and Twitter by centralized oracle. It will probably be restricted for a lot longer than that, and different relevant websites support will be added gradually over time. As well as other functionality which a modern crypto wallet usually lacks, like limit orders and Inaccurate Transfer contract interface.

During beta-test workers will be able to specify any secure address which will receive beta-test salary, the extension is not supposed to hold any funds as of yet. Beta-test salary is possibly the highest salary in RAID value, 1 token per post. After extension will be secure enough, the workers will lock a certain amount of tokens in worker wallet to be able to work. Different jobs could require different lock amounts. Workers can also participate in governance with their locked amounts. The websites can restrict functionality of this extension, but this is solvable by moving away from extension to RAID browser. Could be a fork of Chromium or Firefox.

Tokenomics and strategic funds

Token utility and multi-year token locks require high inflation in order to support decentralization progress.

Starting supply: 1 billion.

Total supply: 1 trillion.

Emission: maximum emission is approximately 1,9 billion each year with 1,7 billion in first 5 years. Can be adjusted to maximum inflation of ~2,2 billion each year or decreased to minimum ~1 billion per year. First year includes testnet rewards, 1 token per post. Note: while some funds' tokens are being unlocked on fixed schedule, it does not mean that all unlocked tokens are being claimed, so it's better perceive these numbers as maximum possible inflation, not actual inflation. The reason behind these numbers is mainly an attempt to make 1 token always affordable to the residents of poorest countries, assuming that Pareto distribution in cryptocurrency is extreme, as the main income behind is passive. RAID is designed to be retarded, so it's important for numbers to be comprehensible to not only economists.

The funds are a set of upgradeable contracts until finalized. After finalized the ownership will be renounced. A deadline of 2 years for finalization is hardcoded in upgradeable proxy, if the contracts won't be finalized at that point in time, they will be set in stone as is. In case

of me feeling like I don't have time left, I will transfer ownership to another developer, or developer + governance multisig, or to governance(if the governance contract will be ready at that moment). Ideally the code should be set in stone as fast as possible, in first months and keys must be burned as soon as possible, so it will less likely end like Bitcoin – tamed. This amount of funds exist specifically as a mention to the purpose of these funds, as a memo on why they exist. There are 7 funds:

1. Marketing fund. 500 billion tokens are locked in this fund with the highest emission of all funds. Approximately 1 billion default emission per year.

Marketing fund will be the backbone of RAID for around 5 centuries. All it is for is to support default campaigns, to promote RAID or whichever name it will have. Workers will receive salary for default campaigns from this fund. _beforeTokenTransfer() fixed emission ensures that too many workers will be unable to consistently claim salaries, while the price of RAID is too low in first years from inception. It does not mean however, that a worker who was unable to claim loses his salary, he will be able to claim *eventually*. This will allow to properly setup and scale oracle network to prepare the network for potentially millions of workers. This could also create an incentive to FUD RAID in case when there will be too many workers, which will result in mostly smart workers getting on board(while Founders would rather shill RAID after Founding Event is over). Default jobs will have least requirement for tokensLocked, and probably least pays. At the start there will be only 1(one) job – RAID job.

2. Liquidity providers and oracles fund. 49 billion tokens. Approximately 100 million default emission per year. It might never require emission that high, just in case. This fund will support regular liquidity providers with less rewards than Founders. This fund will also reward massive oracle network required by RAID.

3. Treasury(salaries, meme fund, movies). 99 billion tokens. Approximately 100 million default emission per year. A fund for salaries of elected community managers, moderators, technical support. This fund is merged with Meme and Art fund, which was considered at early stages of development, so it will support monthly meme contest winners, and also could allow governance to publish at least cheap literature and sponsor indie film makers.

To prevent too much spam in meme contest while at the same time not causing stagnation, only addresses with at least 1 RAID token will be able to submit memes to the community as NFT, and the governance decides on how good are the memes, top third of memes

receiving the most votes in a month are eligible for reward. Winning memes are being resubmitted for the next month, therefore best memes can receive rewards for several months.

4. Independent medical research fund. 99 billion tokens. Approximately 100 million default emission per year. Unlocks after 5 years of RAID operation, since it's not just about fundamentally pure incapable of any malicious activity governance, it is more about developing a careful plan of how exactly the fund money have to be spent. This is very personal, this is basically my final statement, this is why I am doing all this.

My personal proposal is to follow the same paradigm as medical science does – eliminate causes of death no.1. As most popular issues get resolved, scientists and physicians will be able to pay a lot more attention to less popular, basically everybody win. First, we can solve smoking. We could fund cigarettes with 0 nicotine, containing nicotine substitute, ensuring that even chain smokers will quit. Nicotine substitute has already proven itself as the most effective cure against nicotine dependence, all the industry now requires is not tablets but cigarettes containing it. It could be called RAID. RAID could collect a small(actually small not like governments do) fee from revenue. I am not sure however how legal settlement with decentralized entities works or is there even a law on that.

We could also attempt to eliminate depression, as it could potentially be the actual killer no.1, can't really prove that, only speculate. But I believe it's easier to at least somehow tackle depression issue by introducing logic into every school, rather than focusing on treatments. And of course, which could be even better, this fund could probably be spent exclusively on life extension research, cryopreservation and such.

This fund is supposed to support medical research in countries where it will be cheap. It can be at least 2x more effective than super-empires spending. We could start in Greece, as Greece is a powerful meme in first world and the country can quickly get some informational dominance.

5. Free open-source fund. 49 billion tokens. Approximately 100 million default emission per year. This fund will support any established free open-source developers that oracles will be able to fetch from the internet and propose for governance to decide upon. First, as the governance model is not ready, it starts with a centralized list, which includes developers of any libraries and software being used in the creation of RAID. As a great side effect this fund could potentially attract best developers to RAID.

I sincerely hope that free open source crowdfunding will become a standard in cryptocurrency space, as it seems any other attempt, like asking for donations, consistently fails. One day, we will make these heroes rich.

Another purpose of this fund is to also support non-profit social networks like Mastodon and imageboards. Imageboards need next level popularity, next level mainstream adoption, so that people will ask more and more about what is it about being anonymous? Why is it important? So that they will more likely to value privacy, lean towards spyware-free programs and OS. By promoting free software and privacy, we will make hardware developers add label to their product: “we support privacy and free software”. Or else they will be going down in flames, we will promote their rivals who will not be tyrannical.

6. Charity fund. 99 billion tokens. Approximately 100 million default emission per year. Unlocks after 5 years of RAID operation. It is important to be somewhat understandable, so while we are basically a charity providing jobs and money to the poor, we need a dedicated fund. It will mainly sponsor charities of countries participating in RAID in an attempt to reduce crime. It will also allow investors to argue with tax officials. Or what it could do is to buy cheap smartphones for the poor, so they will be able to work in RAID. That would however require an absolutely unthinkable amount of money. Something can be done.

7. Developers fund. 99 billion tokens. Approximately 100 million default emission per year. It could be merged in one with free open-source fund, however it’s important to put an emphasis on that a part of the fund is specifically dedicated to support existing established free open-source, while this one is to develop new free open-source, hence these funds are split in two. Obviously, a little part of this fund will support RAID network developers, which includes everything for decentralized word-of-mouth marketing service to operate smoothly.

I will have fixed 30 mil of RAID tokens from this fund, which is no way anything significant in case if something happens to me, as starting supply is 1 billion. A developer who will help me from the start will have 5-10 mil, or as much as community sees reasonable.

All other developers will not have a specific fixed allocation but a salary instead based on the monthly index of RAID to USD. Their salary can vary from 50k to 500k USD per year, depending on the amount of work and responsibility, and while first some developers will be hired in centralized way, after the governance goes live, the governance can fire any developers they don’t like and hire new ones on defined by governance terms.

When it comes to programming, I am not a believer in big teams. I believe that many will agree that small but dedicated teams can easily turn out to be more efficient. I propose the strategy for this fund to be focused on developing free open-source alternatives of any closed source paid software. So it will be a lot, really a lot of small teams up to 5 people maximum maybe. They will create an alternative to Photoshop, Sony Vegas, Google search engine, car driving AI, etc. Including Windows, GPU drivers, any sort of software, including even game engines, we can develop free open source games with all assets being completely free to reuse, which will decrease the cost of game development. RAID software needs special license so that the developers will be unable to move away from free license, a license that can't be changed. It's either the owner of the software is RAID as decentralized entity, or it's a license that can't be changed as defined in the license, but there could be holes in the law.

If Linux Mint becomes compromised, and it is highly likely as soon as it gets really popular, we can build on top of their legacy and call it Linux Tall Hat, I guess.

There are plenty of things not only to bring open-source but also to develop. To make sure that our software does not make tracking RAID investors easier, we have to create all our software so that it smoothly operates on any OS. The fund will also pay (hopefully the most generous) bug bounty and for audits.

Anonymous trustless oracle network

If we can't know anything about an anonymous wallet except his balance, that could be the only way to define who is more likely to be a unique human. To increase the probability of that the several oracles are definitely not one person, we need to allow anonymous oracles only with considerably high balance, we can even start from whales, top 100 addresses, and if nobody joins, decrease the requirements to top 200 addresses, etc. Ideally richest RAID addresses, so that they have the least incentive to lie as an oracle and to ruin the reputation of the network in the eyes of the workers. RAID however, can know another variable about an anonymous oracle – language. Language communities can elect oracles, and the probability of them being one person decreases even more.

Concentrated wealth however is a point of failure, creates centralization, so we will absolutely have to use oracles with smaller balances, but that will naturally require KYC and reputation.

With Chainlink verifiable random numbers it is possible to allow anonymous and pseudo-anonymous oracles to deliver true results. Oracles shouldn't know what role they are performing in a given iteration of publishing results. There have to be two roles: witnesses and supervisors. Supervisors' results are considered to be true, and witnesses results have to match it. If supervisors' results don't match, majority of identical results of supervisors and witnesses are considered true, and minority results are punished, if there is no clear majority, another attempt of choosing supervisors occurs, until supervisors results match, while published results stay, no republishing occurs during that.

There will be more than one database contract and oracles for each of them, oracles cannot include any addresses not registered in their given database as eligible for payout, so oracles can at best censor some addresses collectively, or increase existing addresses rewards. A sanity check exists in payout contract of how much a human poster can realistically post, so even a collective successful lie won't be devastating to the system.

Results have to be published monthly or weekly. After results are published, they stay for a while for independent reviewers to observe(they could use observer software that will be available for the purpose), if something is wrong, the governance can punish an oracle but only in predetermined lower-upper limits depending of how much lies occurred, only then workers will be able to claim their salaries.

It requires success of lying to be close to 0. Chosen supervisors have to be a small uneven amount of all oracles. This system is a matter of numbers and tweaks. It could potentially be very expensive to maintain such a network, but personally I cannot see a better way yet. At some point oracles job will become even more expensive when it will require the oracle to imitate human browsing for some resources, especially if they will restrict simple efficient fetching on purpose. This network in theory could also serve as a reliable link between blockchains for small value transactions, as an alternative to Polkadot, the question is, if it will be cheaper at all or not, probably not.

Where it is required, fetched by oracles data has to be first voted on by active workers without taking into account their stake(that's why we need to increase the probability of workers being human), we could also use KYC but only for small balances without sense of humor. And only then approved by workers options will be given to the governance of bigger balances which can stay anonymous. For example, oracles could just fake the data about nonexistent medical facility which has a lot of wallets, enough for all oracles, so active workers will probably reject that. Receiving grants address should not be a contract, so it will be harder transparently cooperate for successful lie. This is also the most

important reason to get on our own chain with restricted functionality, so we can protect strategic funds and the purity of the governance.

A challenge is to define what inaccuracy is acceptable to not be punished in the nature of particular job. An honest oracle can easily miss, say, 3 posts out of 10k posts, maybe more, depending on the resource.

RAID oracle network does not require transferring value, but with this architecture there could be safe thresholds for transferring value. Even if it could probably be more efficient to do through Polkadot network, as an alternative users could be buying Matic native token by sending Ether to a contract on Ethereum network. This oracle network can also react to news and create trustless government proposals.

Adding oracles between workers and the blockchain is also an option and there are numerous ways of implementing that, we could either use the same massive trustless system, or we could make it so that a worker connects to several oracles, and if these oracles censor this worker, then he moves to other oracles, essentially censoring oracles lose money.

Fundamentally pure governance

Malicious governance is common. The way is to simply disallow being malicious as much as possible. In case with RAID it’s not just potential riches of strategic funds, it is also about being compromised by a government’ intelligence. First problem is updating contracts maliciously. It seems impossible to me to implement any restrictions on upgrades that the governance can approve. The DAO can override nearly any hardcoded limits. Checking a part of bytecode of next logic implementation in assembly is futile, any variables can be reassigned and overriden.

As far as I went, there is no way to implement any limits in proxy contract except block limit on how often/when the contract can be upgraded and for how long. Could be useful to create investors' confidence for centralized projects with anonymous developers, but not for full DAO, which could potentially be compromised and completely ruin the idea behind the project. So what required is to ensure that code of all contracts will be eventually set in stone with no ability to change the governance contract anymore. As soon as possible.

Second problem is about managing strategic funds and is a lot harder to solve. This functionality requires absolutely next level DAO' purity of intentions. What I propose to resolve it is to only allow certain options for governance to decide upon fetched by trustless oracle network. For example, to sponsor open-source project and to ensure that it is not a scam to get money from RAID governance, oracles fetch only established projects with certain minimum measurable limits like time since inception, popularity and such. Same could go for medical research, oracles can propose only existing established companies or doctors with verifiable profiles by social networks or anyhow transparent and convenient. Supporting charities, movies and literature can be possible by fetching information from right resources with right filtering.

So the governance can choose options that oracles propose. And in this particular case all oracles will be capable of reaching 100% accuracy matches in results. At least with proxies they probably will be, or we will have to exclude certain websites. Any grant is not being transferred in one big transaction. Claiming of the grant starts from 0, not truly final, and the DAO can shut it down, if something is wrong. With this governance model it’s also possible for the DAO to create verifiable tasks in many fields, essentially it allows to create a true government above governments.

Creating a balanced voting system is a challenge. In the early stages of RAID development, a multi-year token lock was the backbone of voting system, and voters didn’t have any passive income. Passive income for voters is what creates imbalance, a fair amount of voters just do not vote, they only need passive income, and therefore nobody can ever be certain of how will given voting participation turn out.

So the idea was about investors locking tokens for at the very least 3 years if not 5 for voting as a means of protecting a bigger investment, passive income comes only from the price increase with right decisions taken. And, last half of year of token lock voting is forbidden for a voter, unless he prolongs the lock. While this model seems great to me, it means that Founders won’t have a certain degree of power required to protect RAID from specific issues discussed in Part 3. It was planned that LGE participants and liquidity providers definitely should not be voting because of the very reason that they have passive income. But that can easily make RAID lose it’s course. So I believe currently, that voting for Founders and liquidity providers should be accessible with their staked liquidity, however only after a lock, if they choose to lock it, or to elect themselves – they can use it as a voting power, if they choose to just have passive income, they don’t need to lock it. A lock should be a sort of sacrifice I believe, it has to be as long as possible, so nobody will lock and disrupt voting balance just because he maybe could be voting. The functionality requires only dedicated voters.

With this model we can have a high percentage for minimum quorum. We can have 40-60% instead of 4-10% for a proposal to be executed. The governance model still remains the biggest challenge of RAID architecture and probably requires way more brain power than I will ever have. We need to discuss it and decide upon the best possible model.

A check if contract should be present, so nobody will be able to easily and transparently trade votes OTC. But in case if with Ethereum 2.0 or any upgrade, check if contract becomes useless, then safety measures are in place, without oracles governance can't choose much. However, that might not be enough, and maybe migrating to RAID chain is the only way to ensure security. ERC-20 allowances can be used to trade locked voting power transparently, so RAID token contract will have an additional check on to which contracts allowance is possible to grant, like DEX contracts. However, if we allow voting with Uniswap LP tokens, then we can't impose any allowance restrictions since the token contract is being deployed through Uniswap factory contract, so what I propose is to maybe gradually decrease voting power of LP tokens over years to around 50% of original voting power, with eventually migrating all voting on our own second layer, which won't have any LP tokens probably. Important to mention that the system does not really critically break if there will be ways to trade votes transparently and even trustlessly outside of Ethereum.

After analyzing current Ethereum incentive collisions between investors and miners, I believe that voting on most critical changes has to be split in stages: first stage is when the smallest balances of active human workers are voting, and if the smallest balances approve a proposal, then it proceeds for voting of biggest balances. For some proposals there could be even more than 2 stages, but basically it will be a lot harder to compromise such a system, if governments can't directly *influence* key party, there should not be any key party like miners with static geographic location unable to be anonymous at all.